НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2025 Том 25 № 3 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2025 Vol. 25 No 3 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

doi: 10.17586/2226-1494-2025-25-3-475-486

A deep learning approach for adaptive electrocardiogram-based authentication in an internet of things enabled telehealth system

Mohamed Abdalla Elsayed Azab✉

ITMO University, Saint Petersburg, 197101, Russian Federation

mohamed.a.azab@itmo.ru✉, https://orcid.org/0009-0000-1748-0029

Abstract

As telehealth services have become integral to healthcare applications; robust authentication mechanisms are critical for safeguarding sensitive patient data and services. Conventional authentication techniques including passwords and tokens are susceptible to theft and security breaches. This vulnerability highlights the need for alternative methods that offer improved security measures and ease of use. Biometric authentication, which leverages unique physical and behavioral traits, has emerged as a promising alternative. Among various biometric modalities, electrocardiogram (ECG) signals stand out because of their uniqueness, stability, and noninvasive nature. This study introduces an innovative deep-learning-based authentication system that utilizes ECG signals to enhance security in Internet of Things (IoT)-powered telehealth environments. The proposed model employs hybrid architecture, starting with a Siamese Neural Network (SNN) for dynamic verification, followed by a Convolutional Neural Network (CNN) for feature extraction, utilizing an optimized Sequential Beat Aggregation approach for robust ECG-based authentication. The system operates securely and adaptively, and performs real-time authentication without requiring human intervention. The research approach involved the acquisition and processing of electrocardiogram data from the ECG-ID dataset which encompassed 310 ECG individuals obtained from 90 individual subjects. This dataset provided a comprehensive set of samples for training and evaluation. The model achieved high authentication accuracy (98.5 %–99.5 %) and a false acceptance rate of 0.1 % with minimal computational overhead, validating its feasibility for real-time applications. This study integrates ECG-based authentication into telehealth systems, creating a secure foundation for safeguarding patient data. The innovative use of ECG signals advances secure and adaptable for a personalized remote health monitoring system development.

Keywords

biometric authentication, telehealth security, adaptive authentication systems, ECG signal analysis, neural networks, hybrid deep learning

For citation: Azab M.A.E. A deep learning approach for adaptive electrocardiogram-based authentication in an internet of things enabled telehealth system. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 3, pp. 475–486. doi: 10.17586/2226-1494-2025-25-3-475-486

УДК 004.056

Глубокое обучение для адаптивной аутентификации на основе электрокардиограммы в системе телемедицины с поддержкой интернета вещей

Мохамед Абдалла Эльсайед Азаб✉

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

mohamed.a.azab@itmo.ru✉, https://orcid.org/0009-0000-1748-0029

Аннотация

Телемедицинские услуги стали неотъемлемой частью медицинских приложений, надежные механизмы аутентификации имеют решающее значение для защиты конфиденциальных данных пациентов и предоставляемых сервисов. Традиционные методы аутентификации, такие как пароли и токены, подвержены кражам и нарушениям безопасности. Эта уязвимость подчеркивает необходимость альтернативных методов, которые обеспечивают более высокий уровень безопасности и удобство использования. Биометрическая

аутентификация, использующая уникальные физические и поведенческие характеристики, стала перспективной альтернативой. Среди различных биометрических методов сигналы электрокардиограммы (ЭКГ) выделяются своей уникальностью, стабильностью и неинвазивным характером. В данном исследовании представлен инновационный метод аутентификации на основе глубокого обучения, использующий ЭКГ-сигналы для повышения уровня безопасности в телемедицинских системах, работающих на базе интернета вещей (IoT). Предложенная модель использует гибридную архитектуру: сначала применяется сиамская нейронная сеть (SNN) для динамической верификации, затем сверточная нейронная сеть (CNN) для извлечения признаков с использованием оптимизированного метода последовательной агрегации сердечных циклов для надежной аутентификации на основе ЭКГ. Система функционирует безопасно и адаптивно, выполняя аутентификацию в реальном времени без вмешательства человека. В рамках исследования была проведена обработка данных ЭКГ из набора данных ECG-ID, включающего 310 ЭКГ-сигналов от 90 различных участников. Этот набор данных предоставил обширную выборку для обучения и оценки. Модель достигла высокой точности аутентификации (98,5–99,5 %) и показателя ложного допуска на уровне 0,1 % при минимальной вычислительной нагрузке, что подтверждает ее применимость для задач в реальном времени. Настоящее исследование интегрирует аутентификацию на основе ЭКГ в телемедицинские системы, создавая надежную основу для защиты данных пациентов. Инновационное использование ЭКГ-сигналов способствует созданию безопасной, адаптивной и персонализированной системы удаленного мониторинга здоровья.

