A PRIVACY-PRESERVING REMOTE HEART RATE ABNORMALITY MONITORING SYSTEM

Simeen Ahmed[1], Dr. K. Palani[2]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, simeens6@gmail.com
[2]Professor & Head, Department of CSE, Shadan Women's College of Engineering and Technology, principalswcet2020@gmail.com

ABSTRACT:
Heart rate arrhythmias are a significant indication of many cardiovascular diseases, and they require real-time monitoring to enable timely intervention. However, older telemedicine systems often display heart rate data in unencrypted, putting patient privacy at risk. To address this, we propose a remote heart rate abnormality monitoring system based on deep convolutional neural networks (CNNs) for the detection of heart rate abnormalities. This system features an easy-to-use Flask UI interface for seamless interaction. Our approach uses a deep CNN to analyze heart rate data in the form of.wav files, offering an effective means of detecting anomalies. The Flask UI interface that goes along with it improves user experience by making it easy to monitor results. Throughout the monitoring procedure, users only view the final tally of abnormalities rather than the original heart rate data. This gadget can be used to remotely monitor heart rate abnormalities, which facilitates the early detection and treatment of cardiovascular issues. Our test results indicate the computational efficiency and feasibility of our technique, ensuring a seamless and effective experience for both users and healthcare professionals.

1. INTRODUCTION

The emergence and spread of the COVID-19 pandemic have brought attention to how crucial telemedicine is to contemporary healthcare. Since the virus is contagious and medical resources are scarce, in-person consultations between patients and physicians are not feasible, which delays the timely treatment of many underlying illnesses. Telemedicine offers a revolutionary means to overcome time and location constraints, lowers the possibility of doctor-patient cross-infection during epidemics, allows for quick diagnosis and treatment of patients in need, and presents a novel approach to treating patients with underlying illnesses. Medical professionals frequently use physiological indications to assess their patients' health, and heart rate is one important physiological indicator that might reveal a person's current state of health. The average person's heart rate falls within a certain range.

Cardiovascular disease is the most serious of the potential health issues that might result from an abnormal heart rate, along with stroke, heart failure, and other conditions. According to the World Health Organization, the mortality rate from cardiovascular disease is still high and is becoming more prevalent in younger people. It poses a serious risk to human life and health and places a heavy financial strain on families and society. Real-time heart rate monitoring is crucial for both working people and the elderly since cardiovascular illness is sneaky, abrupt, and changing quickly, making it difficult for patients to obtain therapy in a timely manner.

In order to provide real-time monitoring for telemedicine, wearable technology is essential. Wearable technology enables telemedicine systems to monitor patients' heart rates in real time, identify aberrant heart rates in time for an early diagnosis, or take preventative action beforehand. However, the limited computer power and storage capacity of smart wearables can limit their usefulness and performance. In order to save power and boost efficiency, some plans have suggested transferring patient data to a cloud server. However, there may be serious security hazards to patient data privacy if cloud servers—an unreliable entity—are used to analyze heart rate data.

2. OBJECTIVE

Several important factors are included in the goal of incorporating a Convolutional Neural Network (CNN) into a Remote Heart Rate Abnormality Monitoring System that Preserves Privacy. First, the CNN must precisely identify irregularities in heart rate from remote physiological signals, including electrocardiogram (ECG) or photoplethysmogram (PPG) data gathered via sensors or wearable technology. A crucial early warning system for possible cardiovascular problems is this detection capability. Second, it is critical to protect the privacy of consumers' health information. Through the use of a CNN architecture in conjunction with federated learning or homomorphic encryption, the system can process data locally on users' devices or in an encrypted manner, protecting private health information from unwanted access" Furthermore, by quickly evaluating physiological signals and sending out alerts or notifications for any anomalies found, the CNN enables real-time monitoring. The CNN model is trained using a variety of datasets that represent various demographics, medical problems, and environmental factors in order to attain adaptability and generalization across numerous populations and circumstances. Another goal is seamless

wearable integration, which calls for the CNN model to be optimized for deployment on devices with limited resources without sacrificing accuracy or efficiency.

3. PROBLEM STATEMENT

Heart rate arrhythmias are a key symptom of a number of cardiovascular conditions, and they must be continuously and continuously monitored in order to facilitate early identification and prompt treatment. Although beneficial, traditional telemedicine systems frequently provide heart rate data in an unencrypted format, jeopardizing patient privacy and data security. The need for a more accurate, safe, and effective heart rate monitoring device is highlighted by this problem. In order to discover anomalies, the suggested method analyzes heart rate data from.wav files using deep convolutional neural networks (CNNs). Moreover, a Flask-based user interface improves usability and accessibility for patients and medical professionals. The technology guarantees data confidentiality and privacy by sharing only the final results, which include information about any irregularities found. In order to improve early intervention and treatment while addressing important privacy concerns, this strategy seeks to offer an efficient, real-time monitoring tool for the detection of cardiovascular disorders.

