International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 3, Issue 4, July – August (2025)

RESEARCH ARTICLE

# REAL-TIME IOT HEALTHCARE MONITORING USING WEARABLE SENSORS AND HYBRID DEEP LEARNING MODELS

Neeta Suryakant Brahme [1, *] and Jameer Kotwal [2]

[1] Research Scholar, Department of Electronics & Communication Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University, Vidyanagari, Jhunjhunu, Rajasthan, India.
[2] Assistant Professor, Department of Computer, Dr. D. Y. Patil Institute of Technology, Pune, Maharashtra, India
[*]*Corresponding e-mail: karhadkarneeta@gmail.com*

**Abstract – The healthcare industry is evolving at a quick pace, and that necessitates the integration of effective, scalable, and secure solutions that will manage the increasing volume of sensitive patient data. This is because of the aging population, increased cases of chronic diseases, and the necessity to track patients in real-time efficiently. To improve remote diagnosis and decrease reliance on hospital-based treatment, the Internet of Things (IoT) and Wireless Sensor Networks (WSNs) have been combined to allow constant monitoring of vital indicators such as heart rate, blood pressure, temperature, and oxygen saturation.However, there are still issues with current IoT-enabled healthcare systems, such as high communication latency, scalability restrictions, impacts about data privacy and security in cloud storage, and a lack of intelligence in analyzing complicated biomedical data. To overcome these issues, this paper proposes an improved Internet of Things (IoT) healthcare monitoring system that combines wearable biomedical sensors, a Raspberry Pi CPU, and fast 5G connectivity for data transfer in almost real-time. The system captures minor changes in biological signals by preprocessing physiological data and using Renyi Entropy to extract important characteristics. These are categorized using a hybrid Temporal Convolutional Network Bidirectional Long Short-Term Memory (TCN-BiLSTM) model that can recognize trends over the short and long term. For remote monitoring, data is safely kept in the cloud and accessed through a web app. Evaluation metrics such as encryption time, decryption time, response time and computation cost.**

***Keywords*** *– Wireless Sensor Networks, Internet of Things, Raspberry Pi, Renyi Entropy, 5G connectivity.*

## 1. INTRODUCTION

The healthcare industry has expanded and evolved, as it currently contributes a lot to revenue generation and job creation [1]. Patients must spend more time in hospitals during the traditional disease diagnostic process since it frequently requires extensive physical examinations that must be performed at medical centres [2]. This system has raised healthcare expenses and placed a lot of strain on medical facilities, particularly in remote and difficult-to-reach areas [3]. Technological advancements, such as the usage of tiny devices like smart watches, have resulted in over-monitoring of health and the diagnosis of several ailments and illnesses. Consequently, the patient-centered healthcare has replaced the hospital-centered system [4]. The services related to health are stretched to their limits by the increasing population of elder citizens and chronic cases.

Remote health monitoring has been adopted to address this challenge by improving patient care, reducing medical costs, and decreasing hospitalisation [5]. There are many health-related data collected by remote monitoring systems; these data include the temperature of the body, heart rate, oxygen, brain (EEG) and heart (ECG) beats. With this information, one can identify the current health issues and offer physicians up-to-date information [6]. Internet of Things (IoT) makes this possible by enabling regular devices with smart features that improve their functionality and communication, especially in healthcare-related services [7]. Remote healthcare services have become possible due to the emergence of connected devices and high-speed networks, such as 5G [8]. Through the help of cloud computing and mobile technology it is now possible to gather, store and analyse vast amounts of patient data successfully [9]. These machines guarantee that essential measurements are possible to be performed in a constant, the illnesses can be identified at a suitable time, and emergency alarms can be dispatched. Patients do not need to visit the hospital on a regular basis to undergo routine diagnostics [10].