Ключевые слова
биометрическая аутентификация, безопасность телемедицины, адаптивные системы аутентификации, анализ ЭКГ-сигналов, нейронные сети, гибридное глубокое обучение

Ссылка для цитирования: Азаб М.А.Э. Глубокое обучение для адаптивной аутентификации на основе электрокардиограммы в системе телемедицины с поддержкой интернета вещей // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 3. С. 475–486 (на англ. яз.). doi: 10.17586/2226-1494-2025-25-3-475-486

Introduction

With the growing adoption of telehealth systems, the demand for secure and reliable management of patient health information has significantly increased. IoT-enabled telehealth systems have become integral in enhancing patient care, enabling remote monitoring, and streamlining healthcare delivery [1, 2]. However, the spread of connected devices has also introduced significant security challenges, particularly in safeguarding sensitive patient data and ensuring secure access to telehealth services. Traditional authentication methods, including passwords and tokens, are increasingly inadequate owing to vulnerabilities, such as theft, replication, and brute-force attacks [3]. In the face of the growing threat landscape, there is an urgent need for new, robust, and flexible authentication systems aimed at addressing the unique needs of Internet of Things (IoT) telehealth environments [4].

Biometric authentication, which leverages unique physiological and behavioral traits, has emerged as a promising solution for securing IoT-enabled systems and providing enhanced security and user convenience. Unlike traditional methods, biometric systems leverage unique physiological or behavioral traits, making it difficult to replicate or falsify [3]. Among the various biometric modalities, electrocardiogram (ECG) signals stand out because of their intrinsic liveness, universality, and resistance to spoofing. ECG signals capture the electrical activity of the heart, offering a dynamic and highly individualized biometric pattern [5]. This unique property makes ECG-based systems robust alternatives for secure and reliable user authentication in IoT-enabled telehealth systems.

ECG signals are private and accurate and more reliable than other biometrics [6]. Such P-Q-R-S-T waveform patterns, as shown in Fig. 1 provide proof of the subject liveness and uniqueness. The nature of ECG signals is complex because of their random, involuntary, and complex characteristics leading to better authentication capabilities [7].

Artificial intelligence improves IoT-enabled telehealth security by enabling reliable ECG-based biometric authentication. Machine learning techniques like K-Nearest Neighbor, Support Vector Machine and Random Forest are used, with deep learning increasingly favored for its pattern analysis and accuracy [8, 9]. Deep Learning techniques, particularly neural networks, have emerged as a possible telehealth ECG signal authentication solution. Using huge datasets of ECG signals, neural networks can be trained to understand the distinctive patterns and properties that distinguish real signals from fraudulent ones [10, 11].

