IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 4, August 2026, pp. 3309~3317
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i4.pp3309-3317

AI-driven hybrid neural network for electrocardiogram-based authentication and predictive health monitoring

Swati Lakshmi Boppana[1], Velicheti Anantha Lakshmi[2], Padala SriKavitha[3], Venkata Ashok Kalaga[4], Venkateswara Rao Naramala[5], Suneetha Thalluru[6], Gunturi S. Raghavendra[7]
[1]Department of Electronics and Communication Engineering, Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, India
[2]Department of Computer Science and Engineering (AI and ML), Pragati Engineering College, Surampalem, India
[3]Department of Electrical and Electronics Engineering, Aditya University, Surampalem, India
[4]Department of Electronics and Communication Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, India
[5]Department of Computer Science and Engineering, R.V.R. and J.C. College of Engineering, Chowdavaram, Guntur, India
[6]Department of Electronics and Communication Engineering, R.V.R. and J.C. College of Engineering, Guntur, India
[7]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India

Article Info

Article history:

Received Apr 20, 2025
Revised May 21, 2026
Accepted Jun 19, 2026

Keywords:

Artificial intelligence
Biometric security
Convolutional neural network
Healthcare data security
Hybrid deep learning
Predictive health monitoring

ABSTRACT

The increasing adoption of digital healthcare systems demands secure and reliable patient authentication mechanisms. Traditional methods such as passwords and PINs are vulnerable to security breaches, motivating the use of biometric-based solutions. Among various biometrics, the electrocardiogram (ECG) signal is distinctive, stable, and non-invasive, making it suitable for secure authentication. This paper proposes CardioGuard, an artificial intelligence (AI)–based authentication framework that employs a hybrid deep learning model combining convolutional neural networks (CNNs) and long short-term memory (LSTM) networks to extract discriminative features from ECG signals and classify users as genuine or impostors. In addition to access control, the system analyzes ECG patterns to support early detection of potential cardiovascular abnormalities. Experimental results demonstrate that CardioGuard achieves improved authentication accuracy and enhanced predictive health insights compared to conventional approaches, highlighting its effectiveness for secure and intelligent healthcare monitoring.

Corresponding Author:

Velicheti Anantha Lakshmi
Department of Computer Science and Engineering (AI and ML), Pragati Engineering College
Surampalem, Kakinada, Andhra Pradesh, India
Email: ananthalakshmi.v@pragati.ac.in

1. INTRODUCTION

Digital healthcare systems have gained significant popularity in recent years, enabling individuals to access remote healthcare services across a wide range of scenarios. However, the deployment of such systems introduces serious security challenges related to the privacy and confidentiality of patient information. In this context, electrocardiogram (ECG) signals have emerged as a promising biometric approach for authentication in digital healthcare systems [1]. ECG data effectively capture the electrical activity of the heart, making them a reliable and distinctive source for personal identification. The incorporation of ECG biometrics in digital healthcare platforms considerably enhances data security and privacy by ensuring that access to sensitive medical information is restricted to authorized users only. Despite these advantages, challenges such as standardization, interoperability, and user acceptance arise during the practical implementation of ECG-based biometric systems. Biometric technologies are increasingly recognized as effective countermeasures against the rising threats of identity theft, terrorist activities, and cybercrime [2]. The global biometric market exceeded USD 20 billion in 2020 and is projected to grow at a rate exceeding 13% compound annual growth rate (CAGR) from 2021 to 2027, underscoring the growing importance of security in modern society. Various biometric recognition techniques exist, including facial recognition, fingerprint analysis, iris recognition, and retina recognition. Among these, ECG-based biometrics stand out as highly reliable due to their universal presence, immutable characteristics, measurable properties, widespread acceptance, and strong capability for unique identification. ECGs offer enhanced confidentiality and security compared to other biometric modalities [3], [4]. Recent studies reveal that ECG signals consist of five sequential waves (P, Q, R, S, and T), which are unique to each individual, as shown in Figure 1. This also confirms the physical presence of the subject, a feature not supported by several other biometric techniques. The generation of ECG signals is inherently complex, as it reflects the autonomous functioning of a vital organ, making signal analysis a challenging task [5], [6].

