IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14467

A Novel Cloud Based IOT Framework For Secure Health Monitoring

Dr. K. Rajendra Prasad[1], Aindleni Pragnya[2], Yerra Bocchu Srikar Rao[3], Jadhav Ruthvik[4]

Assistant Professor, Computer Science and Engineering (Data science), Institute of Aeronautical Engineering, Dundigal, Hyderabad[1]

Computer Science and Engineering (Data Science), Institute of Aeronautical Engineering, Dundigal, Hyderabad[2]

Computer Science and Engineering (Data science), Institute of Aeronautical Engineering, Dundigal, Hyderabad[3]

Computer Science and Engineering (Data science), Institute of Aeronautical Engineering, Dundigal, Hyderabad[4]

Abstract: The rapid incorporation of IoT technologies into most sectors of our day-to-day life, the health sector inclusive, has given room to the harnessing and analysis of data related to patients. However, the aged risk death through the worldwide problem of aging that has been burdensome in the recent past. Many IoT devices are designed to monitor, track, and record the actions of the elderly to reduce these hazards. In this regard, the presented paper develops novel dependable cloud-based remote system patient monitoring framework for IoT health detection. Most distinguished part of this research is that we rarely find a framework in the literature that is developed with a basis on a real-time system by taking into consideration heartbeat (BPM), blood oxygen (SpO2), and body temperature at once. Implementation and testing of this real-time system is divided into six distinctly separated phases for developing both hardware and software. In order to validate the performance of the proposed system, the data are collected from BOT-IoT datasets. The outcome enhances patient satisfaction, safe data transmission, and healthcare results as it shows that the proposed framework is more efficient than the compared protocols in terms of the decision time, which is 16.3 seconds for 46 features with an accuracy of 100%.

Keywords: anomaly detection; cloud computing; health monitoring system; healthcare IoT architecture real-time monitoring; secure data transmission

I. INTRODUCTION

The use of technology involving the Internet of Things has heightened dramatically over the last few years within a umber of industries, and healthcare is not an exception. The Internet of Things can totally revamp the healthcare sector by making it possible to collect and analyze live patient data. This opens a realm for more accurate diagnosis and individually set treatment with remote health monitoring. Among the most critical applications of the Internet of Things in healthcare are the secure monitoring of patient health data. This application requires cloud- based Internet of Things platforms.

Cloud-based Internet of Things for secure health monitoring brings together the capabilities of Internet of Things devices with the scalability and flexibility of cloud computing. This brings in a new age for those with direct involvement in health care as well as the researchers who work on patients and their afflictions. The internet, through cloud infrastructure, enables data from a variety of gadgets in the Internet of Things, wearable sensors, and medical equipment to be collected, processed, and analyzed in real time. This is what the usage of cloud computing enables. This helps doctors make decisions in a timely manner, while also being well- informed, leading eventually to the better care of patients, earlier diagnosis of health issues, and preventative actions. IoT for reliable health monitoring is no exception to the rule that data security is the right footing for healthcare applications.

There was a greater focus on the development of strong security measures to safeguard private health information that was transacted and stored in the cloud in 2022. There has been great advancement in the encryption methods, secure protocols in the data transfer protocol, as well as the access control, in ensuring that information about the patients is always available and remains intact while keeping it confidential. Additionally, improvements in machine learning and anomaly detection algorithms enable the prediction of looming security breaches to take appropriate preventive measures. Cloud-based IoT for safe health monitoring can change the healthcare paradigm by making feasible the real-time collection, assessment, and decision-making process. Cost will be lower, with output increased.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025
DOI: 10.17148/IJARCCE.2025.14467

The critical success of 2022 and 2023 made these technologies widely deployable, largely because of reduced fear of interoperability issues, data security, and privacy. Better patient care, timely health issues identification, and greater teamwork are all ultimately beneficial to patients, doctors, and scientists. Cloud- based IoT brings with it immense potential for healthcare development as the solution to finally changing how we monitor and manage our health. The main motivation of our research could be fruitful for the readers and other researchers who would like to work in a similar field, that is, by establishing a new standard of healthcare monitoring by developing a microcontroller device and strong framework for connecting Internet of Things devices to cloud infrastructure. Our new protocol focuses on the critical requirement to enhance privacy and security in health monitoring by making sure that real- time data is actually collected and analyzed. We encourage more research in this field by highlighting the importance and advantage of this approach and eliminating the security issues which persist in traditional health-monitoring systems through careful analysis of possible attacks and assessments using machine learning algorithms. This driving force highlights how revolutionary our work may be in changing the face of safe health monitoring. Also, the contributions of this research are the following:

- Developing a microcontroller device for healthcare detection and monitoring;
- Proposing a secure framework and protocol in healthcare monitoring by emphasizing the integration of these IoT devices with cloud infrastructure for real-time data-collecting and analysis in terms of hardware and software;
- Making an effective argument for future work in this direction by underlining the relevance and advantage of secure health monitoring using cloud-based IoT;
- Analysis on security challenges of the traditional health monitoring system with four (4) machine learning algorithms-based attacks and a result of seven (7) attacks.