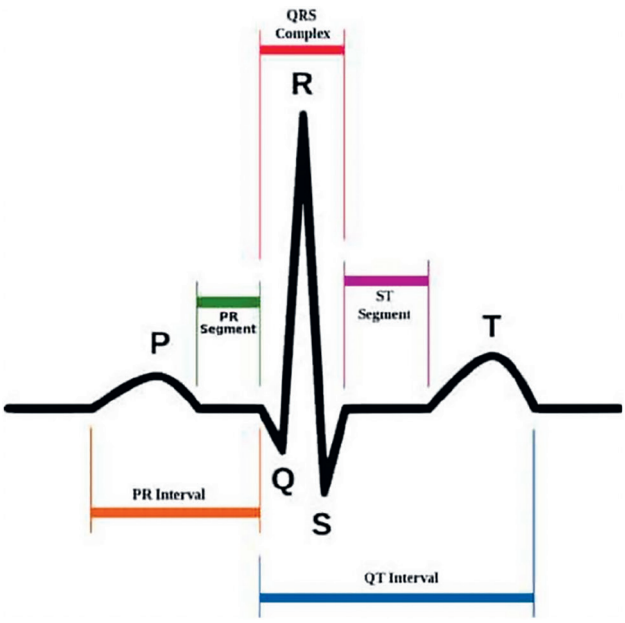

Fig. 1. Segment Representation of ECG

This study addresses the growing demand for robust authentication systems amid rising digital reliance and data security challenges. By leveraging deep learning, it proposes an adaptive authentication framework that combines Siamese Neural Networks (SNNs) for verification and Convolutional Neural Networks (CNNs) for multiclass authentication, utilizing an optimized Sequential Beat Aggregation approach. The system enhances ECG biometrics, improves authentication speed and efficiency, and detects noise-inducing abnormalities, addressing key IoT telehealth challenges, such as evolving threat landscapes, dynamic user behavior, and real-time processing requirements.

Our study presents three key contributions: showing the use of ECG signals for adaptive authentication in IoT telehealth systems, developing advanced deep learning models that merge biometric verification with authentication, and assessing the system resilience under various signal conditions to enhance security and accessibility in IoT-based healthcare environments.

Literature Survey

ECG Authentication Using Machine Learning and Deep Learning Models

Several studies have explored the use of Machine Learning and Deep Learning models for ECG-based authentication. Asadian et al. [12] examined the feasibility of ECG-based authentication systems, while Shdefat et al. [13] discussed opportunities and challenges in their implementation. Lin Li et al. [14] extended the literature by discussing the application of ECGs, Electroencephalography, and Photoplethysmogram in authentication systems. Pereira et al. [15] researched different ways of capturing data to make the authentication process more efficient in terms of its precision.

Hammad et al. [16] proposed using Deep Neural Networks with architectures such as Residual Convolutional Neural Networks (ResNet) and end-to-end CNNs for reliable human authentication. Using datasets like Physikalisch-Technische Bundesanstalt (PTB) and Check Your Bio-Signals Here, their models achieved an average accuracy of 98.5 %. Similarly, Labati et al. [17] introduced Deep-ECG, a biometric recognition method combining signal preprocessing, CNN feature extraction, and SoftMax-based detection. Their work demonstrated improved performance in scenarios such as identity verification and periodic re-authentication, outperforming earlier approaches.

Hybrid and Advanced Architectures

Martin et al. [18] proposed "BioECG" which integrates CNN and Long short-term memory model to enhance authentication precision. Their method emphasized the importance of addressing temporal dependencies in ECG signals, resulting in improved accuracy and robustness. D'angelis et al. [19] employed Vision Transformers for ECG biometric recognition, effectively capturing intricate temporal and spatial signal features. AlDuwaile and Islam [20] utilized single heartbeat analysis with CNNs, simplifying data collection while maintaining high accuracy.

Some of the studies also highlighted novel hybrid system models. For instance, Ivanciu et al. [21] implemented a SNN using ECG signal images, achieving an accuracy of 87.3 %. Albuquerque et al. [22] employed Random Under-Sampling Boosting and Nearest Neighbor Search, achieving accuracy rates of 97.4 % and 99.5 %, respectively, for ECG-based user identification. These works highlight the potential of hybrid models for improving authentication accuracy and adaptability.

Multi-Modal Biometric Systems

In order the overcome the above-mentioned limitations of uni-modal systems, Alkeem et al. [23] introduced a multi-modal biometric system that integrates ECG signals, facial images, and fingerprints. The system utilized multitasking learning and feature fusion, demonstrating superior accuracy and generalization. Multi-modal methods outperformed single-modal approaches, proving highly effective for secure authentication and gender classification.

Emerging Techniques and Applications

Recent advancements have introduced novel techniques such as lightweight multi-factor authentication strategies [23] which incorporate digital signatures and device capabilities to enhance IoT security. Similarly, studies [24] tailored authentication methods for the Internet of Medical Things, utilizing human biometrics to establish secure device communication. Blockchain-based solutions have also emerged, such as the "Bubbles-of-Trust" scheme [25], which employs virtual trust zones and Ethereum blockchain technology to streamline authentication in IoT networks [26–28].