4. EXISTING SYSTEM

In the era of "Big Data," the healthcare sector is increasingly integrating machine learning (ML). Machine learning techniques have become increasingly popular and have shown remarkable results in the medical field, particularly in the area of diagnostic prediction. The field of medical imaging, where reports are generated by machine learning algorithms, also exhibits this tendency. An example of a well-known algorithm that is currently in use is the Collaborative Mining System. Using collective intelligence, this sophisticated technique automatically makes recommendations or forecasts user interests. This method creates a collaborative mining network (CMN) by gathering taste data from multiple users. Medical practitioners can use the CMN to evaluate large datasets and identify trends and patterns that aid in their decision-making.

Disadvantage of Existing System

- More computational complexity, which could result in bigger resource needs and slower processing times.
- Distribution, storage, and revocation of keys can be problematic, particularly in a healthcare context where user engagement is dynamic.
- It is less flexible when datasets or the number of persons participating rise, which affects the system's overall effectiveness.

5. PROPOSED SYSTEM

The suggested method uses a deep convolutional neural network (CNN) to identify heart rate abnormalities in real-time, addressing a crucial symptom of many cardiovascular diseases. Since typical telemedicine systems sometimes present heart rate data in an unencrypted format, patient privacy is at risk. Our approach uses heart rate data from.wav files and applies a deep CNN for efficient analysis and anomaly detection in order to counteract this. The accompanying Flask UI interface ensures a seamless user experience and allows users and healthcare professionals to obtain the monitoring findings without revealing the original heart rate data. Through remote monitoring of heart rate anomalies, our approach facilitates early diagnosis and management, improving the timely treatment of cardiovascular diseases. Because users only see the final number of anomalies and not the raw heart rate data, this innovative system prioritizes computing performance while protecting patient privacy. The testing findings confirm the system's viability, guaranteeing a smooth and efficient experience for both patients and medical personnel. All things considered, the proposed approach offers a reliable way to remotely monitor abnormal heart rhythms, which enables early cardiovascular problem detection and treatment.

Advantages of Proposed System

- Benefits include the ability to accurately detect minor patterns suggestive of arrhythmias by automatically identifying pertinent elements from complex heart rate data.
- Skilled in examining the temporal correlations in heart rate signals, which enables the identification of anomalies that might appear over time.
- Abnormalities in heart rate are monitored in real time, allowing for timely intervention.

6. RELATED WORKS

Many researches have been conducted for automatically predicting cardiovascular diseases using machine learning and deep learning methods by utilizing ECG as digitals or images data representation. Reference has compared machine learning and deep learning methods on UCI heart disease dataset to predict two classes. Deep learning method achieved the highest accuracy rate of 94.2%. In their architecture of deep learning model, they used three fully connected layers: the first layer consists of 128 neurons followed by a dropout layer with 0.2 rate, the second layer consists of 64 neurons followed by a dropout layer with 0.1 rate, and the third layer consists of 32 neurons. While the machine learning methods with features selection and outliers' detection achieved accuracy rates as: RF is 80.3%, LR is83.31%, K-NN is 84.86%, SVM is 83.29%, DT is 82.33%, and XGBoost is 71.4%. The research in concluded that deep Personal use is permitted, but republication/redistribution requires

IEEE permission. See This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: Transactions on Artificial Intelligence learning has proven to be a more accurate and effective technology for a variety of medical problems such as prediction. And, deep learning methods will replace the traditional machine learning based on feature engineering. Kiranyaz et al. proposed a CNN that consisted of three layers of an adaptive implementation of 1D convolution layers. This network was trained on the MIT-BIH arrhythmia dataset to classify long ECG data stream. They achieved accuracy rates of 99% and 97.6% in classifying ventricular ectopic beats and supraventricular ectopic beats respectively. Also, the work in proposed a CNN that consisted of three 1D convolution layers, three max pooling layers and one fully connected layer and one softmax layer. The filter size for first and second convolutional layer was set to 5 and a stride of 2 was used the first two max pooling layers. They achieved an accuracy rate of 92.7% in classifying ECG heart beats using MIT-BIH arrhythmia dataset

7. METHODOLOGY OF PROJECT

Integrating deep CNN-based heart rate abnormality detection with secure Flask UI functionality, this system provides a powerful tool for remote cardiovascular monitoring. It enables real-time detection of heart rate abnormalities, facilitates early diagnosis, and ensures the privacy and security of patient data.