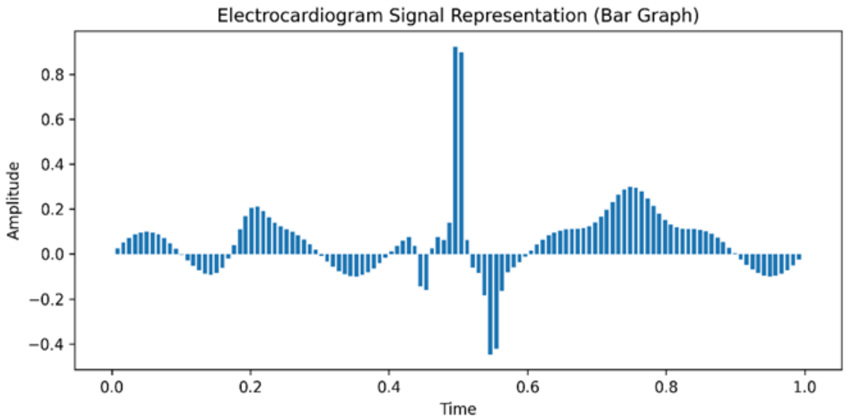


Figure 1. ECG signal representation for biometric authentication analysis

The adoption of artificial intelligence (AI) has greatly improved the security of digital healthcare environments through dependable ECG-based biometric authentication systems. Numerous machine learning (ML) techniques have been employed to evaluate authentication performance, with widely adopted methods including k-nearest neighbor (KNN), support vector machine (SVM), and random forest (RF). In recent years, deep learning methodologies have attracted considerable attention for biometric authentication applications, particularly those utilizing ECG signals [7]–[11]. Deep neural network models exhibit significant capability in authenticating ECG data by extracting complex features from large-scale datasets and accurately distinguishing authentic signals from manipulated or unauthorized ones [12]–[14]. This research highlights several important gaps that still require detailed investigation, including the enhancement of ECG biometrics using advanced deep learning architectures and optimized datasets, improvement of authentication speed and computational efficiency, incorporation of biometric fusion techniques to achieve higher accuracy, and effective differentiation between normal and abnormal ECG patterns during authentication procedures. The proposed study addresses the increasing demand for secure and dependable authentication solutions caused by the rapid expansion of digital technologies and growing concerns regarding information security. Compared with traditional authentication approaches, ECG signals provide two major advantages: enhanced protection through biometric verification and the capability to support early identification of cardiovascular abnormalities, which aligns with the application of AI in predictive healthcare systems. The proposed CardioGuard framework evaluates ECG signals to authenticate individuals and detect anomalies associated with potential cardiac risks, thereby promoting proactive and preventive healthcare management strategies.

The proposed architecture is designed to address inter-subject variability in ECG signals by learning hierarchical representations that capture discriminative and informative features. This study demonstrates the effectiveness of CardioGuard as a reliable ECG-based authentication framework, offering improved accuracy, robustness, and suitability for practical applications through detailed analysis and comparative evaluation. The major contributions include a novel automated authentication framework that jointly exploits spatial and temporal ECG characteristics to enhance protection against spoofing and unauthorized access, a hybrid deep learning model integrating convolutional neural networks (CNNs) and long short-term memory (LSTM) networks to achieve superior recognition accuracy, seamless integration into smart healthcare systems for flexible authentication, and an efficient preprocessing and augmentation strategy for public ECG datasets that improves data quality and enables fair comparison with existing state-of-the-art (SOTA) models.

Several studies have explored ECG signal analysis for biometric authentication using ML and deep learning techniques. Asadianfam *et al.* [15] examined the ECG-based authentication systems, while Shdefat *et al.* [16] reviewed the opportunities and challenges associated with ECG biometrics. Li *et al.* [17] highlighted the potential of physiological signals such as ECG, electroencephalogram (EEG), and photoplethysmogram (PPG) for improving authentication frameworks. Pereira *et al.* [18] analyzed various ECG data acquisition strategies and their influence on authentication performance. Hammad *et al.* [19] proposed deep neural network–based authentication models using residual CNNs and end-to-end CNN architectures, evaluated on the National Metrology Institute of Germany or Physikalisch-Technische Bundesanstalt (PTB) and check your bio-signals here initiative (CYBHi) datasets, achieving an average accuracy of approximately 98.5%. Labati *et al.* [20] introduced the deep-ECG framework, which combines signal preprocessing, CNN-based feature extraction, and softmax classification [21]. Evaluated using the PTB diagnostic ECG database, their approach outperformed several existing methods in biometric recognition tasks. Martin and Reillo [22] presented the BioECG framework, which integrates CNN and LSTM models along with an enhanced and diversified dataset to improve ECG biometric performance. Their results demonstrated improved identification accuracy and highlighted the potential of deep learning–based ECG biometrics for security and healthcare applications. Hosseinzadeh *et al.* [23] provided a comprehensive review of ECG-based authentication techniques, categorizing them into uni-modal and multi-modal systems. Their analysis revealed that most uni-modal approaches rely on SVM and artificial neural networks, while multi-modal systems combine ECG with other biometrics or cryptographic mechanisms, each presenting distinct limitations and research challenges. Ivanciu *et al.* [24] proposed a siamese neural network–based ECG authentication framework using image representations of ECG signals. Tested on the ECG-ID dataset within a private cloud environment, the system achieved authentication accuracy of 87.3%. Albuquerque *et al.* [25] introduced an ECG-based identification method using random under-sampling boosting (RUSBoost) and compared it with nearest neighbor search (NNS). Experimental results showed that RUSBoost achieved superior balance in accuracy, sensitivity, and F1-score, while NNS demonstrated slightly higher overall accuracy.