In spite of all these, there are still several challenges that hinder the implementation of smart healthcare systems to its maximum potential [11]. Even though networks are used to share confidential medical information and store it in cloud servers, one of the primary concerns is data security and privacy [12]. The sheer volume of data produced by IoT devices poses a problem in data processing and administration too. Additionally, traditional systems lack intelligence to analyse complex medical data appropriately. Because of the physical and financial limitations, not all healthcare facilities can introduce such technology, especially in low-resource settings [13]. To overcome these challenges, a proposed IoT healthcare monitoring system

uses a Raspberry Pi, wearable biomedical sensors, and 5G connectivity to monitor patients in almost real-time.

- The proposed method uses a hybrid TCN-BiLSTM model for classification after applying preprocessing and Renyi Entropy to identify significant features from minute fluctuations in physiological data.
- For remote healthcare monitoring, patient data is safely kept in the cloud and accessed through a web application.
- Metrics including encryption time, decryption time, response time, and computing cost are used to assess the system's performance.

The rest of this paper is divided in the following way: Section 2 will give the Literature Survey on the existing techniques. Section 3 describes the Proposed Methodology. Section 4 covers the Results and Performance Analysis and Section 5 concludes the paper with future work.

## 2. LITERATURE SURVEY

In 2023 Pushpakumar, R., [14] suggested a Hybrid encryption method as the way to ensure the safety of the patient data in IoT-based healthcare systems on the cloud. The suggested approach was a combination of RSA and AES to provide secure key exchange and expedited dealings. Overall, the suggested approach is a balanced and effective solution that optimizes the functionality and scalability of the system and data security of medical data to be exchanged and stored on cloud technologies.

In 2023 Jabeen, T., et al., [15] suggested an intelligent healthcare system wherein nano sensors are used to gather and relay real-time health information to experts via wireless networks. The suggested solution adopted a genetic-based encryption system, in order to protect information against possible attacks in transit. The findings indicate that the suggested approach was lightweight, power-saving, and reduces time delay by 90%, therefore, a secure and efficient alternative in an IoT-based healthcare.

In 2024 Sangeetha, S.B., et al., [16] suggested a Secure Healthcare Access Control System (SHACS) framework to enhance the efficiency and safety of the access to Electronic Health Records (EHRs) by mobile healthcare application. The suggested approach integrated the Role-Based Access Control (RBAC) and the Attribute-Based Access Control (ABAC) in authentication. In general, the security and reliability of the proposed method performance are considerably improved.

In 2024 Baccour, E., et al., [17] proposed a pruning model of Deep Neural networks (DNNs) in healthcare with Explainable AI (XAI) to realize pruning without retraining. The proposed methodology offers a balance between precision and resource consumption in the combination of distributed inference and Non-Linear Integer Programming (NLP), and it will generate real-time pruning choices with the assistance of the Reinforcement Learning. This method offers an effective, adaptable, and non-invasive mode of accurate DNN inference in real-time hospitals.

In 2025 Zhang, Y., [18] proposed a Fine-grained ciphertext sharing system model to help in managing medical data in the clouds safely and efficiently. The proposed solution combined the Searchable encryption, proxy re-encryption and differential privacy in order to obtain privacy and usability. A performance analysis and a security analysis demonstrate that the proposed methods ensure the medical data are secured.

In 2025 Yan, P., et al., [19] proposed a Hybrid Cloud Architecture TwoFish Encryption Algorithm to provide an efficient and fast way of securing data. The proposed solution used the fingerprint authentication and fingerprint virtual machine to create the untraceable security keys to enhance the overall security. The overall proposed performance against conventional approach was the high access speed and encryption.