MODULE DESCRIPTION:

1. Dataset:

In the first module, we developed the system to get the input dataset for the training and testing purpose. We have taken the dataset for Arrhythmia detection. The dataset consists of 800 wave files including Arrhythmia and normal.

2. Importing the necessary libraries:

Python will be the language we use for this. The required libraries, including Librosa, Numpy, sklearn, and keras for creating the primary model and dividing the training and test data into arrays, will be imported first. The building blocks required to develop wave files, information retrieval systems, and additional libraries like tkinter, PIL, matplotlib, OS, and streamlit are provided.

3. Information retrieval:

We'll obtain the wave files along with their labels. The waves dataset should then be resized to the default train size because all wave files need to be the same size in order to be detected. Librosa offers the building blocks required to construct information retrieval systems for wave files and then translate the information retrieved from wave files into NumPy arrays.

4. Dataset Splitting:

Divide the dataset into test and train sets. 20% is test data and 80% is train data.

5. Training algorithm:

The convolution neural network uses gradient descent as its backward propagation training strategy. The discrepancies between the output vector and the predicted output vector, or the loss function, are used to estimate the network hyperparameters. Hyperparameters consist of the convolution layer's convolution kernel parameter W, the pooling layer's sampling weight coefficient α, the fully-connected layer's network weight w, and each layer's offset b. There are two stages to training a convolution neural network: forward propagation and reverse propagation. During the forward propagation stage, the neural network receives the training data and computes the middle and output layer output vectors. The output vectors of the output layer are compared to the expected output vectors in the reverse propagation step, and the loss function in relation to the network weights is computed. To update the weights for each neuron in each layer, the gradient descent algorithm is used to transmit the loss back to the beginning layers (in reverse direction). Unlike the forward computation, gradient descent consists of two steps: first, the gradients of the loss function are calculated using chain rules; second, weight is updated in the opposite or reverse direction of the gradient of the loss function. Additionally, a cost function is computed for each hidden layer's neuron output in order to constantly tune the network's hyperparameters. When the set error is reached after several iterations, the network stops training.

6. Model construction:

We'll utilize the sequential model from the Keras library for construction. The layers that make up our neural network will then be added. The kernel size is (2, 2), and we have employed 16 filters in the first 1 Conv2D layers. The MaxPool2D layer will choose the maximum value of each 2 x 2 section of the wave files because we have maintained the pool size at (2, 2). By doing this, the wave files' values will decrease by a factor of two. We have set the dropout rate in the dropout layer to 0.25, which indicates that 25% of neurons are eliminated at random. With a few parameter changes, we apply these three layers once more. After that, we use the flatten layer to transform 2-D data into 1-D vectors. A dense layer, a dropout layer, and another dense layer come after this one. Two nodes are produced by the final dense layer as the arrhythmia detecting system. The softmax activation function, which provides a probability value, is used in this layer to determine which of the two possibilities has the highest likelihood.

7. Model application and plot accuracy :

The model will be assembled and applied using the fit function. The size of the batch will be 128. Our average

training and validation accuracy were 98.7% and 87.6%, respectively.

8. Accuracy on test set:

On the test set, our accuracy was 98.3%.

9. Preserving the Trained Model:

Using a library like save or pickle, save your trained and tested model into a.h5 or pkl file as soon as you're comfortable enough to move it into a production-ready setting. Make sure your environment has save/pickle installed. The module will then be imported, and the model will be dumped into a.h5 or. pkl file.