Limitations and Gaps in Existing Research

While the reviewed studies demonstrate significant advancements in ECG biometrics, several limitations persist. Many approaches [16, 17, 29] focus primarily on accuracy, often neglecting computational efficiency and robustness against noisy or heterogeneous datasets. Additionally, while methods integrating CNN and LSTM architectures [18, 20] show promise, they often fail to fully leverage the potential of these models for capturing complex temporal dynamics in ECG signals. Moreover, scalability and real-time processing remain challenges in deploying these systems for practical IoT telehealth applications.

Proposed Methodology

In this paper, we have proposed an innovative approach to use deep learning-based ECG in IoT-based telehealth systems for patient or user authentication and attempted to develop a model. By passing through steps like: data gathering, preparation, model creation, training, testing, tuning, implementation and monitoring it ensures security and flexibility. Fig. 2 shows how this process helps solve authentication problems.

The proposed model

Our Adaptive Authentication System is built on SNN and CNN as foundational models for ECG signal analysis. SNN model is for time related change, and CNN model is to interpret the pattern over the signals. Being trained on thousands of highly processed ECG data, and continuing to show robust performance in test data with accuracy,

Fig. 2. Deep learning process for adaptive authentication

sensitivity, precision, F1-score, Area Under the Curve (AUC), specificity. The system improves incrementally with small changes contributed over time. It also keeps a good balance between being secure and easy to use, offering a safe and practical solution for users.

The core feature of this model is its adaptability to dynamic conditions, making it particularly suitable for IoT-enabled telehealth environments. The deep learning mechanisms within the architecture are designed to adjust to evolving threat landscapes and changing user behaviors, ensuring high levels of dependability and efficiency [30]. The model uses Sequential Beat Aggregation, training with individual heartbeats and aggregating predictions from multiple beats during inference, balancing simplicity with accuracy while reducing complexity and data demands of longer concatenated signals.

Sequential Beat Aggregation approach actually improves robustness by reducing anomalous beats impact, ensuring real-time adaptability essential for IoT telehealth. It can be seamlessly integrated with IoT devices to work efficiently in the real world. The lightweight, adaptive, and fast design of this system makes it an excellent choice for secure and practical telehealth deployments and applications.

To provide a comprehensive overview, Fig. 3 explains the methodology of the proposed model, highlighting the integration of data processing, model architecture, and deployment strategies.

The ECG signal first enters through the SNN which mainly focuses on capturing the changes over time and important details. The result is then sent to the CNN where layers find patterns in the signal and reduce its size for quicker processing. This step-by-step method improves the ability to identify key features. The CNN result is turned into a single line of data and sent to a dense layer, which prepares it for further processing. Lastly, a classifier at the end of the model turns the scores into a format that can be used for identifying different classes. The model learns from the key points in the ECG signal to tell the difference between real and fake signals, making sure it works well and accurately for user identification. This proposed design effectively combines speed and accuracy in classification tasks.

Convolution neural network layers

It is a feed-forward neural network that is very frequently used for medical analysis, object detection, face recognition, and picture classification [31]. The CNN network has a variety of designs, including VGG-Net [32], Inception [33], ResNet [16] DenseNet [34], and Xception Net [35]. Generally, the layers used for experimental analysis are the same in all CNN models. The first layer typically used to extract features from an ECG trace is the convolution layer. To achieve this, move a kernel or feature detector over the input data or feature vector and compute the dot product of the input and kernel at each location. After extracting the features, the network is made non-linear using activation function which also speeds up total computation. After the activation layer, a rectified feature map is put through the max pooling layer. The down-sampling process of pooling lowers the feature map size. Then, a shared feature map is sent to be flattened into a single, lengthy continuous linear vector. This study used six convolution layers and an identical number of pooling layers. Batch normalization was also performed in various layers to solve the covariate shift problem [23].

