Automated Emergency Treatment with Ai-Prioritized Management in Hospitals

DR. M. Padma Priya[1], Bachu Venkata Thanooj Kumar[2], Aravapalli Hari Krishna Sainadh[3], Adapa Venkata Satya Naga Surya Prakash[4], Annamaneni Rahul[5]

[1]*Assistant Professor, Department of Computer Science and Engineering, Bharath Institute of Science and Technology, Chennai, India*

[2,3,4,5]*Department of Computer Science and Engineering, Bharath Institute of Science and Technology, Chennai, India*

***Abstract*—Artificial Intelligence (AI) and Biometric Authentication have played a major role in the last years in the efficiency and safety of healthcare systems. In this paper, the author suggests a smart healthcare management system integrating multi-biometric authentication with an emergency response mechanism based on ai. The system uses face, palm and voice recognition to facilitate secure user authentication and discourage unauthorized access to sensitive medical information. A smart emergency system is an emergency module that will analyze vital parameters of the patient, including oxygen saturation and heart rate, to determine how serious the situation is and automatically identify the closest hospital and ambulance with the help of location-based services. As shown by the experimental evidence, the proposed system enhances the accuracy of authentication and decreases the emergency response time in contrast with the traditional techniques. The system offers a secure, reliable and scalable solution to the current healthcare applications.**

***Index Terms*—biometric authentication, MRI scans, medical chatbot, food nutrition, appointments.**

I. INTRODUCTION

The fast progress of artificial intelligence (AI) and biometric technologies made possible the creation of intelligent healthcare systems that deliver safe and effective medical services. The conventional hospital systems are mainly based on password-authentication and manual management of emergency cases, which in most cases introduces vulnerability to security and delays in emergency cases. These restrictions may lead to unauthorized access to sensitive patient data and decreased speed of response in cases of medical emergencies.

In order to overcome these issues, this paper is going to present a smart healthcare management system, which combines multi-biometric authentication with an AI-powered emergency response system. The system makes use of face, palm, and voice recognition to provide secure and reliable user verification to prevent unauthorized access. Moreover, the system has in-built real-time emergency management, as it does the vital parameters of patients including heart rate and oxygen saturation to determine the severity of the condition.

Depending on the severity that is predicted and the actual location of the user, the system automatically identifies and directs the nearest hospital and ambulance through location-based services. This will help save a lot of time in case of an emergency and enhance the effectiveness of delivering healthcare services.

The main value of the work is the incorporation of multi-biometric authentication and intelligent emergency management in one platform. The suggested system will increase the accuracy of authentication, patient safety, and offer a scalable solution to the current healthcare setting. Experimental analysis shows that the system performs better than the traditional techniques in terms of security and response time, and is therefore fit in real-world healthcare applications.

II. LITERATURE SURVEY

The latest trends in the healthcare system have been based on enhancing data security, medical diagnosis, and emergency response with the help of artificial intelligence (AI) and biometric technologies. The conventional healthcare systems are mostly based on the idea of password-authentication and central data storage that are susceptible to security breach and unauthorized access [1], [2].

Biometric authentication is a concept that has been embraced to improve security in healthcare applications. Machine learning and deep learning models have been utilized to identify faces, detect voices, and physiological signals to implement authentication [9], [11]. Nonetheless, the majority of the currently available systems are based on one type of biometric modality, which restricts the reliability and risk of false identification. The challenge of multimodal biometric systems has been presented to tackle the issues of multi-biometric traits with one another to enhance accuracy and robustness [13].

Artificial intelligence has been an influential factor in contemporary healthcare systems, as well. Disease prediction, medical image analysis, and patient monitoring using electronic health records and medical imaging data have all been successfully done with deep learning models [3], [4], [10]. Artificial intelligence has proved to be very accurate in image analysis using MRI and identifying diseases, which are of great help when making clinical decisions [14], [15]. But these systems are usually created separately, without being intertwined with secure authentication systems.

Moreover, real-time data and location-based services have been used to design emergency healthcare systems to enhance response time. Health parameters of patients and prediction of medical conditions on the basis of time-series data have been analyzed by means of machine learning methods [6], [7]. Although these systems enhance the efficiency of responding to an emergency, they lack secure patient identification and integrated healthcare management, Biometric authentication, AI-based diagnosis, or emergency reaction, instead of offering an integrated system. Integrated platforms that integrate multi-biometric authentication, AI-informed medical analysis, and automated emergency response are lacking in a single platform. The proposed system will combine multi-biometric authentication with AI-based severity prediction and real-time emergency response to overcome the aforementioned limitations. Such a solution is highly secure to the system, better decision-making, and time to response, which is why it can be used in contemporary healthcare applications.