In 2025 Iot, H.T., [20] proposed a Reinforcement Learning (RL) based on IoT healthcare to enhance real-time decision-making, patient care, and resource allocation. The proposed model provided a dynamic and elastic model of computing with recurrent RL to dynamically manage the resources based on the demand of the system. The proposed solution provides intelligent, scalable, and sustainable healthcare to emerging digital ecosystems

## 3. PROPOSED METHODOLOGY

In this section, the system starts with the patient having a number of sensors and these sensors include sensors of temperature, heart rate, blood pressure, and oxygen level. These detectors involve the gathering of the physiological signals which is converted to a digital format through an analog-to-digital converter (ADC). The digital data is received in a Raspberry Pi device which then act as the processing centre and transmits the data via a 5G connection to a remote server. A display unit is attached to this server as a monitoring tool and it can be used via Wi-Fi to provide medical assistance. The collected data is then subjected to a data processing phase. The initial stage is pre-processing which cleans it and prepares it to be analyzed. Features are then extracted on the sensor data by means of Renyi entropy which helps in the identification of the most informative features. These characteristics are then forwarded into a disease prediction model that relies on TCN-BiLSTM (Temporal Convolutional Network - Bidirectional Long Short-Term Memory), a powerful deep learning model that is able to identify health anomalies. A critical case check is performed after prediction. When the situation appears to be critical, medical support is arranged immediately, otherwise the system might make the patient be ambulanced. The overall proposed framework is depicted in the figure 1.