2. METHOD

The proposed CardioGuard framework employs a systematic workflow consisting of ECG data acquisition, preprocessing, model development, training, evaluation, optimization, deployment, and continuous monitoring. The framework combines CNNs and LSTM networks to extract both spatial and temporal features from ECG signals effectively. Model performance is evaluated using metrics such as accuracy, sensitivity, precision, F1-score, specificity, and area under the curve (AUC). The architecture is designed to ensure security, reliability, and efficient authentication in smart healthcare applications. Figure 2 presents the overall workflow of the CardioGuard model, including ECG acquisition, preprocessing, CNN-based feature extraction, LSTM-driven temporal learning, flattening, and final classification through dense and softmax layers for accurate authentication of ECG signals.

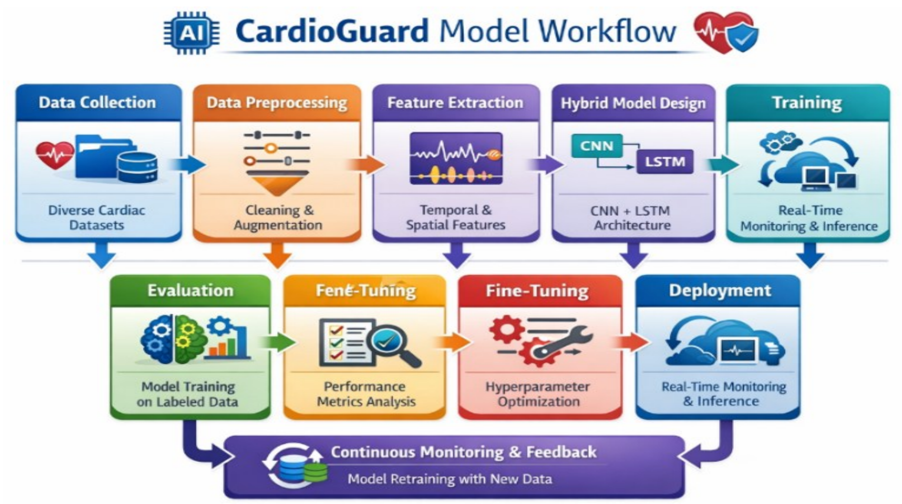


Figure 2. Schematic representation of the proposed methodology

2.1. Proposed CardioGaurd model

The proposed CardioAuth framework employs a hybrid CNN-LSTM architecture with a dense layer for ECG-based authentication. Initially, ECG signals are processed through CNN layers to extract important features, while pooling layers reduce feature dimensions. The extracted features are then forwarded to the LSTM network, which captures temporal dependencies and preserves long-term signal characteristics through gated memory mechanisms. The LSTM output is flattened into a one-dimensional vector and passed to a dense layer for refined feature learning. Finally, a softmax classifier performs multi-class classification by generating probability scores for authentication. Using ECG peak features, the model accurately distinguishes authorized and unauthorized signals. Figure 3 presents the block diagram of the proposed CardioGuard framework.

Regarding the CNN layers, these feed-forward networks are widely used in medical signal analysis, object detection, facial recognition, and image classification [26]. Common CNN architectures include visual geometry group (VGG)-Net, Inception, ResNet, DenseNet, and Xception Net [27]. Across these models, the layer configurations for feature extraction remain largely consistent. The convolutional layer is typically the first layer, which slides a kernel across the input data to compute dot products and extract features. The output is passed through a rectified linear unit (ReLU) activation function, introducing non-linearity and enhancing computational efficiency. Subsequently, a max pooling layer downsamples the feature map to reduce dimensionality. The resulting shared feature maps are then flattened into a single linear vector. In this study, six convolutional layers with corresponding pooling layers were employed. Additionally, batch normalization was applied across several layers to mitigate covariate shift and improve training stability [28].