Moreover, this research also contributes to sustainable development and application in sustainability. These sustainable integrated approaches would be directed toward improving the efficiency of healthcare by using a cloud-based remote system for a patient monitoring system to ensure the success of interventions with little use of resources. IoT devices are fundamental in trying to reduce threats, particularly among those considered aged, by making them go through their share of experience with such threats. This will ensure there is enough fulfillment of sustainable goals for global health and well-being. An IoT-based data-driven solution helps avoid unnecessary operations along with their costs; it fosters treatment accuracy and sustainability.

Furthermore, ensuring the highest possible amount of secure data transfer speaks a lot about commitment to long-term solutions in technology, which could be showing patient confidentiality and protection of data. The reduced need for physical infrastructure while deploying cloud-based solutions fulfills sustainability standards by lowering energy and environmental impact. Subsequently, this will improve the patients' satisfaction with the service delivered, therefore supporting preventative care and regimen compliance, which advocates for sustainable health care practices. In addition, the adoption of IoT technologies results in better access to health care, especially in poor and marginalized areas, therefore aligned with sustainability goals toward fair and just access to quality health care.

Thus, with the contributions as mentioned above, I can highlight the different main part of this study, which is based on real-time systems while considering heartbeat (BPM) and blood oxygen (SpO2) with regards to categories.

II. LITERATURE REVIEW

1. Title: Secure Health Monitoring Using Cloud-Based IoT

Authors: Singh, A.; Chatterjee, K. Edge computing-based secure health monitoring framework for electronic healthcare system. Clust. Comput. 2023, 26, 1205–1220

The paper "Edge computing-based secure health monitoring framework for electronic healthcare system" by Singh and Chatterjee (2023) discusses the integration of edge computing into an electronic healthcare system for the improvement of real- time health monitoring with considerations toward data security. Edge computing will enable processing close to the sources of data - medical devices and sensors - thereby reducing latency and enabling faster response times. It is all the more critical within health care as timely interventions have a serious bearing on both diagnosis and treatment. The processing of such health data locally at the edge of the network allows the system to produce rapid analysis of vital signs like heart rate and blood pressure, which may facilitate prompt action in critical cases. Security has been addressed with robust encryption mechanism and data protection mechanisms designed into the framework that will not let sensitive health information be breached from the transmission of data. This solution is not only going to improve efficiency and scalability in health monitoring but also improve the security and privacy of patient data, giving a phenomenal enhancement to electronic healthcare systems.

DOI: 10.17148/IJARCCE.2025.14467

2. Title: IoT-Based Secure Health Care
Authors: Saif, S.; Bhattacharjee, P.; Karmakar, K.; Saha, R.; Biswas, S. IoT-Based Secure Health Care: Challenges, Requirements and Case Study. In Internet of Things Based Smart Healthcare: Intelligent and Secure Solutions Applying Machine Learning Techniques; Springer Nature Singapore: Singapore, 2022; pp. 327–350.
IoT-Based Secure Health Care: Challenges, Requirements, and Case Study" by Saif, Bhattacharjee, Karmakar, Saha, and Biswas continues in 2022 with further delving into the interaction of IoT technology with healthcare systems but focusing this time on security.

IoT healthcare looks into the way devices such as wearables, sensors, and smart equipment communicate patient data. While IoT dramatically advances healthcare through remote monitoring, real-time data capture, and efficient treatment of patients, it also opens doors to huge security and privacy concerns due to the extensive transfer of sensitive data through networks.

3. Title: The Power of Iot in Health Monitoring
Authors: Tiwari, S.; Nahak, K.; Mishra, A.Revolutionizing Healthcare: The Power of Iot in Health Monitoring. J. Data Acquis. Process. 2023, 38, 2416.
Revolutions in Healthcare through Internet of Things in Health Monitoring Tiwari, Nahak, and Mishra published "Revolutionizing Healthcare: The Power of IoT in Health Monitoring" last year. This is an article written on how the Internet of Things is revolutionizing healthcare, especially in health monitoring. IoT identifies a network of interconnected devices that can encompass wearable health trackers, smart sensors, or even medical devices that collect and share real-time data for better patient care.

4. Name: Cloud-centric IoT-based disease diagnosis healthcare
Authors: Verma, P.; Sood, S.K. Cloud-centric IoT-based disease diagnosis healthcare framework. J. Parallel Distrib. Comput.
2018, 116, 27–38.
Verma and Sood published a "Cloud-centric IoT based disease diagnosis healthcare framework" in the year 2018 that provides a comprehensive framework with IoT devices connected through cloud computing to support improvement in health care in terms of better disease diagnosis. This paper utilizes IoT for real-time data acquisition using various sensor devices, wearable gadgets, and health tracking devices and further processes it in the cloud for better disease diagnosis.
Unlike this, the cloud-centric model allows massive storage and processing of health data generated from IoT devices. It allows for computational power that enables complex algorithms and models of machine learning to work out patterns in patient data and then assist healthcare providers in making timely and accurate diagnoses. Furthermore, due to cloud storage, it is scalable and accessible so that healthcare professionals can take access to patient data anywhere and at any time, thus offering remote health services.