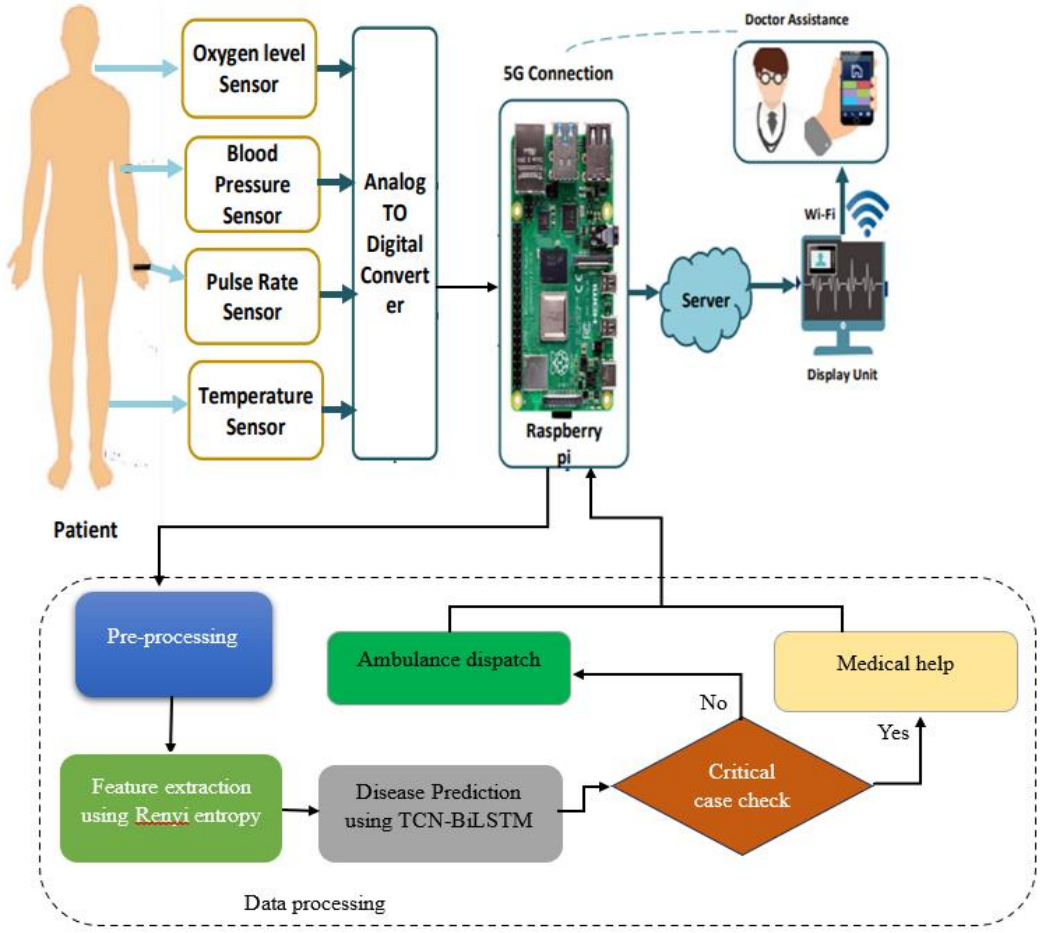


**Figure 1.** Proposed Methodology

**Sensor Interfacing:**

To collect information, the system initially attaches biomedical sensors to a platform of Raspberry Pi. The sensors include blood pressure sensor, heart rate sensor, body temperature monitoring sensor and oxygen saturation sensor (SpO2). Such devices offer real time and continuous physiological data that are necessary in establishing the condition of the patients.

$$S = \{BP, HR, Temp, SpO2\}$$

**Data Acquisition and Preprocessing:**

The collected data of measurements is sent to the preprocessing stage. Here, the data integrity is established through the elimination of noise, normalization of values and handling of any missing/distorted data point. This stage standardizes the data to be analyzed and extracts the characteristics in an accurate manner.

$$D_{pre} = normalize(denoise(S))$$

**Feature Extraction (Renyi Entropy):**

In order to enhance sensitivity management to indicate distributions, this system employs Renyi Entropy, a prolonged form of Shannon entropy instead of conventional ANN-based feature extraction. Renyi Entropy is a measure of the complexity and unpredictability of biomedical signals. It is particularly good at distinguishing normal and abnormal physiological trends in non-stationary non-linear data, such as rise in temperature, PPG, or ECG. The result of this process is a small feature set that is highly discriminative.

$$F = RenyiEntropy(D_{pre})$$

**Decision Making (TCN-BiLSTM):**

The extracted features are classified with the help of a hybrid deep learning model that involves the combination of Bidirectional Long Short-Term Memory (BiLSTM) and Temporal Convolutional Networks (TCN). TCN guarantees the efficacy of parallel processing along with the motion patterns and the lengthy-range interdependence of the time series health information. BiLSTM examines forward and backward sequences of features in order to model the incorporate past and future context to make more accurate predictions. By combining convolutional and recurrent temporal modeling features, the hybrid TCN-BiLSTM model enhances the accuracy of detection of crucial health events.

$$\hat{y} = Model_{TCN-BiLSTM}(F)$$

**Cloud Storage and 5G Transmission:**

The output of the analysis is stored safely on the cloud, ensuring scalability and easy accessibility. The processed data is then provided to remote computers and health providers with low latency using 5G network access, which can then monitor and respond nearly in real-time.

$$CloudData = upload(\hat{y}) \xrightarrow{5G} Server$$

**Web Application and Data Retrieval:**

The medical experts can access patient data through a specialized online application. The system retrieves the latest records in the cloud in order to visualize and facilitate decision-making and monitoring.

$$View = fetch(CloudData)$$

**Critical Case Verification and Response:**

During a critical case check, the condition of the patient is evaluated to determine whether the case is an emergency case or not. Healthcare personnel are notified through a medical help request in an event where a critical situation is diagnosed. In other cases, an ambulance dispatch is initiated when there is a necessity of immediate transportation. This improves the chances of the survival of the patient and ensures early intervention.