Fully connected layers

A dense block comprises interconnected hidden layers where each neuron receives input from all preceding neurons. Using matrix-vector multiplication, it adjusts output dimensionality and applies an activation function for accurate classification or prediction.

$$y = activation(z), \text{ where } \mathbf{z} = W \times x + b,$$

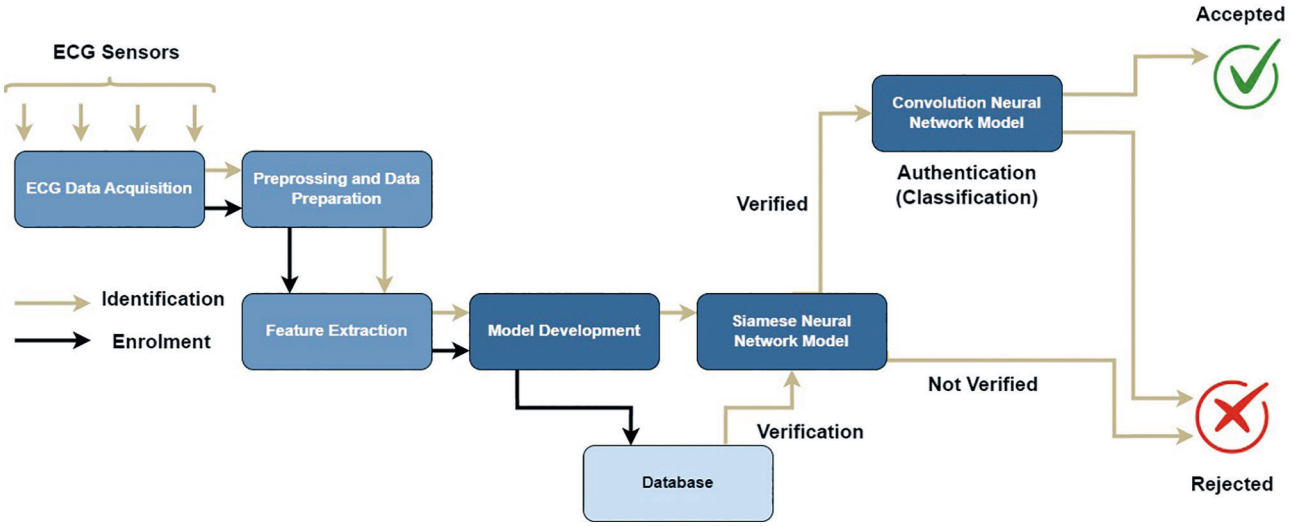

Fig. 3. Adaptive Authentication Biometric System Proposed Model

where **z** is the pre-activation vector and activation represents the activation function σ. Dense layers are integral to neural networks, connecting inputs to outputs for precise predictions. For ECG-based authentication, a single dense layer with 286 neurons enables accurate classification. The setup is: Hybrid SNN-CNN output → Flatten Layer → Dense Layers → Classifier. Fig. 4 illustrates the CNN architecture.

Threshold based-authentication algorithm

The probability-based threshold function is the probability of a match between a test signal and a stored reference signal, usually for signal processing applications like a biometric authentication system. It calculates the Probability Density Functions (PDF), of the test and reference signals for likelihoods of different values of the signal. Comparing the PDFs gives the match probability. The threshold value is determined based on the required security level and False Acceptance Rate (FAR). Increasing the threshold makes FAR higher but improves security, whereas decreasing it reduces both.

Loss function

This function measures an algorithm performance by quantifying discrepancies between predicted outputs and target values, often using cross-entropy for assessing classification models accuracy against actual labels. This study used Binary Cross Entropy (BCE) as a loss function for binary classification tasks like ECG data authentication [24]. In a hybrid SNN-CNN model for human authentication, BCE loss can help the general model focus on the essential ECG signal regions while ignoring the areas that are less important to the authentication goal. BCE will be used as an optimization method to discover the best values valid for human authentication based on ECG signals [25].

$$BCE = -\frac{1}{N}\sum_{i=0}^{N} y_i \log(\hat{y}_i) + (1 - y_i)\log(1 - \hat{y}_i).$$

Here, predictions and true values are represented by y_i and $\hat{y}_i$, respectively, where N denotes the number of training sets for the i-th slice ($i \in N$).