DATA FLOW DIAGRAM

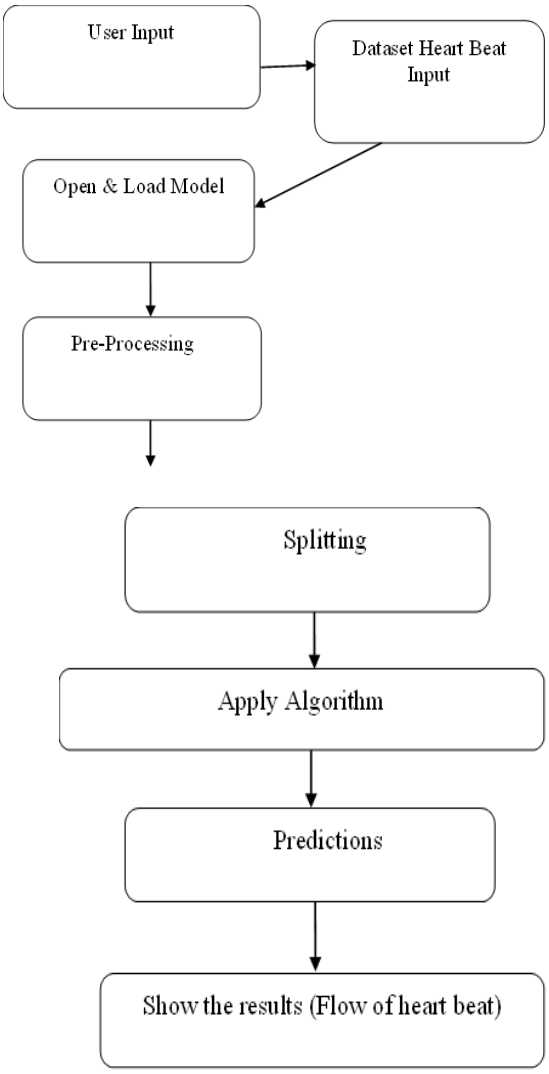

Fig: 7 Flow Diagram

ALGORITHM USED IN PROJECT

The suggested method uses a deep convolutional neural network (CNN) to identify heart rate abnormalities in real-time, addressing a crucial symptom of many cardiovascular diseases. Since typical telemedicine systems sometimes present heart rate data in an unencrypted format, patient privacy is at risk. Our approach uses heart rate data from.wav files and applies a deep CNN for efficient analysis and anomaly detection in order to counteract this.