$$Alert = R(\hat{y} - T)$$

$$Alert = 1 \; if \; y \geq T$$

$$Alert = 0 \; if \; y < T$$

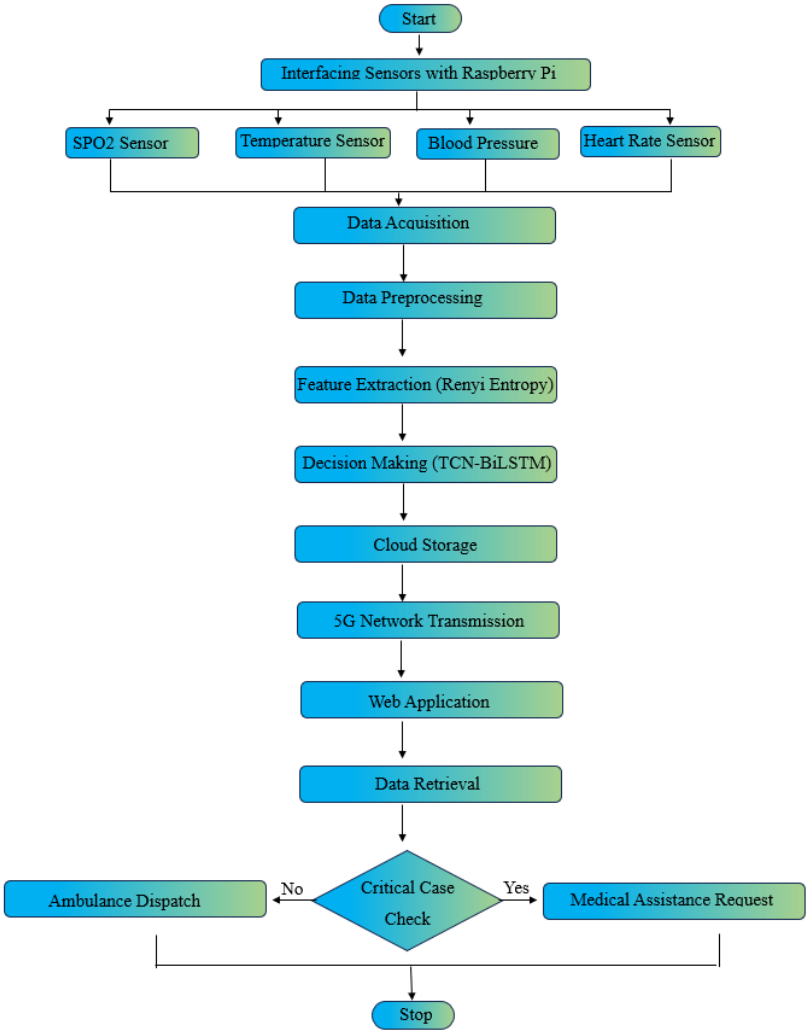


**Figure 2.** Flow chart for Proposed methodology

## 4. RESULTS & DISCUSSIONS

The proposed IoT healthcare system uses wearable sensors, a Raspberry Pi, and 5G for near real-time monitoring. Renyi entropy is used to preprocess the data and extract features. Health problems can be accurately classified using a TCN-BiLSTM model. Performance is evaluated using encryption time, decryption time, response time, and computation cost, showing better accuracy, speed, and efficiency than existing methods.

### *4.1 Performance metrics*

**Computation cost:** The entire amount of energy, memory, and CPU cycles used for encryption, decryption, and other security procedures. $C_{enc}$ denotes the cost of encryption, $C_{dec}$ indicates the cost of decryption and $C_{com}$ represents the cost of computation overhead.

$$C_{com} = C_{enc} + C_{dec} + C_{com}$$

**Encryption time:** The amount of time the algorithm needs to transform unencrypted data into encrypted text.$S_{enc}$ denotes the speed of encryption and N indicates the input data size.

$$T_{enc} = \frac{N}{S_{enc}}$$

**Decryption time:** The amount of time needed to restore the original plain data from the ciphertext. $S_{dec}$ denotes the speed of decryption and N indicates the ciphertext size.

$$T_{dec} = \frac{N}{S_{dec}}$$

**Response time:** The entire amount of time which includes encryption, transmission, and decryption that passes between a request and the system's provision of the final result.$T_{enc}$ denotes the encryption time, $T_{trans}$ indicates the transmission time, and $T_{dec}$ represents the decryption time.

$$T_{res} = T_{enc} + T_{trans} + T_{dec}$$

### *4.2 Comparative Analysis*

The proposed method has been compared with the existing techniques such as NS-GBE, RRL, RSA-AES in terms of response time, computation cost, encryption and decryption time.