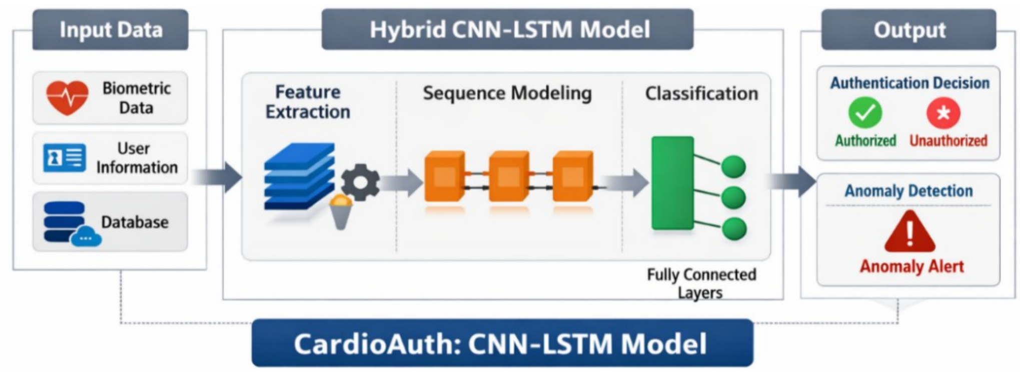
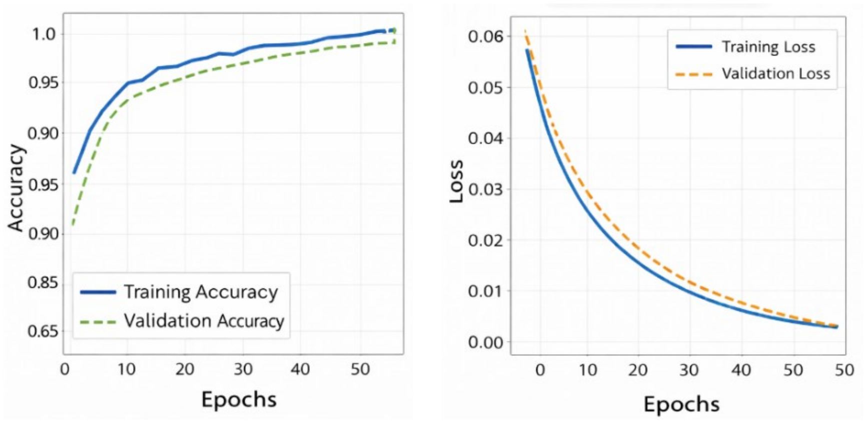


Figure 3. Schematic of the proposed CardioAuth CNN-LSTM model workflow

3. RESULTS AND DISCUSSION

The CardioGuard framework is trained using cardiac electrical signals within a deep learning architecture developed for biometric authentication. CNN layers extract discriminative spatial features from ECG waveforms, while LSTM layers capture temporal dependencies in the signal patterns. The learned spatiotemporal features are then used to classify signals as genuine or impostor. Before training, preprocessing and feature enhancement techniques are applied to improve dataset quality and diversity. The model is trained using a batch size of 64, the Adam optimizer, binary cross-entropy loss, and an adaptive learning strategy with ReduceLROnPlateau for efficient convergence. A softmax activation layer generates final classification probabilities. The framework is implemented using Keras with TensorFlow backend, with 80% of the dataset used for training and 20% for validation. An optimal authentication threshold is selected using validation data by analyzing the probability distributions of genuine and unauthorized ECG samples to maximize verification performance.

Threshold adjustment enables the CardioGuard system to maintain a balance between security and usability. A higher threshold lowers false acceptance rates and strengthens protection against unauthorized access, whereas a lower threshold reduces false rejections for genuine users. During authentication, ECG signals are acquired, preprocessed, and evaluated by the trained model, where access is granted if the predicted probability exceeds the selected threshold. Model performance is analyzed using training and validation accuracy and loss curves as shown in Figure 4, which demonstrate effective learning, stable convergence, and minimal overfitting through smooth trends and close curve alignment. Figure 4(a) presents the training and validation accuracy across epochs, while Figure 4(b) illustrate the corresponding loss variations. Figure 5 compares the performance of the proposed CardioAuth model with several SOTA deep learning models. The results demonstrate the superior classification capability and overall effectiveness of the proposed approach over existing methods. In addition, the confusion matrix is used to evaluate classification performance by measuring metrics such as accuracy and precision, highlighting the capability of the CardioGuard framework to reliably distinguish genuine and unauthorized users.