SYSTEM ARCHITECTURE

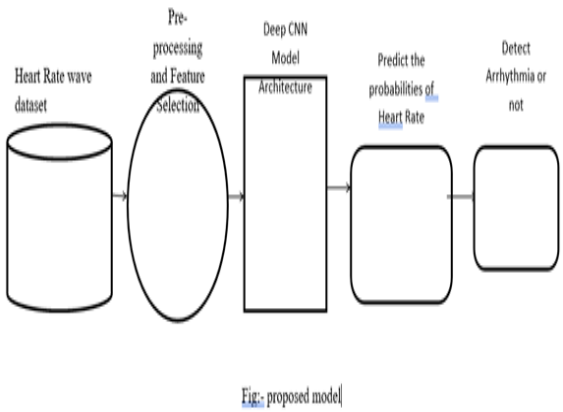

Fig: 8 SYSTEM ARCHITECTURE OF PROJECT

RESULTS

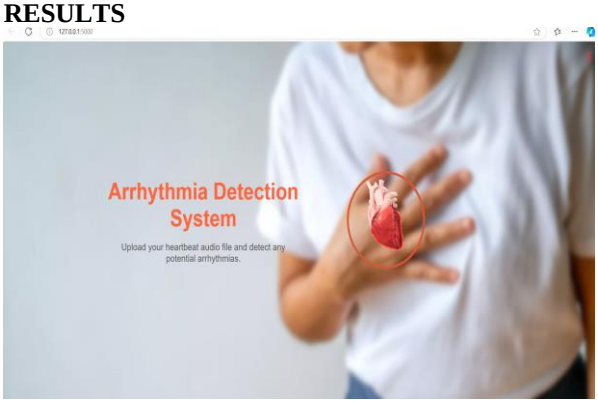

Fig. 7.1 Home page

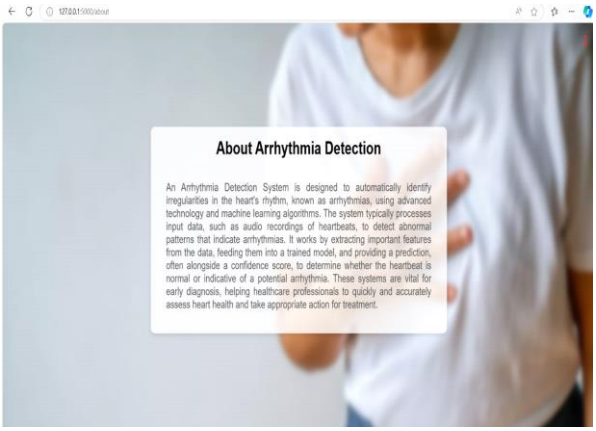

Fig. 7.2 About page

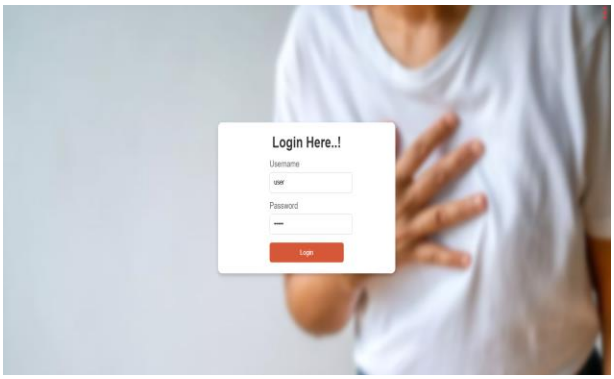

Fig. 7.3 Login page

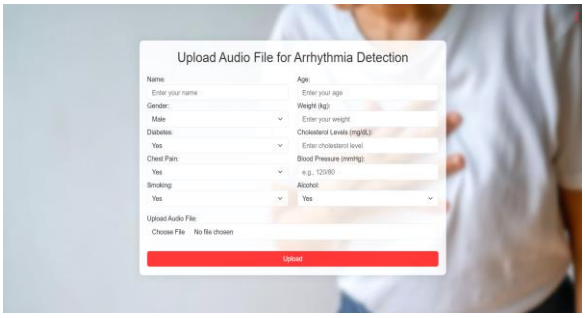

Fig 7.4 Uploading Data and Audio Files Page

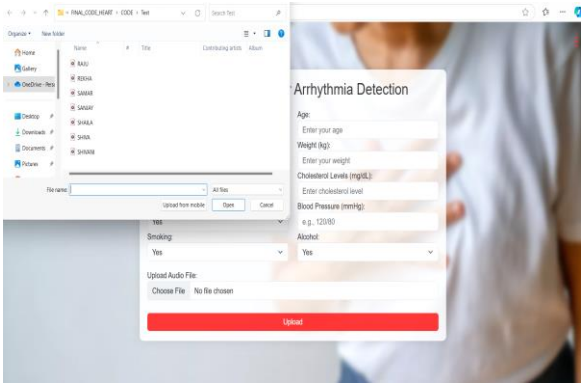

Fig. 7.5 Pretrained Audio Files of Patients

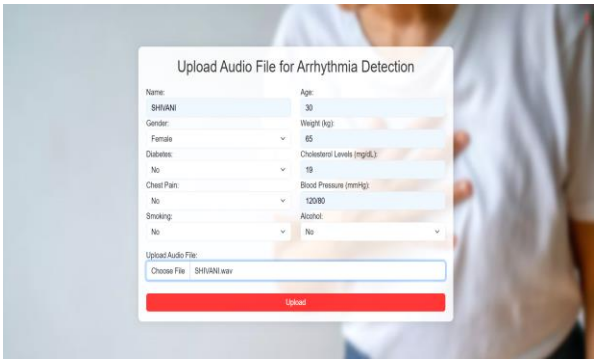

Fig. 7.6 Uploading Patient 1 Detail Record

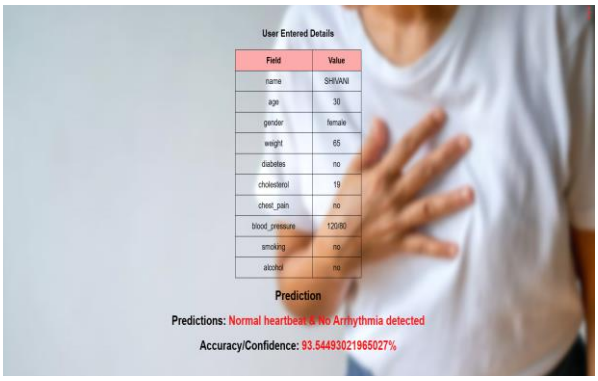

Fig. 7.7 Heartrate Prediction and Confidence Score for Patient 1

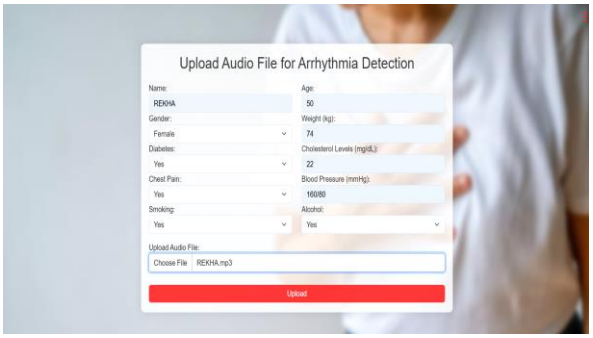

Fig. 7.8 Uploading Patient 2 Detail Record

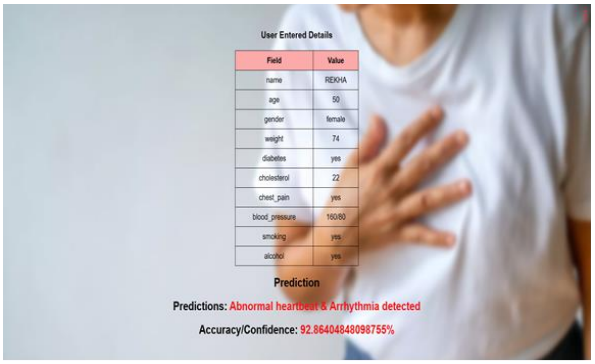

Fig. 7.9 Heartrate Prediction and Confidence Score for Patient 2

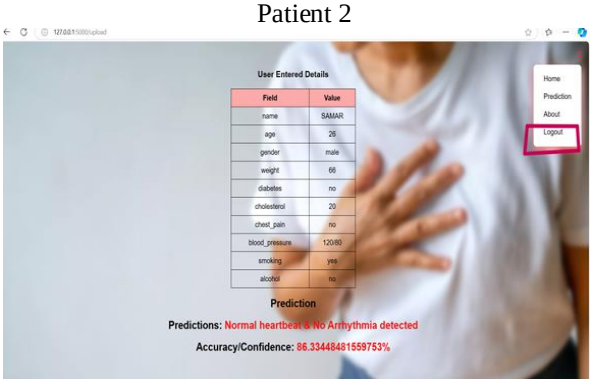

Fig. 7.10 Logout Page

FUTURE ENHANCEMENT

The privacy-preserving strategy for remote heart rate abnormality monitoring can be improved by concentrating on making it more user-friendly, flexible, and quick. Simplifying the encryption procedures would accelerate the system, but it's crucial to make sure it can support additional users without experiencing any performance issues. Using wearable technology to share data in real time can give a more complete picture of a user's health. Furthermore, heart rate data will be more accurate and valuable if it is combined with other health metrics and the monitoring procedure is customized. " Adapting anomaly detection criteria dynamically according to each person's health profile can increase efficacy even more. The creation of an intuitive user interface for both patients and doctors, together with compatibility with current healthcare systems, will promote uptake and participation. Last but not least, constant assessment and improvement of the system will keep it efficient and current with changing requirements.

CONCLUSION

Finally, in order to protect patients' private health information and facilitate efficient medical intervention, we have implemented a strong privacy-preserving plan for remote heart rate abnormality monitoring. The security of heart rate data, patients' healthy heart rate range, and monitoring outcomes are guaranteed by our technique, which uses Paillier homomorphic encryption. Physicians can