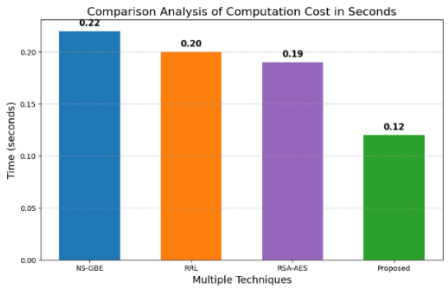


**Figure 3.** Computation cost

Fig 3. Illustrates the bar graph compares the computation costs for four distinct methods NS-GBE, RRL, RSA-AES, Proposed and all expressed in seconds. The methods with the fastest computation times are NS-GBE (0.22 seconds), RRL (0.20 seconds), and RSA-AES (0.19 seconds). The highest performance is shown by the proposed method, which is substantially faster than the other methods and achieves the lowest calculation cost of 0.12 seconds. The efficiency of the proposed method in terms of computing overhead is demonstrated by this decrease in processing time, which makes it more appropriate for situations where quick execution is essential.

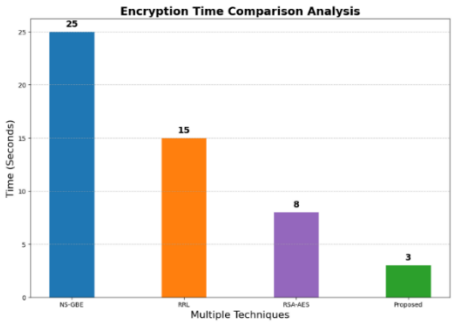


**Figure 4.** Comparison of Encryption time

Fig 4. Demonstrates the comparison of encryption time using four approaches such as NS-GBE, RRL, RSA-AES, and Proposed. The Proposed approach has the least encrypted time of less than 3 seconds which is very much superior to others. This considerable reduction shows the increased speed and efficiency of the suggested approach which is particularly beneficial in the cases when rapid encryption is highly required. The existing NS-GBE has the slowest encryption time of 25 seconds, which implies slower performance, RWL of 15s and, RSA-AES of 8s, respectively.

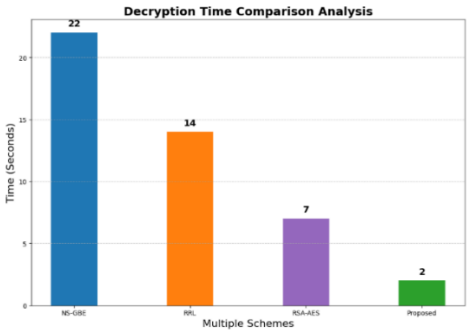


**Figure 5.** Comparison of Decryption time

Fig 5. illustrates the comparison of the decryption times using four methods such as, RSA-AES, RRL, NS-GBE, and proposed. The proposed technique achieves the best performance and requires 2 seconds to decrypt data. This dramatic improvement confirms the fact that the proposed method is very fast in decrypting information, thus it will be suitable in processes of applications that need fast turnaround. The existing NS-GBE scheme is slower evidenced by the longest decryption time of 22 seconds, RR with a shorter time of 14 seconds, and RSA-AES is even more efficient with a time of 7 seconds, respectively.

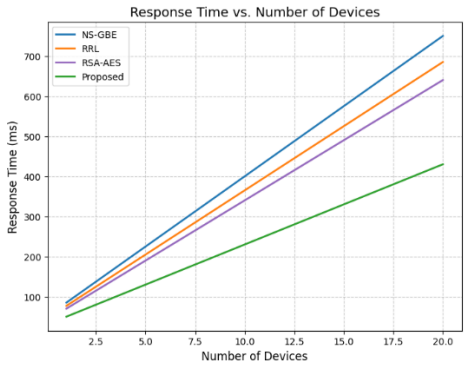


**Figure 6.** Response time

Fig 6. Illustrates the line graph shows the correlation between reaction time and device count for four distinct schemes: The suggested approach, RSA-AES, RRL, and NS-GBE. Response times for all schemes gradually increase as the number of devices rises from 1 to 20. RRL and RSA-AES exhibit moderate gains, whereas NS-GBE regularly has the fastest reaction times. The proposed approach performs better than all others while keeping reaction times noticeably reduced for all device counts.