(a) (b)

Figure 4. Training and validation curves associated with CardioGuard architecture: (a) accuracy and (b) loss

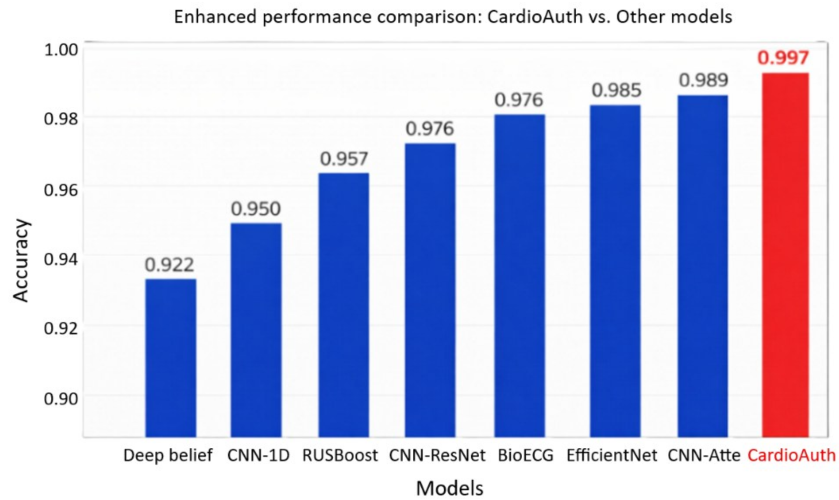


Figure 5. Performance comparison of the CardioGuard model demonstrates its superior accuracy compared to the best SOTA models

The performance of the proposed cardiac signal–based authentication model is assessed using the receiver-operating characteristics (ROC) curve under different decision threshold settings. The AUC is utilized as an important measure to determine the overall classification capability of the framework. The ROC analysis offers a detailed assessment by representing the relationship between sensitivity and specificity across multiple threshold values, which helps in identifying an appropriate operating threshold according to application needs. A ROC curve positioned near the diagonal line represents classification performance similar to random prediction, while a curve located closer to the upper-left region indicates higher sensitivity and specificity, demonstrating effective authentication capability. Figure 6 illustrates the ROC characteristics of the proposed framework at a threshold level of 0.80.

The CardioGuard model is analyzed using widely adopted evaluation measures such as accuracy, precision, sensitivity, specificity, F1-score, and AUC-ROC. The proposed framework achieves superior performance compared with existing SOTA techniques, obtaining an accuracy of 99.7%. Moreover, the model records excellent results across additional performance parameters, including an AUC of 0.99, sensitivity of 0.99, specificity of 0.99, and an F1-score of 0.99. These outcomes validate the efficiency, robustness, and dependability of the proposed ECG-based authentication framework. The consistently high performance across multiple evaluation criteria demonstrates that CardioGuard is highly appropriate for practical implementation in healthcare and security systems, where reliable and precise biometric authentication is critically required.

The proposed CardioGuard framework demonstrates superior authentication performance with an accuracy of 99.7%, confirming the effectiveness of the hybrid CNN–LSTM architecture in learning discriminative spatial and temporal features from ECG signals. This improved performance is consistent with recent deep learning studies, which reported that hybrid CNN-based models, including multi-view convolutional neural network (MVCNN) architectures, significantly enhance ECG feature extraction, classification accuracy, robustness, and model stability for healthcare applications [29]. These findings further validate the proposed framework as a reliable and efficient solution for secure ECG-based authentication and predictive health monitoring.