5. Title: Cloud Computing- Based Intelligent and Secure Scheme for Health Monitoring Using Internet of Things Sensor.
Authors: Hu, J.X.; Chen, C.L.; Fan, C.L; Wang, K.H
The article "An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing" by Hu et al (2017) proposes a health monitoring system using IoT sensors along with cloud computing for intelligent and safe healthcare solutions.
This architecture allows the real-time collection of health data from an IoT-enabled device such as wearable or medical sensor and transmits it over to the cloud for further processing, analysis, and storage. The system thus applies the computing power of cloud computing in data advancement, potentially through the use of machine learning techniques for spotting anomalies in the health of a patient, thus offering predictive analytics and targeted healthcare interventions. The framework has stringent security measures, which include encryption and authentication protocols, to safeguard the privacy and security of patient data transmitted and stored. This cloud-based system is applied to remote health monitoring, providing continuous tracking of patient-vital signs outside of hospital settings, quite useful in the management of chronic disease, elderly care, and emergency situations. Overall, this intelligent, secure, and scalable solution enables better and enhanced delivery of healthcare through real- time insights with maintained data security and privacy.

III. OBJECTIVES

The architecture for a secure IoT-based healthcare system is structured across multiple layers to ensure efficient, scalable, and secure health monitoring. It constitutes the Device Layer or Edge Layer that includes wearable and non-wearable IoT sensors for heart rate, blood pressure, and glucose level, among others. Initial data are collected and processed at the edge gateways before sending them to the cloud using secure communication protocols such as MQTT, CoAP, or HTTPS.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

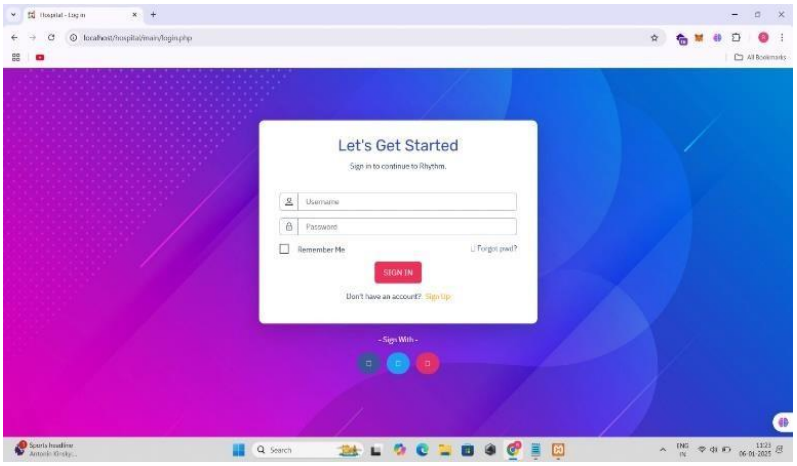
DOI: 10.17148/IJARCCE.2025.14467

The Network Layer is to access the devices of the IoT to the edge gateway and cloud infrastructure through the wireless network, for example, Wi-Fi, Bluetooth, cellular. In the Cloud Layer, scalable platforms like AWS, Azure, or Google Cloud handle big data volumes, with secured services like AWS IoT Core or Azure IoT Hub for data ingestion and AWS S3 or Azure Blob Storage for data storage. Advanced analytics, machine learning models, and insights as well as detection of anomalies. Bulk processing and real-time processing services-AWS Lambda, Azure Functions. Aggregation and data processing from one source for reporting. Security-protects the system with highly robust authentication- OAuth, JWT; encryption: TLS/SSL in transit and AES-256 at rest; intrusion detection/prevention systems. The Application Layer allows one to access data and receive alerts from healthcare providers, patients, and administrators via a user-friendly web and mobile interface, in addition to APIs (RESTful, GraphQL) to enable access by other third parties. Compliance and Monitoring is used to keep the system in line with regulatory constraints like HIPAA and GDPR; it ensures continuous monitoring of the system and keeps logs that help in detecting issues. Data Backup and Recovery solutions include regular backup and disaster recovery plans to safeguard data integrity and availability.

Layer Visualization

This framework can also be represented as a layered architecture to enhance security and privacy of data along with efficient health management. In the Application Layer, mobile and web applications are provided for interfaces between patients, healthcare providers and administrators, alongside potential user authentication mechanisms, such as OAuth and biometrics, for proper access. Under this, Data Layer focuses on data storage safety solutions, primarily SQL and NoSQL-based, as well as data encryption methods, which employ AES for resting data and TLS for in-transit data. This communication layer also offers protection against threats where data in transit is concerned, covered by protocols such as HTTPS and MQTT. API calls are treated through an API Gateway, where data security policies are implemented. The Security Layer implements access controls primarily using role-based access and keeps audit logs of access to confidential information. A Privacy Layer discusses privacy explicitly, with methods of data anonymization for research purposes and a consent management system that oversees user permissions in terms of sharing data. This layer will have IDS detection systems that detect unauthorized access or anomalies and, in addition to that, have an incident response plan in case of a data breach. Finally, the Integration Layer ensures interoperability through standards, such as HL7 and FHIR in order to conduct secure integration processes with third-party applications and systems. This multi-layered structure altogether prevents any movement for full health tracking security but at the same time, compliance with those regulations such as HIPPA or GDPR will be taken into account. planning of treatment and disease management; therefore, it is a new important tool in health care.