give individualized advise without jeopardizing patient privacy because the system merely indicates whether the heart rate data is normal or bad, not specific values. Additionally, the privacy comparison protocol and our dual cloud server-assisted computing model improve the security of the monitoring process by prohibiting separate servers from independently deriving results. Our scheme's efficacy is validated experimentally, and a comprehensive security analysis shows that it can meet strict security goals. All things considered, the framework we have suggested for remote heart rate abnormality monitoring is strong, strikes a balance between privacy protection and precise medical insights, and has the potential to be implemented in healthcare settings.

REFERENCES:

[1] J. Huang, S. Lin, N. Wang, G. Dai, Y. Xie, and J. Zhou, ‘‘TSE-CNN:A two-stage end-to-end CNN for human activity recognition,’’ IEEE J.Biomed. Health Informat., vol. 24, no. 1, pp. 292–299, Jan. 2020, doi:10.1109/JBHI.2019.2909688.

[2] J. Liang, Z. Qin, S. Xiao, J. Zhang, H. Yin, and K. Li, ‘‘Privacy-preserving range query over multi-source electronic health records in public clouds,’’ J. Parallel Distrib. Comput., vol. 135, pp. 127–139, Jan. 2020.

[3] M. Pettai and P. Laud, ‘‘Combining differential privacy and secure multiparty computation,’’ in Proc. 31st Annu. Comput. Secur. Appl. Conf., Dec. 2015, pp. 17–19, doi: 10.1145/2818000.2818027.

[4] Y. Zhou, Y. Tian, F. Liu, J. Liu, and Y. Zhu, ‘‘Privacy preserving distributed data mining based on secure multi-party computation,’’ in Proc. IEEE 11thInt. Conf. Adv. Infocomm Technol. (ICAIT), Oct. 2019, pp. 173–178, doi:10.1109/ICAIT.2019.8935900.

[5] M. Tebaa, S. E. Hajji, and A. E. Ghazi, ‘‘Homomorphic encryption applied to the cloud computing security,’’ in Proc. World Congr. Eng., vol. 1, no. 1.London, U.K., 2012, pp. 4–6.

[6] S. J. Mohammed and D. B. Taha, ‘‘Performance evaluation of RSA,ElGamal, and Paillier partial homomorphic encryption algorithms,’’ inProc. Int. Conf. Comput. Sci. Softw. Eng. (CSASE), Mar. 2022, pp. 89–94,doi: 10.1109/CSASE51777.2022.9759825.

[7] Z. H. Mahmood and M. K. Ibrahem, ‘‘New fully homomorphic encryption scheme based on multistage partial homomorphic encryption appliedin cloud computing,’’ in Proc. 1st Annu. Int. Conf. Inf. Sci. (AiCIS),Nov. 2018, pp. 182–186, doi:10.1109/AiCIS.2018.00043.