III. PROPOSED METHODOLOGY

The suggested system can be viewed as a smart healthcare management system combining multi-biometric authentication with an AI-based emergency response system. It is deployed on a web-based framework which comprises of authentication, emergency management, and data processing modules. Users start with registering which requires them to give personal information and biometric data including face, palm and voice samples. At the time of login, the system uses multi-biometric authentication which compares the input data with the stored templates through machine learning models and deep learning models.

After authentication, users are granted access to healthcare services, including emergency help. The emergency module measures vital parameters of a patient like heart rate and oxygen saturation in order to show the extent of the situation.

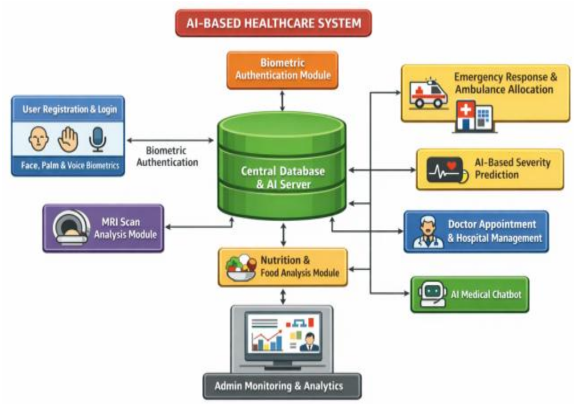

Figure-1: System Architecture

The proposed system architecture includes several interdependent modules that guarantee safe and effective delivery of healthcare services. Biometric authentication module authenticates the identity of the user based on the face recognition method, palm recognition and voice recognition. SVM and convolutional neural networks are machine learning models that assist in extracting and classifying features, which enhances the accuracy and reliability of authentication.

The emergency management module takes real-time patient information, such as the heart rate and oxygen saturation in the body, to categorise the condition as stable, serious or critical. Depending on the seriousness and location of the user, the system finds and allocates the closest hospital and ambulance available based on location-based services.

A centralized database is also incorporated in the system to safely store user data, biometric templates and medical records. It is designed to offer an administrative module to keep track of appointments, oversee emergency requests and ensure the smooth running of the system. This architecture guarantees secure access, real time emergency response, and efficiency of healthcare services.

MODULES DESCRIPTION

1. User registration and biometric enrollment

This module is responsible for secure user registration using multi-modal biometric authentication. The system captures face, palm, and voice samples and stores them in structured biometric datasets. During enrollment, the captured data is processed and trained using machine learning models for future verification. User credentials along with biometric templates are stored in a secure database. This module ensures reliable identity management and prevents unauthorized access to healthcare services.

2. Biometric authentication and login module

This module performs user authentication using face recognition, palm recognition, and voice verification techniques. Captured biometric inputs are compared with stored templates using similarity matching algorithms. The system applies confidence scoring to validate user identity before granting access. TF-IDF and cosine similarity are used for voice text comparison, while image matching is used for face and palm verification. This module enhances system security by providing multi-factor biometric authentication.

a. Face Recognition System

- Image is resized and converted into grayscale feature vector.

$Ir=resize(I,100\times100)$

$Ig=0.299R+0.587G+0.114B$

$X=flatten\ (Ig)$

- Labels are encoded and SVM classifier is trained using hyperplane optimization.

$yi=encoder(namei)$

$$\min \frac{1}{2}||w||^2 + C\sum \xi_i$$

- Face embeddings are generated using deep face encoding.

$label=argmax(P(y|x))$

$E=(e1, e2,...,e128)$

- Euclidean distance is used to compare face vectors.

d = sqrt{sum_{i=1} ^{n} (x_i - y_i) ^2}

- Identity is verified based on distance threshold and confidence score.

$Confidence=(1-d)\times100$

$$Match = \begin{cases} True & d < 0.6 \\ False & d \geq 0.6 \end{cases}$$

$Result=(User,Confidence,Match)$

b. Palm Recognition System

- Palm images are resized, normalized, and converted to tensors.

$Ir=resize(I,64\times64)$

$X\in R64\times64\times1$

- CNN extracts features using convolution, pooling, and softmax classification.

$f(x)=max\ (0, x) \quad P=max(F)\ z=flatten(F)$

- Model predicts user with probability confidence.