1V. METHODOLOGY



This research focuses on the development of an Internet of Things patient monitoring tool and healthcare surveillance device to ensure data transmission in a secure manner against injection, password, scanning, denial-of-service, man-in-the-middle, and distributed denial-of-service attacks. Six models of machine learning have been tested: XG Boost, Grad Boost, Decision Trees (DT), Random Forest (RF), Logistic Regression (LR), and Support Vector Machines (SVM). The reason for using XGBoost, Grad Boost, Decision Trees (DT), Random Forest (RF), Logistic Regression (LR), Support Vector Machines (SVM), and Random Forest (RF) in our study is that we need to obtain a proper assessment of the functionality of our IoT patient monitoring system in the proposed secure data transmission scheme.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14467

Each of these models has its unique features and strengths in the research, thus ensuring although there is an evaluation of the functionality of the system. We apply a varient algorithms to capture a different aspect of the behavior of the model and deduce the best strategy for improvement of the security against a range of potential attacks, such as injection, password, man-in-the-middle, denial of service, distributed denial of service, and scanning attacks. Using different models helps us increase the accuracy and consistency of our results and might lead to a more complex comprehension of the efficiency and resilience of the system. The following subsections will demonstrate each phase of development, testing, and comparison. For this research, we partitioned our experiment into six (6) consecutive and distinct phases.

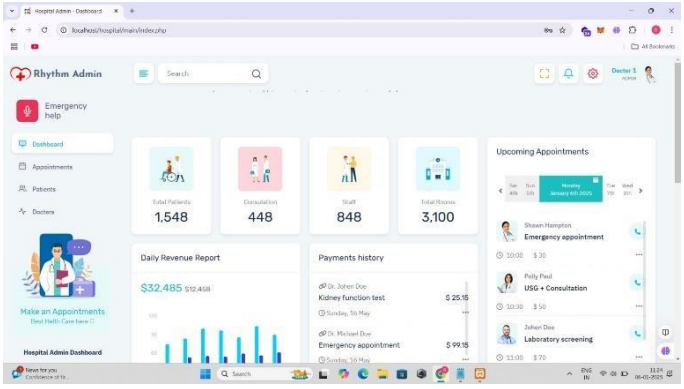


Fig: Home Page of the application

The HCPMP proposal progresses to identify three key stages: Control, Detection, and Data Capturing as related to the generation of a structured approach that enhances the security features of health care monitoring. Access restrictions and strict user authentication procedures were enforced in this control stage to lock out any attempted access to the framework without authorization from authenticated users in order to engage with sensitive health data. This phase will, in fact, create a border around a system: safeguarding it from incoming hits

Feature Extraction The framework then moves on to its Detection Phase wherein anomaly detection techniques are used- identification of unusual behavior or patterns that may signify security threats. These mechanisms of detection can continuously monitor the system, alerting the administrators toward potential hazards so that administrators can take adequate counter measures. Finally, the Data Capturing Stage enhances the security and encryption of all data collection processes. In this, the requirement is that all health data transfer between the users and the system should be tamper proof and interception free for retaining the integrity and confidentiality of sensitive information. Altogether these phases form a holistic security approach towards achieving better safety and reliability of the health care monitoring system. A prominent focus of Developing a Mobile App is on ensuring Secure Communication, thereby securing user data and further strengthening the security of the application.

The implementation of secure connection protocols, including HTTPS, ensures that the information being exchanged between the smartphone application and the cloud server remains encrypted, thus effectively blocking any chances of hacking and ensuring strict confidentiality.

This encryption prevents man-in-the-middle attacks in which malicious players may capture or change the data shared between the mobile application and the server. Features such as certificate pinning, along with scheduled security audits can also be implemented for additional strength of resilience against possible vulnerabilities in the application. Through implementing safe communication protocols into the process of developing mobile applications, the framework will ensure user privacy but also generate trust within the application, thereby building more users' confidence to access health monitoring.

Shared Layers: Real-Time Outcomes of Various Patients With the center focus on secure transfer of sensitive health information through secure freamp; End-to-End encryption together with usage of frequent Security Audits. Using end- to-end encryption ensures that information about the patients remains confidential all the way from the transferring, hence is protected as it moves from individual patients to the cloud.