## 5. CONCLUSION

This paper proposes an IoT-based healthcare monitoring system, in which a Raspberry Pi, wearable biomedical sensors, and 5G are utilized to track patients in nearly real-

time. The suggested approach employs a hybrid TCN-BiLSTM model to classify following preprocessing and Renyi Entropy to find the significant features among minute variation of physiological data. The performance of the proposed method is evaluated using parameters such as response time, computation cost, encryption and decryption time based on the existing methods such as RSA-AES, RRL, and NS-GBE. The proposed method can be compared to NS-GBE and seems to be more suitable in real-time and large-scale applications due to its significantly lower response time, reduced computational scale, and improved scalability. The weaknesses are that it requires 5G connectivity and accurate sensors to work reliably, and there is a possibility of insecure and privacy issues in cloud storage without implementing appropriate encryption or access controls. The blockchain-based access control and advanced encryption will be further employed in cloud storage to enhance security measures

## CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest.

## FUNDING STATEMENT

Not applicable.

## ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

## REFERENCES

[1] N. Alharbe, and M. Almalki. IoT-enabled healthcare transformation leveraging deep learning for advanced patient monitoring and diagnosis. Multimedia Tools and Applications, vol. 84, no. 19, pp. 21331-21344, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] M.N. Khan, Z. Rahman, S.S. Chowdhury, T. Tanvirahmedshuvo, M.R.O. Hossain, M.D. Hossen, N. Khan, and H. Rahman, "Real-Time Health Monitoring with IoT". *International Journal of Fundamental Medical Research (IJFMR),* vol. 6, no. 1, pp. 227-251, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] A.H. Najim, K.A.M. Al-sharhanee, I.M. Al-Joboury, D. Kanellopoulos, V.K. Sharma, M.Y. Hassan, W. Issa, F.H. Abbas, and A.H. Abbas. "An IoT healthcare system with deep learning functionality for patient monitoring". *International Journal of Communication Systems*, vol. 38, no. 4, p.e6020, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] G. Gardašević, K. Katzis, D. Bajić, and L. Berbakov. "Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare". *Sensors*, vol. 20, no. 13, pp. 3619, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] K. Ghoumid, D. Ar-Reyouchi, S. Rattal, R. Yahiaoui, and O. Elmazria. "Protocol wireless medical sensor networks in IoT for the efficiency of healthcare". *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10693-10704, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] G. Premi, P. Solainayagi, C. Srinivasan, and P.G. Kuppusamy, Data Privacy and Confidentiality in Healthcare Applications of IoT-Enabled Wireless Sensor Networks. In 2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon), pp. 610-614, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] X. Zhou, W. Liang, I. Kevin, K. Wang, H. Wang, L.T. Yang, and Q. Jin, "Deep-learning-enhanced human activity recognition for internet of healthcare things". *IEEE Internet of Things Journal,* vol. 7, no. 7, pp. 6429-6438, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] K. Thilagam, A. Beno, M.V. Lakshmi, C.B. Wilfred, S.M. George, M. Karthikeyan, V. Peroumal, C. Ramesh, and P. Karunakaran, "Secure IoT Healthcare Architecture with Deep Learning-Based Access Control System". *Journal of Nanomaterials*, vol. 2022, no. 1, pp. 2638613, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] S. Sengan, O.I. Khalaf, D.K. Sharma, and A.A. Hamad, "Smart healthcare security device on medical IoT using raspberry pi". *International Journal of Reliable and Quality E-Healthcare (IJRQEH),* vol. 11, no. 3, pp. 1-11, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] M. Mamun-Ibn-Abdullah, and M.H. Kabir, "A healthcare system for internet of things (IoT) application: machine learning based approach". *Journal of Computer and Communications*, vol. 9, no. 7, pp. 21-30, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] I. Sharma, K. Kaushik, V. Pahuja, and G. Chhabra, "Employing convolutional neural network for iot healthcare attack detection in intensive care unit". *In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I),* vol. 6, pp. 798-803, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] P.J. Chen, T.H. Hu, and M.S. Wang, "Raspberry Pi-based sleep posture recognition system using AIoT technique". *In Healthcare*, vol. 10, no. 3, p. 513, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] H.J. Mohammed, "IoT-Based Low-Cost Smart Health Monitoring System using Raspberry Pi Pico W and Blynk Application". *Journal of Engineering*, vol. 30, no. 07, pp. 90-108, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] R. Pushpakumar, "Secure Healthcare Data Management: Integrating AES and RSA Cryptography on Cloud Solutions". [CrossRef] [Google Scholar] [Publisher Link]