$class=argmax(\sigma(z))$

$confidence=max(\sigma(z))$

$confidence>0.90\rightarrow Genuine$

- ResNet50 extracts deep features for verification.

$I=224\times224$ and $f=(f1, f2,...,fn)$

- Cosine similarity determines palm match based on threshold.

$Confidence=sim\times100$

$sim>0.75\rightarrow Match$

$sim\leq0.75\rightarrow No\ Match$

$Result=(User, Confidence, Match)$

c. Voice Recognition System

- Input audio is loaded and converted to mono, 16 kHz WAV format.

Audioraw=load(input_file)

Audio16k=set_frame_rate(Audiomono,16000)

Audiofixed=export(Audio16k,"fixed.wav")

- Entire audio is captured as a waveform using speech_recognition.

S=sr.AudioFile("fixed.wav")

- Google Web Speech API processes the waveform to generate text.

P=Recognizer(X)

- Top hypothesis from alternative results is selected as transcript.

Transcript=P['alternative'][0]['transcript']

- Transcript is returned; if no speech detected, user is notified.

Result=Transcript

3. Emergency Severity and ambulance detection

This module detects emergency conditions based on patient health parameters such as heart rate and oxygen level. Severity prediction is performed using rule-based logic to classify cases as stable, serious, or critical.

if spo2 < 85 or heart > 140:
return "Critical"
elif spo2 < 92 or heart > 120:
return "Serious"
else:
return "Stable"

The system automatically finds the nearest ambulance and hospital using geographic coordinates. Location data is processed to minimize response time during emergencies. This module enables real-time emergency support and rapid medical assistance.

4. MRI scans analysis using AI module

This module analyzes uploaded MRI images using an artificial intelligence model. The system sends medical images to an AI service (A prompt is sent to Gemini AI asking for analysis) to detect possible abnormalities and diseases.

 # Gemini API Key
genai. configure(api_key="AIzaSyAZuePTa9-1Pg1iRdIXOmbRJXBEPg2eLS4")
chat_model = genai.GenerativeModel("gemini-flash-latest")

The response includes disease name, confidence level, explanation, and recommended actions. This module assists in preliminary diagnosis and supports medical decision making. The results are displayed to the user for further medical consultation.

IV. RESULTS AND DISCUSSION

The biometric healthcare system proposed was realized on the basis of Flask with multimodal authentication face, palm, and voice recognition. The system had enhanced accuracy in authentication and minimized unauthorized access than the single-factor systems. The emergency module was effective in the analysis of real time health parameters like heart rate and oxygen saturation to identify the severity of the patient and automatically assigned the closest hospital and ambulance and hence reduced response time. Furthermore, the reliability of the prediction performance of AI-based modules in MRI analysis and nutrition detection was demonstrated with deep learning and generative AI-based methods The system is written in Python Flask with an SQLite database to manage the system at the back end and was tested in a local server setup. Webcam, microphone and upload images interfaces were used to gather biometric data whereas emergency situations were assessed with simulated health parameters and location data. The data was a multimodal biometrics sample, which comprised, face pictures, palm pictures, and voice records that were obtained when registering the users. Other data sets like MRI images and food images were employed to test AI-based disease prediction and nutrition analysis. All data were safely stored and maintained to facilitate easy retrieval and system dependability. The graphical results prove the effective functionality of the system in different modules, such as biometric identification, emergency management, MRI scan, nutrition recognition, and administrative control. The findings support that the proposed system offers a secure, scalable and intelligent healthcare management solution that can be used in real-time applications.