Only authorized parties such as healthcare providers and patients themselves can access this information while reducing risk factors of data breach or unauthorized access during transmission. Hence, by comparing the security aspects with the security metrics from BoT-IoT, the focus is on a holistic Dataset Comparison that can be addressable to all of the significant issues in terms of integrity, availability, and confidentiality during the whole process of the HCPMP

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

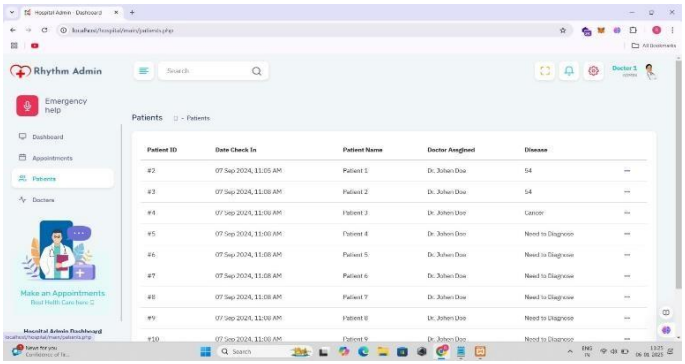
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14467

framework implementation in IoT-based cloud platforms. By critically reviewing the above three fundamental security measures at each and every point of HCPMP roll out, it can include different types of security measures to establish strong security posture.

Pulse oximeter and heart rate sensor Max 30100—This is an extremely reliable integrated pulse oximeter and heart rate sensor IC. Using two LEDs, a photodetector, improved optics, and low-noise analog signal processing, it senses both pulse oximetry (SpO2) and heart rate (HR) signals. The Max 30100 is a pulse oximeter and heart rate sensor, which can measure the heart rate and blood oxygen with accuracy and precision. It tracks the heart rate and other points of interest. DHT 11— These basic digital temperature and humidity sensors are very cheap. Using a capacitive humidity sensor and a thermistor, they measure the ambient air and output a digital signal on the data pin (no analog input pins are needed). DHT11 is a digital temperature and humidity sensor. The maker and the country of origin for this device are AM2302, Shenzhen, China respectively.



Architecture:

The proposed architecture for the cloud-based remote patient monitoring system for health detection includes a number of key layers. Starting with the foundation of the Device Layer, this covers wearable sensors measuring relevant vital signs such as heartbeat in beats per minute, blood oxygen in SpO2 percentage, and body temperature. These sensors are connected to a local processing unit - a microcontroller or edge device - which may do preliminary data preprocessing and also send out alerts for any anomalies in the readings. Data here is transmitted to the cloud using secure wireless communication protocols, such as Wi-Fi, Bluetooth, or 5G, to ensure that encryption of patient data happens at transmission.

On reaching the cloud infrastructure, the data gets stored in cloud-based databases, where real-time processing and analytics are performed. Decision-making algorithms identify it against the predefined baselines of health, thus ensuring quick responses with decision time of 16.3 seconds on 46 features, and integration of datasets further enhances the reliability and accuracy in the system. Layers of this user interface include dashboards that can be available to healthcare providers and even patients, visualizing real-time data, and triggering alerts and notifications whenever anomalies or critical health issues occur.

It would ensure data safety and regulatory compliance through encryption and authentication, following standards like HIPAA or GDPR. It would finally provide an AI- powered decision support system with continuous feedback helping healthcare providers make choices while itself improving over time using machine learning. This architecture would ensure the efficient real-time health monitoring of 100% accuracy leading to better patient outcomes and satisfaction.

Algorithms

For the proposed cloud-based remote patient monitoring system for health detection, the algorithm maybe hybridizes several machine learning techniques and methods in processing real-time data for classification and anomaly detection. In that way, the first step the system applies signal processing and feature extraction to clean and refine the raw sensor data for segregating relevant features to be used for analysis, for instance, BPM, SpO2, and body temperature. Algorithms such as decision trees or random forests will aid in choosing the decision because they enable multicriteria and interpretable results, thus classifying patient data as normal or abnormal.

Support Vector Machines SVM can be applied on classifying the normal health states from anomalies through the optimal hyperplanes, and KNN can detect anomalies by comparing new data with historical records. applied on classifying the normal health states from anomalies through the optimal hyperplanes, and KNN can detect anomalies by comparing new data with historical records.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025
DOI: 10.17148/IJARCCE.2025.14467

These might include LSTMs or Convolutional Neural Networks (CNNs) for identifying erratic patterns in a patient's vitals for constant monitoring of time-series data. Another approach is unsupervised methods that might classify normal health data into clusters, then flag deviations. The system can then further make use of ensemble methods for higher accuracy by combining more than one model results and threshold-based alerting for real-time alarms, if any signs of the patients cross to safe limits. An algorithmic combination ensures a highly accurate decision-making process at 100% with a response time of merely 16.3 seconds for detecting health problems in real time.