[8] N. Dawar and N. Kehtarnavaz, ‘‘A convolutional neural network-based sensor fusion system for monitoring transition movements in healthcare applications,’’ in Proc. IEEE 14th Int. Conf. Control Autom. (ICCA),Jun. 2018, pp. 482–485, doi: 10.1109/ICCA.2018.8444326.

[9] J. Liu, J. Yang, L. Xiong, and J. Pei, ‘‘Secure skyline queries on cloud platform,’’ in Proc. IEEE 33rd Int. Conf. Data Eng. (ICDE), Apr. 2017, pp. 633–644, doi: 10.1109/ICDE.2017.117.

[10] S. Zhang, S. Ray, R. Lu, Y. Zheng, Y. Guan, and J. Shao, ‘‘Towards efficient and privacy-preserving user-defined skyline query over single cloud,’’ IEEE Trans. Depend. Secure Comput., vol. 20, no. 2, pp. 1319–1334,Mar. 2023, doi: 10.1109/TDSC.2022.3153790.

[11] S. Zhang, S. Ray, R. Lu, and Y. Guan, ‘‘PPsky: Privacy-preserving skyline queries with secret sharing in eHealthcare,’’ in Proc. GLOBECOM IEEE Global Commun. Conf., Dec. 2022, pp. 5469–5474, doi: 10.1109/GLOBE-COM48099.2022.10000905.

[12] S. Paliwal, C. V. Lakshmi, and C. Patvardhan, ‘‘Real time heart rate detection and heart rate variability calculation,’’ in Proc. IEEE Region10 Humanitarian Technol. Conf. (R-HTC), Dec. 2016, pp. 1–4, doi:10.1109/R10-HTC.2016.7906818.

[13] H.-Y. Kwon and M.-K. Lee, ‘‘Comments on ‘PassBio: Privacy-preserving user-centric biometric authentication,’’’ IEEE Trans. Inf. Forensics Security,