[15] T. Jabeen, I. Jabeen, H. Ashraf, N.Z. Jhanjhi, A. Yassine, and M.S. Hossain. "An intelligent healthcare system using IoT in wireless sensor network". *Sensors*, vol. 23, no. 11, pp. 5055, 2023[CrossRef] [Google Scholar] [Publisher Link]

[16] S.B. Sangeetha, C. Selvarathi, S.K. Mathivanan, J. Cho, and S.V. Easwaramoorthy. "Secure Healthcare Access Control System (SHACS) for Anomaly Detection and Enhanced Security in Cloud-Based Healthcare Applications". *IEEE Access*, 2024[CrossRef] [Google Scholar] [Publisher Link]

[17] E. Baccour, A. Erbad, A. Mohamed, M. Hamdi, and M. Guizani, "Reinforcement learning-based dynamic pruning for distributed inference via explainable AI in healthcare IoT systems". *Future Generation Computer Systems*, vol. 155, pp.1-17, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Y. Zhang, "Medical Data Security and Sharing Mechanisms in Cloud Computing Environments". *Procedia Computer Science*, 259, pp. 766-777, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] P. Yan, H. Peng, and F. Qi. Enhancing medical cloud security: a multi-level approach with twofish encryption and fingerprint authentication. Sādhanā, vol. 50, no. 3, pp. 148, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[20] H.T. Iot, "Sustainable Healthcare Through Iot and Pervasive Computing: A Reinforcement Learning Approach". *Journal of Neonatal Surgery*, vol. 14, no. 10s, 2025. [CrossRef] [Google Scholar] [Publisher Link]

**AUTHORS**

**Neeta Suryakant Brahme** is a Research Scholar in Electronics & Communication Engineering Department at JJTU Rajasthan India and also working as an Assistant Professor at Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade, Pune, Maharashtra, India. She has completed her M. Tech. (Electronics-VLSI) from Bharati Vidyapeeth University, Maharashtra, Pune. Ms. Neeta has 17 years of Teaching experience. She has published 13 articles in National and International Conferences and journals. She has 2 patents (National). She is Life member of ISTE, IETE and IAENG. Her research interest areas are Wireless Communication, Embedded System, Signal and Image Processing, Machine Learning.

**Jameer Kotwal** is working as an Assistant Professor in Computer department at Dr.D.Y.Patil Institute of Technology, Pune. He has 15 years of teaching experience. He has completed his Ph.D. from Amity University in 2024. His area of specialization is Deep Learning, Machine Learning etc. He has received a grant of 1.5 Lakhs from NVIDIA company for setting up a GPU lab. He has published 5 patents in IPR and 16 copyrights. He has published papers in Scopus and SCI indexed journals. She has attended many international conferences. He also stood second in Amity Incubation Centre.

Arrived: 24.07.2025
Accepted: 30.08.2025