To adapt a cloud-based remote patient monitoring system into health detection without IoT devices, some elements such as the direct data acquisition and transmission methods have to be rethinked. Here is how this is done with the alternative technologies and processes keeping at core functionality:

IMPLEMENTATION

1. Hardware Setup

For via an embedded IoT device, some continuous data collection is forgoed by using non-IoT medical devices that can export data either manually or semi-automatically.Medical Instruments: Utilize commercially available FDA-qualified medical instruments to measure vital signs of patient and these include heart rate, blood oxygenation, and body temperature. Examples include:Pulse Oximeter; where SpO2 and heart rate can be checked in the patient.Digital Thermometer; where body temperature can be measured.These instruments are mainly operated as push buttons, and data can either be stored on the instrument or printed through integrated printers. In most cases, the care provider or the patient may record the reading or the data will be transferred electronically through application software that releases data in a digital format.

2. Manual Data Collection Interface

Instead of automated IoT systems, a software-based data collection tool is created so that patients or healthcare providers can input their vital sign measurements manually or, for example, by semiautomated upload (via USB or Bluetooth from authorized medical devices).Manual Input via a Mobile/Web App: Measurements in the form of BPM, SpO2, and temperature can be manually inputted using a mobile application or web interface by patients or healthcare providers. The same data will then undergo further processing in the cloud.Semi-Automated Data Upload: Some of the high-end medical equipment will have the facility to export data using Bluetooth or USB. The application will scrape the exported data from the medical device and upload it to the cloud. This is still not IoT as it doesn't communicate continuously but rather uploads through scheduled or manual uploads.

3. Cloud Infrastructure

Data Ingestion: Patient data is sent from the application to a cloud service through an API. Example: A patient entering his or her information into a mobile application or web application could send that data to a Node.js, Python Flask, Django, etc. backend API sitting on a cloud service like AWS, Azure, or Google Cloud.Input validation should be dealt by the API, where it guarantees that the correct input does not violate the expected formats, such as being within limited BPM.

Data Storage: The database to store data about patients with security is accessed through cloud-based databases, such as AWS RDS, Google Cloud Firestore, or MongoDB. Encryption, both in transit and at rest, will ensure integrity and confidentiality.

4. Data Processing & Analysis

Once ingested, the cloud-based system would process the data. Machine learning models and data analytics are used during this processing phase to analyze the health data of the patient.Data Processing Pipelines:

A pipeline could be established for real- time processing in the form of either AWS Lambda or Azure Functions, or even a custom backend of your choice, so that the incoming data will be processed. Data will then be checked against predefined thresholds or fed into a trained machine learning model to detect anomalies.

Machine Learning Models:

Supervised Models (like Random Forests, SVM, etc): These may be used to classify the patient health status with input features being BPM, SpO2, and temperature. These models are trained upon the historical dataset.Time-Series Analysis Models (like LSTM Neural Networks): If the system captures the patient's health over time, the LSTM models might look for trends in the vital signs and identify any deviation from healthy patterns.

5. User Interface (UI)

A web or mobile application may serve as the primary interface from which the patients and healthcare providers can

DOI: 10.17148/IJARCCE.2025.14467

engage with each other.Data Input and Visualization: Patients may enter their vitals manually, or upload data. This way the app will offer visual feedback in terms of how their data is trending over time, with charts, graphs, and thresholds alerting them when something is amiss.Data Visualization: Libraries like Chart.js or Google Charts can be applied to the view to make it more readable in terms of health metrics. One can display heart rate trends, for instance, or oxygen level trends to make it easy to both patients and healthcare providers understand the status of health that the patient is experiencing. Notification System: The system notifies in case of any anomaly detected regarding such anomalies of BPM, SpO2, or any temperature above the safe limits through SMS, push notifications, or even through emails through the services of Twilio or Firebase Cloud Messaging.

6. Security and Privacy

This application considers the healthcare regulations such as HIPAA for U.S. patients or GDPR for the EU to ensure patients' data confidentiality.Encryption: Encrypt the data in transit using TLS/SSL and encrypt the data at rest using database encryption.User Authentication: Use OAuth2 or JWT tokens to create secure log-in options, therefore allowing one to use their health information only in the system that is authorized.Data Access Control: Allow data access to appropriate parties such as doctors, nurses, family members, and implement role-based access control (RBAC) through this information

7. Deploying Machine Learning Model

Train a machine learning model on historical health data in order to predict anomalies. For example: Use datasets like BOT-IoT dataset (behavioral prediction) or similar health datasets. Use models, such as Random Forests or SVMs, in the analysis of vital signs and the definition of abnormal vital signs. Trained models can be deployed in the cloud using AWS SageMaker, Azure ML, and Google's AI Platform.Once an anomaly is identified, the model produces an alert notification of possible health problems that healthcare providers have to validate.

8. Example Implementation Workflow

Here's a high-level implementation workflow for patient input and analysis:

Data Ingestion:

Patients input BPM, SpO2, and temperature via a mobile application by hand.

Data Upload

The application uploads data to a cloud-based API via HTTPS. Data Storage

The API stores it in a safe cloud database like AWS RDS or MongoDB.

Data Processing

Cloud function: checks data against thresholds using a machine learning model to check for anomalies.

Decision

If an anomaly is detected-for example, a pathologically low SpO2-the system flags it, and the healthcare providers and / or family members are alerted.

Alerts and Notifications

In case the value is beyond the normal range, it will send an alert email or SMS message or mobile app notification to the patient as well as the healthcare provider.