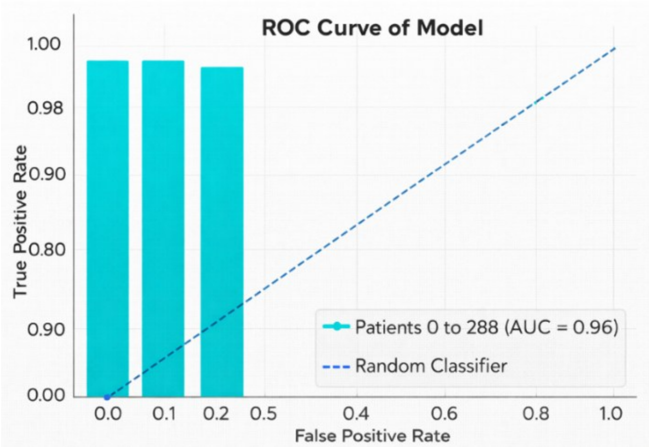


Figure 6. The CardioGaurd model's ROC curve at a threshold value of 0.8

4. CONCLUSION

The rapid advancement of deep learning methodologies has increased research interest in cardiac signal–driven authentication frameworks. Traditional authentication techniques are generally invasive, inefficient, and susceptible to security threats, creating a demand for secure and user-friendly alternatives. To address these limitations, this study presents a hybrid deep learning model that combines CNNs with LSTM networks for authentication using cardiac electrical signals. The CNN layers extract meaningful spatial characteristics, whereas the LSTM component learns temporal patterns present within cardiac waveforms. The proposed system is trained and validated on a large-scale dataset, where experimental findings demonstrate superior authentication capability across multiple evaluation measures. The study also emphasizes the importance of signal preprocessing in enhancing classification reliability and model stability. Therefore, several preprocessing operations, including denoising, normalization, and resampling, are applied systematically to improve signal quality, resulting in noticeable performance enhancement. Although the proposed framework achieves strong results, additional improvements can still be explored. Future research will focus on advanced deep learning strategies, including graph-based convolutional methods and attention-driven architectures, to better model contextual and inter-signal relationships. Furthermore, integrating additional physiological signals such as PPG and EEG may further strengthen authentication accuracy and reliability. Overall, the proposed CNN–LSTM authentication framework demonstrates considerable potential as a scalable, efficient, and non-invasive solution for practical healthcare and security applications.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to their respective institutions for providing the necessary academic support, infrastructure, and research facilities that contributed to the successful completion of this work.

FUNDING INFORMATION

The authors declare that no funding was received for this study.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Swati Lakshmi Boppana	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓
Velicheti Anantha Lakshmi	✓		✓	✓	✓		✓			✓	✓		✓	✓
Padala SriKavitha	✓		✓	✓			✓			✓	✓		✓	
Venkata Ashok Kalaga	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Venkateswara Rao Naramala		✓			✓		✓			✓		✓		
Suneetha Thalluru		✓				✓		✓	✓	✓	✓	✓		
Gunturi S. Raghavendra	✓				✓		✓	✓	✓	✓	✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The author declares that there are no known conflicts of interest associated with this publication. There are no financial or personal relationships that could inappropriately influence or bias the content of this work.

DATA AVAILABILITY

The data used to support the findings of this study are available from the corresponding author, [VAL], upon reasonable request.

REFERENCES

[1] A. Odeh, E. Abdelfattah, and W. Salameh, "Privacy-preserving data sharing in telehealth services," *Applied Sciences*, vol. 14, no. 23, Nov. 2024, doi: 10.3390/app142310808.
[2] Z. Wenhua *et al.*, "A lightweight security model for ensuring patient privacy and confidentiality in telehealth applications," *Computers in Human Behavior*, vol. 153, Apr. 2024, doi: 10.1016/j.chb.2024.108134.
[3] A. H. Sodhro, A. I. Awad, J. V. D. Beek, and G. Nikolakopoulos, "Intelligent authentication of 5G healthcare devices: a survey," *Internet of Things*, vol. 20, Nov. 2022, doi: 10.1016/j.iot.2022.100610.
[4] Q. Xia, H. Jiang, X. Liu, L. Yin, and X. Wang, "Advances in engineered nano-biosensors for bacteria diagnosis and multidrug resistance inhibition," *Biosensors*, vol. 14, no. 2, 2024, doi: 10.3390/bios14020059.
[5] A. Chakraborty, S. Chatterjee, K. Majumder, R. N. Shaw, and A. Ghosh, "A comparative study of myocardial infarction detection from ECG data using machine learning," in *Advanced Computing and Intelligent Technologies*, 2022, pp. 257–267, doi: 10.1007/978-981-16-2164-2_21.
[6] A. Barros, D. Rosario, P. Resque, and E. Cerqueira, "Heart of IoT: ECG as biometric sign for authentication and identification," in *2019 15th International Wireless Communications and Mobile Computing Conference, (IWCMC 2019)*, 2019, pp. 307–312, doi: 10.1109/IWCMC.2019.8766495.
[7] S. K. Kim, C. Y. Yeun, E. Damiani, and N. W. Lo, "A machine learning framework for biometric authentication using electrocardiogram," *IEEE Access*, vol. 7, pp. 94858–94868, 2019, doi: 10.1109/ACCESS.2019.2927079.
[8] I. U. Rehman *et al.*, "A comprehensive systematic literature review of ML in nanotechnology for sustainable development," *Nanotechnology Reviews*, vol. 13, no. 1, Aug. 2024, doi: 10.1515/ntrev-2024-0069.
[9] A. V. L. N. Sujith, G. S. Sajja, V. Mahalakshmi, S. Nuhmani, and B. Prasanalakshmi, "Systematic review of smart health monitoring using deep learning and artificial intelligence," *Neuroscience Informatics*, vol. 2, no. 3, 2022, doi: 10.1016/j.neuri.2021.100028.
[10] H. A. Shah, F. Saeed, S. Yun, J. H. Park, A. Paul, and J. M. Kang, "A robust approach for brain tumor detection in magnetic resonance images using finetuned efficientNet," *IEEE Access*, vol. 10, pp. 65426–65438, 2022, doi: 10.1109/ACCESS.2022.3184113.
[11] H. Khan, T. Hussain, S. U. Khan, Z. A. Khan, and S. W. Baik, "Deep multi-scale pyramidal features network for supervised video summarization," *Expert Systems with Applications*, vol. 237, 2024, doi: 10.1016/j.eswa.2023.121288.