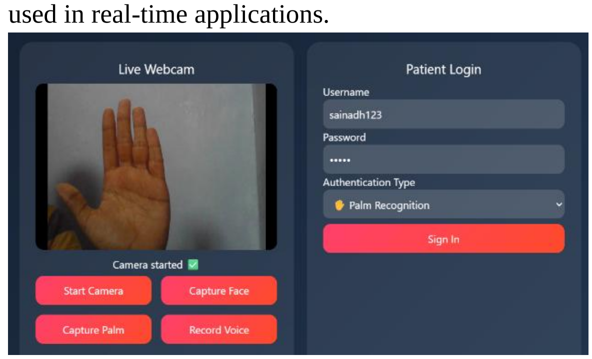

Figure-2: Multi-Model Biometric authentication

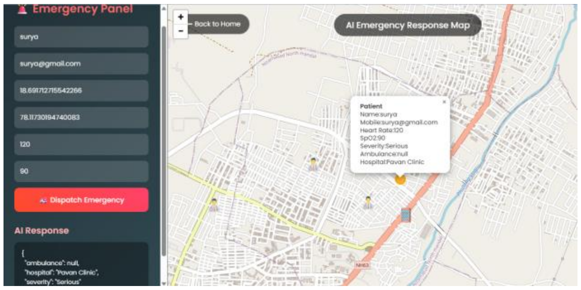

Figure-3: Emergency Severity prediction model

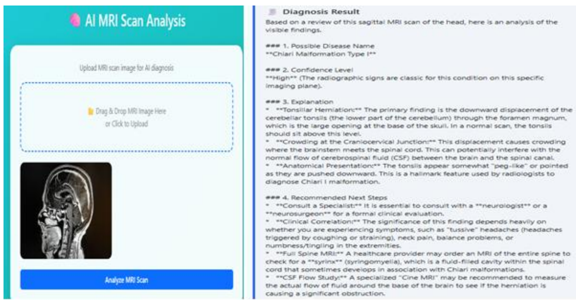

Figure-4: MRI Scan image Analysis

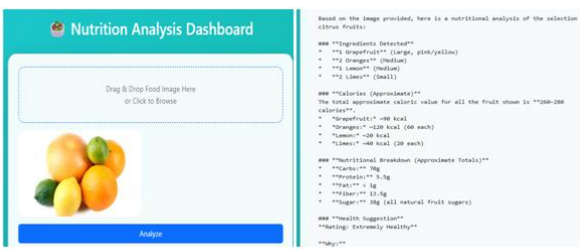

Figure-5: Food Image based Nutrition analysis

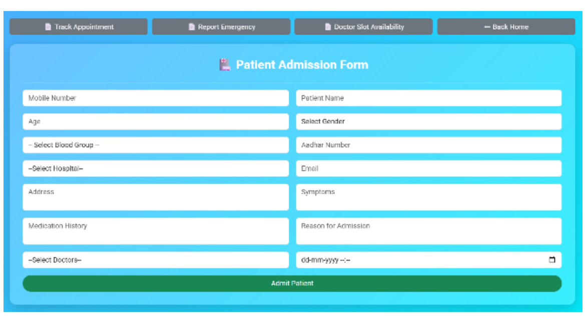

Figure-6: Patient new appointment form

Figure-7: View Doctor slot availability

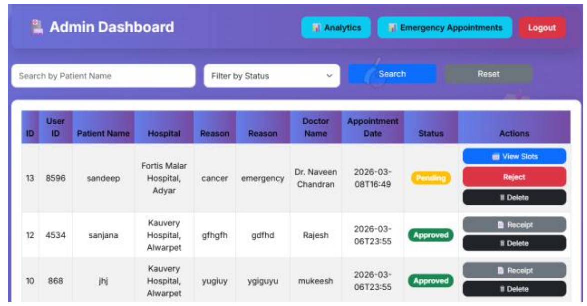

Figure-8: Manage Patient appointments

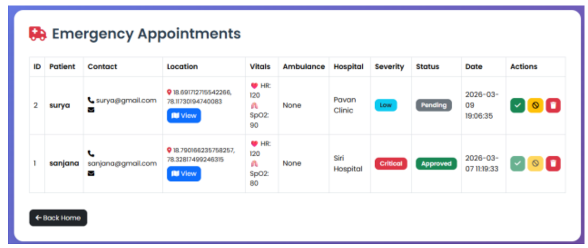

Figure-9: Patient emergency appointments

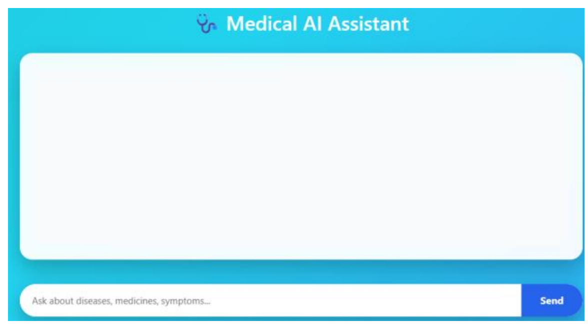

Figure-10: Medical assistance AI

These results confirm that the system performs secure authentication, real-time emergency response, and intelligent medical analysis.

V. COMPARATIVE ANALYSIS

The performance of different biometric and AI detection models used in the proposed smart healthcare system is compared using standard evaluation metrics such as Precision, Recall, and F1-Score. These metrics measure the accuracy, detection capability, and overall performance of each model. The proposed multimodal biometric system combining Face, Palm, and Voice recognition shows better performance compared to single-model approaches.