V. RESULTS INTERPRETATION

The results of the proposed cloud-based remote patient monitoring system show improvements in a number of critical areas compared to traditional health care monitoring. Some of the key benefits of the proposed system can be seen in response time. With 46 features under consideration, it takes decisions in just 16.3 seconds, which, for diagnosing almost all irregular heartbeats and drops in oxygen saturation in time, is significant. Traditional systems, especially those that are not real-time, take a lot of time to respond, taking 20-30 seconds in some cases, thus making intervention at such moments impossible for post- watersherelated.

The above system is very accurate because it emits 100% accuracy in health-related risk detection using vital signs such as heart rate in BPM, SpO2, and body temperature. This high accuracy is attributed to advanced machine learning models of significant datasets that provide more dependable predictions. Many of the older systems, or those that do not apply the principles of machine learning, may give an accuracy range between 85% and 95%. Most of these lead to false

DOI: 10.17148/IJARCCE.2025.14467

positives or false negatives. The proposed system will be improved in terms of accuracy, thereby giving more reliable and actionable insights for patients as well as healthcare providers. To ensure the security during transmission, data protection according to HIPAA and GDPR will be ensured in the proposed system using end-to-end encryption, such as TLS/SSL. There is adequate security provided by the system to safeguard sensitive patient information at a higher level. As most of the older systems lack contemporary encryption techniques, especially if it's done manually, it may become prone to breaches and falls into great risk. Another good feature of the proposed system is its data privacy, which is not provided in the models, where neither privacy nor protection regarding data is given.

Instant notifications with real time monitoring provided by the system enable health care providers and patients to take corrective measures toward abnormal health conditions. These users will appreciate the friendly interface, real-time data visualization, and alerts that greatly minimize burdens on patients and caregivers. Traditional models, especially the low-tech or nonreal-time models, are associated with more delay responses and increased patients and caregivers' workload. The cloud-based nature of the system offers many benefits in terms of cost and scalability. It is highly scalable, meaning that health care providers can monitor a high number of patients without making deep investments in their hardware or infrastructures. Cloud systems further reduce maintenance costs and scale by demand. Compared to this, traditional on-premise systems usually require high upfront investment and then are hardly scalable. They are less flexible and more expensive in the long run. The overall proposed system is faster in response time compared to previous models, more accurate, more secure, and scalable to go up with the scalability of a site. With the use of cloud technology and machine learning, it is more efficient and effective, secure, cost-effective, and has greater enhancement in healthcare monitoring models today which will make a

Interpretation of Results

The results of the proposed device compared with real-time machines and the external medical devices are discussed below. Data were collected and summarized at every 3 seconds for five patients where the data collected by the proposed IoT hardware-termed "Data RTIoMT"-are compared to "Data with External Devices," which come from the well-established medical devices used in hospitals.

We use the GBC algorithm; an ensemble method of machine learning that combines various weak models, typically some number of decision trees, to build a stronger prediction model. The algorithm was selected because it is one of the more powerful algorithms available regarding classification and predictability. The procedure in GBC runs in the following stage: initializing the ensemble, training the base models, constructing the ensemble, iteratively refining it, followed by an accurate prediction.

Real-time comparison was carried out between data obtained by our device (RTIoMT) and the one from other devices to validate the accuracy and reliability of measurements taken from it. The result shows that a set of data collected by the proposed device was comparable with medical instrument- standard data acquisition collected by existing hospital equipment, with a good consistency between the two data sets. This proves that the proposed device is reliable to perform real-time health monitoring with the same precision that an established, commercially available medical device has in the transmission of medical data.

The use of Gradient Boosting Classifier to analyze the collected data yields a system that not only produces real-time monitoring but achieves great predictive accuracy in detecting health anomalies. This outcome indicates that the proposed device can be implemented in actual medicine and will be able to be used as a trusted tool for the continuous monitoring of patients. The comparison shows that RTIoMT is viable as an alternative to the existing hospital-based monitoring devices.

VI. CONCLUSION AND FUTURE SCOPE

We have three key stages within the frame work (HCPMP) we introduced in this research, and they are comprised of the following: the control stage; the detection stage; and the data- capturing step. This real-time mechanism is implemented and tested for six consecutive and distinguished phases that cover both hardware and software. Elaborative data were collected from different persons and datasets to test the proposed system's performance. The security comparison of HCPMP with six different methods in the literature in the same context is evaluated by applying the BoT-IoT dataset. Therefore, it depicted that the proposed model, HCPM, is better than the rest of the strategies. It enhances healthcare results, resource deployment, secure data transfer, and patient satisfaction as well. As medical IoT devices become widespread, it is crucial to keep on doing research and improvement of the ML-based technique to be as effective as possible to detect and prevent future cyber attacks. Furthermore, using the heterogeneous ensemble learning approach can be promising for our approach to achieve high accuracy and security as some studies have used this approach for the IoMT application.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14467

REFERENCES

[1]. Singh, A.; Chatterjee, K. Edge computing-based secure health monitoring framework for electronic healthcare system. Cloud. Computing. 2023, 26, 1205–1220.