[12] N. Ibtehaz *et al.*, "EDITH : ECG biometrics aided by deep learning for reliable individual authentication," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 4, pp. 928–940, 2022, doi: 10.1109/TETCI.2021.3131374.

[13] F. Y. O. Abdalla, L. Wu, H. Ullah, G. Ren, A. Noor, and Y. Zhao, "ECG arrhythmia classification using artificial intelligence and nonlinear and nonstationary decomposition," *Signal, Image and Video Processing*, vol. 13, no. 7, pp. 1283–1291, 2019, doi: 10.1007/s11760-019-01479-4.

[14] H. A. Shah, F. Saeed, M. Diyan, N. A. Almujally, and J. M. Kang, "ECG-TransCovNet: a hybrid transformer model for accurate arrhythmia detection using electrocardiogram signals," *CAAI Transactions on Intelligence Technology*, 2024, doi: 10.1049/cit2.12293.

[15] S. Asadianfam, M. J. Talebi, and E. Nikougoftar, "ECG-based authentication systems: a comprehensive and systematic review," *Multimedia Tools and Applications*, vol. 83, no. 9, pp. 27647–27701, 2024, doi: 10.1007/s11042-023-16506-3.

[16] A. Shdefat, N. Mostafa, L. Saker, and A. E. Topcu, "A survey study of the current challenges and opportunities of deploying the ECG biometric authentication method in IoT and 5G environments," *Indonesian Journal of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 394–416, 2021, doi: 10.52549/ijeei.v9i2.2890.

[17] L. Li *et al.*, "A survey of PPG's application in authentication," *Computers and Security*, vol. 135, 2023, doi: 10.1016/j.cose.2023.103488.

[18] T. M. C. Pereira, R. C. Conceição, V. Sencadas, and R. Sebastião, "Biometric recognition: a systematic review on electrocardiogram data acquisition methods," *Sensors*, vol. 23, no. 3, 2023, doi: 10.3390/s23031507.

[19] M. Hammad, P. Pławiak, K. Wang, and U. R. Acharya, "ResNet-attention model for human authentication using ECG signals," *Expert Systems*, vol. 38, no. 6, 2021, doi: 10.1111/exsy.12547.

[20] R. D. Labati, E. Muñoz, V. Piuri, R. Sassi, and F. Scotti, "Deep-ECG: convolutional neural networks for ECG biometric recognition," *Pattern Recognition Letters*, vol. 126, pp. 78–85, 2019, doi: 10.1016/j.patrec.2018.03.028.

[21] I. Ahmad *et al.*, "Multi-feature fusion based convolutional neural networks for EEG epileptic seizure prediction in consumer internet of things," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 5631–5643, Aug. 2024, doi: 10.1109/TCE.2024.3363166.

[22] P. T. Martin and R. S. Reillo, "BioECG: improving ECG biometrics with deep learning and enhanced datasets," *Applied Sciences*, vol. 11, no. 13, 2021, doi: 10.3390/app11135880.

[23] M. Hosseinzadeh, B. Vo, M. Y. Ghafour, and S. Naghipour, "Electrocardiogram signals-based user authentication systems using soft computing techniques," *Artificial Intelligence Review*, vol. 54, no. 1, pp. 667–709, 2021, doi: 10.1007/s10462-020-09863-0.

[24] L. Ivanciu, I. A. Ivanciu, P. Farago, M. Roman, and S. Hintea, "An ECG-based authentication system using siamese neural networks," *Journal of Medical and Biological Engineering*, vol. 41, no. 4, pp. 558–570, 2021, doi: 10.1007/s40846-021-00637-9.