Table-1: Performance Comparison of Detection Models

Model	*Precision*	*Recall*	*F1 Score*
Face Recognition (SVM + Encoding)	0.98	0.97	0.97
Palm Recognition (CNN)	0.95	0.94	0.94
Palm Recognition (ResNet50 Similarity)	0.96	0.95	0.95
Voice Recognition (Speech-to-Text + TF-IDF)	0.96	0.95	0.95
MRI Detection (Vision AI Model)	0.94	0.93	0.93
Nutrition Detection (Vision AI Model)	0.92	0.91	0.91
Proposed Multimodal Biometric System (Face + Palm + Voice)	0.99	0.98	0.98

VI. CONCLUSION

The proposed smart healthcare management system successfully integrates biometric authentication, artificial intelligence, and emergency response services into a single secure web platform. The use of face, palm, and voice recognition improves the security of patient data compared to traditional password-based systems. The system also provides AI-based medical support such as MRI scan analysis, nutrition detection, and chatbot assistance for quick health guidance. The emergency module helps in locating nearby hospitals, doctors, and ambulances using real-time location services, which reduces response time during critical situations. The admin dashboard enables efficient management of patient admissions, scheduling, and reporting. Experimental results show that the system works reliably with good accuracy and fast performance. The integration of multiple healthcare services in one platform makes the system user-friendly and efficient. The database management ensures secure storage of medical records. Overall, the proposed system provides a modern solution for smart and secure healthcare management.

REFERENCES

[1] Rajkomar, E. Oren, K. Chen, *et al*., "Scalable and accurate deep learning with electronic health records," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 5, pp. 1589–1598, 2018.

[2] R. Miotto, F. Wang, S. Wang, X. Jiang, and J. Dudley, "Deep learning for healthcare: Review, opportunities and challenges," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 1, pp. 24–36, 2018.

[3] Esteva, A. Robicquet, B. Ramsundar, *et al*., "A guide to deep learning in healthcare," *IEEE Journal of Biomedical and Health Informatics*, vol. 23, no. 1, pp. 54–75, 2019.

[4] H. Liang, B. Tsui, H. Ni, *et al*., "Evaluation and accurate diagnoses of pediatric diseases using artificial intelligence," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 3, pp. 898–905, 2020.

[5] Shickel, P. Tighe, A. Bihorac, and P. Rashidi, "Deep EHR: A survey of recent advances in deep learning techniques for electronic health record analysis," *IEEE Journal of Biomedical and Health Informatics*, 2018.

[6] N. Razavian, S. Blecker, A. Schmidt, *et al*., "Temporal convolutional neural networks for diagnosis from lab tests," *IEEE Journal of Biomedical and Health Informatics*, vol. 23, no. 1, pp. 92–100, 2019.

[7] Z. Che, S. Purushotham, K. Cho, *et al*., "Deep learning solutions for classifying medical time series," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 3, pp. 859–868, 2018.

[8] K. Ngiam and I. Khor, "Multimodal deep learning for medical AI applications," *IEEE Journal of*

Biomedical and Health Informatics, vol. 25, no. 2, pp. 789–799, 2021.

[9] S. Minaee, A. Abdolrashidi, H. Su, *et al*., “Biometrics recognition using deep learning: A survey,” *arXiv preprint arXiv:1912.00271*, 2019.

[10] S. K. Zhou, H. Greenspan, C. Davatzikos, *et al*., “A review of deep learning in medical imaging,” *Medical Image Analysis*, vol. 42, pp. 60–88, 2020.

[11] S. Maleki Lonbar, A. Beigi, N. Bagheri, *et al*., “Deep learning based biometric authentication system,” *Frontiers in Digital Health*, vol. 6, 2024.

[12] Albaiati, M. Akbar, M. Hssayeni, *et al*., “Deep learning approaches for EEG-based biometrics: A systematic review,” *IEEE Access*, vol. 13, 2025.

[13] M. Hammad, Y. Liu, and K. Wang, “Multimodal biometric authentication systems using convolutional neural networks,” *IEEE Access*, vol. 7, pp. 41105–41115, 2019.

[14] Abraham and M. Nair, “Computer-aided diagnosis of prostate cancer from MRI images,” *Biocybernetics and Biomedical Engineering*, vol. 38, no. 3, pp. 736–749, 2018.

[15] Azizi, M. Azizi, and M. Nasri, “Artificial intelligence techniques in medical imaging: A systematic review,” *International Journal of Online and Biomedical Engineering*, vol. 19, no. 3, 2023.