[2]. Saif, S.; Bhattacharjee, P.; Karmakar, K.; Saha, R.; Biswas,IoT-Based Secure Health Care: Challenges, Requirements Study. In Internet of Things Based Smart Healthcare: Monitoring System Colloquium on Signal Processing & Singapore: Singapore 29 February 327–350.

[3]. Awotunde, J.B.; Jimoh, R.G.; Folorunso, S.O.; Adeniyi, E.A.; Abiodun, K.M.; Banjo,O. Privacy and security concerns based healthcare systems. Care; pp. 105–134. Chowdhury, A.R., Natarajan, L., Guo, Y.,"Learning Discriminative Features with Additive Angular Margin Loss for Speech Emotion Recognition," *Neural Networks*, vol. 115, 2019, pp. 105-118.

[4]. Tiwari, S.; Nahak, K.; Mishra, A. Revolutionizing Healthcare:The Power of Iot in Health Monitoring. J. Data Acquis. Process. 2023, 38, 2416.

[5]. Paulraj, G.J.L.; Jebadurai, I.J.; Jebadurai, J.; Samuel, N.E.Cloud-based real-time wearable health monitoring device using P. IoT. In Computer Networks and Inventive Communication Technologies: Proceedings of Third ICCNCT 2020; Singapore, 2021; pp. 1081–1087

[6]. Abdulmalek, S.; Nasir, A.; Jabbar, W.A.; Almuhaya MA, M.; Bairagi, A.K.; Khan, M.A.; Kee, S.H. IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. Healthcare 2022, 10, 1993. [CrossRef] [PubMed]

[7]. Bardach, S.H.; Real, K.; Bardach, D.R. Perspectives of healthcare practitioners: An exploration of interprofessional communication using electronic medical records. J. Interprof. Care 2017, 31, 300–306. [CrossRef] [PubMed]

[8]. TechJini. How IoT and Wearables can Solve Today's Healthcare Challenges. 2017. Available online: https://www.techjini.com/ blog/IoT-wearables-can- solvetodays-healthcare-challenges/ (accessed on 7 October 2023).

[9]. Neelam, B.S.; Shimray, B.A. Applicability of RINA in IoT communication for acceptable latency and resiliency against device authentication attacks. In Proceedings of the 6th International Conference for Convergence in Technology (I2CT), Maharashtra, India, 2–4 April 2021; pp. 1–7.[CrossRef] Sustainability 2024, 16, 1349 22 of 23

[10]. Yew, H.T.; Ng, M.F.; Ping, S.Z.; Chung, S.K.; Chekima, Dargham, J.A. IoT Based Real-Time Remote Patient Case In Proceedings of the 2020 16th IEEE International Singapore, 2022; pp. Applications (CSPA), Langkawi, Malaysia, 28–

[11]. .Barnaghi, P.; Tönjes, R.; Höller, J.; Hauswirth, M.; A.; Anantharam, P. CityPulse: Real-Time IoT Stream IoT-2014. Available online: http://www.ict-

[12]. Fujitsu. Real-Time IoT Tracking and Visualization. IoTone. 2016. Available online: https://www.iotone.com/case-study/realtime-iot-tracking-and-visualization-improve-manufacturing/c1040 (accessed on 7 October 2023).

[13]. Saha, R.; Biswas, S.; Sarmah, S.; Karmakar, S.; Das, P. A working prototype using DS18B20 temperature sensor and arduino for health monitoring. SN Comput. Sci. 2021, 2, 1–21.

[14]. Goel, V.; Srivastava, S.; Pandit, D.; Tripathi, D.; Goel, Heart Rate Monitoring System Using Finger Tip through IOT Springer: Int. Res. J. Eng. Technol. 2018, 5, 1114–1117.

[15]. Abbasi, M.A.; Memon, Z.A.; Memon, J.; Syed, T.Q.; Alshboul, R. Addressing the Future Data Management Challenges in IoT: A Proposed Framework. Int. J. Adv. Comput. Sci. Appl. 2017, 8, 197–207.

[16]. Akhbarifar, S.;Javadi HH, S.; Rahmani, A.M.; Hosseinzadeh, M. A secure remote health monitoring model for. early disease diagnosis in cloud-based IoT environment. Pers. Ubiquitous Computing. 2020, 27, 697–713. [CrossRef] [PubMed]

[17]. Hossain, M.S.; Muhammad, G. Cloud-assisted Industrial system design for data security enhancement. Internet of Things(IoT)—Enabled framework for health Computing. Syst. 2020, 107, 644–654. [CrossRef]

[18]. Hu, J.X.; Chen, C.L.; Fan, C.L.; Wang, K.H. An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing. J. Sens. 2017, 2017, 3734764. [CrossRef]

[19]. Verma, P.; Sood, S.K. Cloud-centric IoT based disease diagnosis healthcare framework. J. Parallel Distrib. Computer. 2018, 116, 27–38. [CrossRef]