vol. 17, pp. 2816–2817, 2022, doi: 10.1109/TIFS.2022.3195380.
[14] Y. Liu, Y. Yang, Z. Ma, X. Liu, Z. Wang, and S. Ma, ‘‘PE-HEALTH: Enabling fully encrypted CNN for health monitor with optimized communication,’’ in Proc. IEEE/ACM 28th Int. Symp. Quality Service (IWQoS), Jun. 2020, pp. 1–10, doi: 10.1109/IWQoS49365.2020.9212822.
[15] J. Hua, H. Zhu, F. Wang, X. Liu, R. Lu, H. Li, and Y. Zhang, ‘‘CINEMA:Efficient and privacy-preserving online medical primary diagnosis withskyline query,’’ IEEE Internet Things J., vol. 6, no. 2, pp. 1450–1461,Apr. 2019, doi: 10.1109/JIOT.2018.2834156.
[16] A. Alnemari, R. K. Raj, C. J. Romanowski, and S. Mishra, ‘‘Interactiverange queries for healthcare data under differential privacy,’’ in Proc. IEEE9th Int. Conf. Healthcare Informat. (ICHI), Aug. 2021, pp. 228–237, doi:10.1109/ICHI52183.2021.00044.
[17] M. Nassar, A. Erradi, and Q. M. Malluhi, ‘‘Paillier’s encryption:Implementation and cloud applications,’’ in Proc. Int. Conf. Appl. Res.Comput. Sci. Eng., 2015, pp. 1–5, doi: 10.1109/ARCSE.2015.7338149.
[18] M. Zheng, Y. Cui, and L. Chen, ‘‘Security analysis of a Paillier-based threshold proxy signature scheme,’’ in Proc.12th IEEE Int. Conf.Trust, Secur. Privacy Comput. Commun., Jul. 2013, pp. 683–687, doi:10.1109/TrustCom.2013.83.
[19] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, ‘‘PEC: A privacy-preserving emergency call scheme for mobile healthcare social networks,’’J. Commun. Netw., vol. 13, no. 2, pp. 102–112, Apr. 2011, doi:10.1109/JCN.2011.6157409.
[20] R. Lu, ‘‘A new communication-efficient privacy-preserving range queryscheme in fog-enhanced IoT,’’ IEEE Internet Things J., vol. 6, no. 2,pp. 2497–2505, Apr. 2019, doi: 10.1109/JIOT.2018.2871204.
[21] A. Rasheed, E. Iranmanesh, W. Li, H. Ou, A. S. Andrenko, and K. Wang,‘‘A wearable autonomous heart rate sensor based on piezoelectric-charge-gated thin-film transistor for continuous multi-point monitoring,’’ in Proc39th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), Jul. 2017,pp. 3281–3284, doi: 10.1109/EMBC.2017.8037557.
[22] R. Lu, X. Lin, and X. Shen, ‘‘SPOC: A secure and privacy-preservingopportunistic computing framework for mobile-healthcare emergency,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 3, pp. 614–624, Mar. 2013,doi: 10.1109/TPDS.2012.146.
[23] P. Li, C. Xu, H. Xu, L. Dong, and R. Wang, ‘‘Research on data privacy protection algorithm with homomorphism mechanism based on redundantslice technology in wireless sensor networks,’’ Chin Commun., vol. 16,no. 5, pp. 158–170, May 2019, doi: 10.23919/j.cc.2019.05.012.
[24] S. Panda, A. Mukherjee, R. Halder, and S. Mondal, ‘‘Blockchain-enabled emergency detection and response in mobile healthcare system,’’ in Proc.IEEE Int. Conf. Blockchain Cryptocurrency (ICBC), May 2022, pp. 1–5,doi: 10.1109/ICBC54727.2022.9805544.
[25] M. Yang, J. Guo, and L. Bai, ‘‘A data privacy-preserving method forstudents’ physical health monitoring by using smart wearable devices,’’in Proc. IEEE Int. Conf Depend., Autonomic Secure Comput., Int. Conf.Pervasive Intel. Compute., Int. Conf Cloud Big Data Compute., Int. ConfCyber Sci. Technol.Congr.(DASC/PiCom/CBDCom/CyberSciTech),Aug. 2020, pp. 29–34, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00021.
[26] A. V. Sokolova and T. I. Buldakova, ‘‘Network architecture of telemedicinesystem for monitoring the Person’s condition,’’ in Proc. 3rd Int. Conf.Control Syst., Math. Modeling, Autom. Energy Efficiency (SUMMA),Nov. 2021, pp. 361–365, doi: 10.1109/SUMMA53307.2021.9632199.
[27] T. Li, Y. Liu, N. N. Xiong, A. Liu, Z. Cai, and H. Song, ‘‘Privacy-preservingprotocol for sink node location in telemedicine networks,’’ IEEE Access,vol. 6, pp. 42886–42903, 2018, doi: 10.1109/ACCESS.2018.2858274.
[28] G. A. Macriga, S. R. L. Siddarth, and P. Sivadinesh, ‘‘Monitoring realtime data and secure retrieval for telemedicine systems,’’ in Proc. Int.Conf. Smart Syst. Inventive Technol. (ICSSIT), Nov. 2019, pp. 552–556,doi: 10.1109/ICSSIT46314.2019.8987813.
[29] S. S. Sahoo and S. Mohanty, ‘‘Cloud-assisted privacy preserving authen-tication scheme for telecare medical information systems,’’ in Proc. IEEE
Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS), Dec. 2018, pp. 1–6, doi:10.1109/ANTS.2018.8710128.
[30] M. Bian, G. He, G. Feng, X. Zhang, and Y. Ren, ‘‘Verifiable privacy-preserving heart rate estimation based on LSTM,’’ IEEE Internet ThingsJ., early access, Jun. 29, 2023, doi: 10.1109/JIOT.2023.3290651.
[31] S. Hochreiter and J. Schmidhuber, ‘‘Long short-term memory,’’ NeuralComput., vol. 9, no. 8, pp. 1735–1780, Nov. 1997.
[32] K. Kalyan, V. K. Chugh, and C. S. Anoop,‘‘Non-invasive heart ratemonitoring system using giant magneto resistancesensor,’’ in Proc.38th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), Aug. 2016,pp. 4873–4876, doi: 10.1109/EMBC.2016.7591819.
[33] D. Zhu, H. Zhu, C. Huang, R. Lu, D. Feng, and X. Shen, ‘‘Efficient andaccurate cloud-assisted medical pre-diagnosis with privacy preservation,’’IEEE Trans. Depend. Secure Comput., early access, Apr. 3, 2023, doi:10.1109/TDSC.2023.3263974.
[34] M. Zalloum and H. Alamleh, ‘‘Privacy preserving architecture forhealthcare information systems,’’ in Proc. IEEE Int. Conf. Commun.,Netw. Satell. (Comnetsat), Dec. 2020, pp. 429–432, doi: 10.1109/Comnet-sat50391.2020.9328985.

[35] W. Wang, Y. Jin, and B. Cao, ‘‘An efficient and privacy-preserving range query over encrypted cloud data,’’ in Proc. 19th Annu. Int. Conf.Privacy, Secur. Trust (PST), Aug. 2022, pp. 1–10, doi: 10.1109/PST55820.2022.9851989.Informatics, Vol. 57, 101085, 2020, https://doi.org/10.1016/j.ecoinf.2020.101085.