[25] S. L. Albuquerque, C. J. Miosso, A. F. Rocha, and P. R. L. Gondim, "Authentication based on electrocardiography signals and machine learning," *Engineering Research Express*, vol. 3, no. 2, 2021, doi: 10.1088/2631-8695/abffa6.

[26] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, "A survey of convolutional neural networks: analysis, applications, and prospects," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 12, pp. 6999–7019, Dec. 2022, doi: 10.1109/TNNLS.2021.3084827.

[27] F. Chollet, "Xception: deep learning with depthwise separable convolutions," in *2017 IEEE Conference on Computer Vision and Pattern Recognition*, Jul. 2017, pp. 1800–1807, doi: 10.1109/CVPR.2017.195.

[28] N. Tajbakhsh *et al.*, "Convolutional neural networks for medical image analysis: full training or fine tuning?," *IEEE Transactions on Medical Imaging*, vol. 35, no. 5, pp. 1299–1312, May 2016, doi: 10.1109/TMI.2016.2535302.

[29] D. Santhakumar, K. D. Shree, M. Buvanesvari, A. S. Kumar, and A. O. Salau, "HD-MVCNN: High-density ECG signal based diabetic prediction and classification using multi-view convolutional neural network," *Egyptian Informatics Journal*, vol. 28, Dec. 2024, doi: 10.1016/j.eij.2024.100573.

BIOGRAPHIES OF AUTHORS

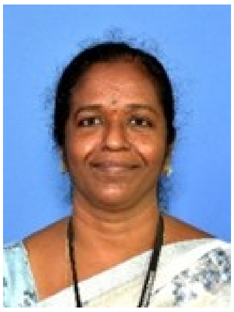
Swati Lakshmi Boppana is an assistant professor in the Department of Electronics and Communication Engineering at Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, India. She is actively involved in teaching and research activities within the department. Her research contributions include work on embedded systems and communication technologies, as evidenced by her publications in international conferences and journals. She has co-authored several technical papers on topics such as digital emergency systems and antenna design. She can be contacted at email: boppanaswathi@gmail.com.

Velicheti Anantha Lakshmi is working as an assistant professor in the Department of Computer Science and Engineering (AI and ML) at Pragati Engineering College, Kakinada, India. She is currently pursuing her Ph.D. in Computer Science and Engineering at Acharya Nagarjuna University, Guntur. She completed her M.Tech. in Computer Science and Engineering from Jawaharlal Nehru Technological University Kakinada and her B.Tech. in the same specialization from Jawaharlal Nehru Technological University Hyderabad. Her areas of interest include cloud computing, machine learning, deep learning, and transfer learning. She has guided several student projects focusing on these technologies and various web-based applications. She can be contacted at email: ananthalakshmivelicheti@gmail.com.

Padala SriKavitha is assistant professor in the Department of Electrical and Electronics Engineering, Aditya University, Kakinada, India. She pursed Masters of Technology from Kakinada Institute of Engineering and Technology, Korangi, India in 2018. Her main research work focuses on machine learning and deep learning applications. She can be contacted at email: srikavithapadala@gmail.com.

Venkata Ashok Kalaga is Sr. assistant professor in the Department of Electronics and Communication Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram, India. He pursued Master of Technology from Jawaharlal Nehru Technological University, Kakinada in 2012 and pursuing Ph.D. from Andhra University. His research work focuses on signal processing, IoT. He can be contacted at email: ashok.516m@gmail.com.

Dr. Venkateswara Rao Naramala is working as a professor in the Department of Computer Science and Engineering at R.V.R. and J.C. College of Engineering, Guntur, India. His academic and research interests include AI, artificial neural networks, and human–computer interaction. He is actively engaged in teaching and research, contributing to advancements in these areas through scholarly publications and academic activities. He can be contacted at email: vnaramala@gmail.com.



Dr. Suneetha Thalluru is associate professor in the Department of Electronics and Communication Engineering, R.V.R. and J.C. College of Engineering, Guntur, India. Research interests in the fields of microstrip patch antennas, microprocessors, computer networks. She can be contacted at email: suneethalluru@gmail.com.

Gunturi S. Raghavendra is assistant professor in the Department of Computer Science and Engineering, coordinator, and academics at Koneru Lakshmaiah Education Foundation Bachupally Campus Hyderabad, India. His research areas of interest include ML, big data, cloud computing, and deep learning. He can be contacted at email: g.raghavendra@klh.edu.in.