Hyperparameters settings

Hyperparameters optimize the training success of the hybrid SNN-CNN deep learning model for ECG-based authentication. Key parameters include the loss function, optimizer, batch size, learning rate, and epochs, significantly boosting efficiency while ensuring adaptability if the primary objective encounters challenges. Lists of the hyperparameters chosen for training SNN end CNN: loss functions — Categorical Cross Entropy; learning rate — 0.00001; batch size — 64; epochs — 100; optimizer — Adam.

Similarly, these hyperparameters are frequently adjusted using a grid search methodology to obtain the best possible combination for the training process. For instance, rapid convergence of the model that shoots past the global minimum may be caused by a high learning rate [36]. On the other hand, a slow learning rate may stall training, while too few epochs cause underfitting, and too many lead to overfitting. Proper parameter tuning enhances model accuracy and robustness.

Experiment Results

Dataset description

The ECG-ID database consists of 310 ECG recordings from 90 subjects, aged 13–75, including 44 men and 46 women. Each recording is a 20-second ECG Lead I signal, sampled at 500 Hz with 12-bit resolution and a nominal range of ±10 mV. The dataset includes 2–20 recordings per individual, collected over a period of up to six months, with intervals ranging from days to months between sessions. This multi-session structure allows for the evaluation of temporal variability in ECG signals, making it suitable for assessing the long-term stability of ECG-based biometric systems.

The dataset provides both noisy raw signals (Signal 0) and filtered signals (Signal 1), enabling detailed analysis of ECG morphology under different noise conditions. The recordings were collected using standard ECG electrodes placed on the wrists, making the acquisition process non-invasive and suitable for real-world applications.

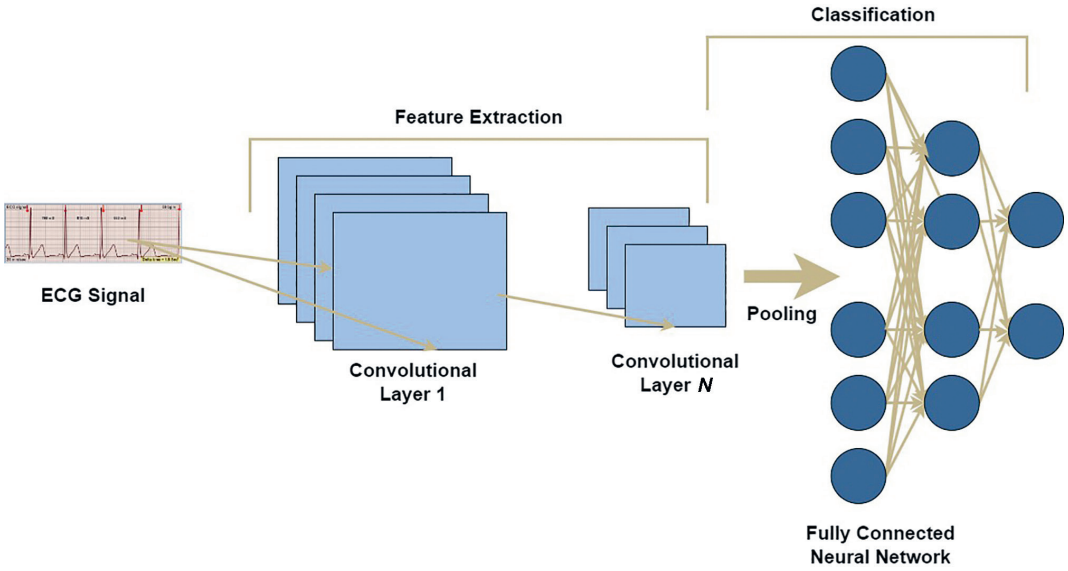

Fig. 4. Diagram of CNN Architecture

Dataset preprocessing and augmentation

Data preparation would enhance quality data analysis on ECG-ID dataset signals by effectively cleaning the initial raw signals. These are the high pass set up to remove, baseline drift and notch filter to remove power line interference along with resampling [37]. Preprocessing also standardizes the ECG signals, and quality control is used in order to filter artifacts also forms part of it. Data augmentation shown in Fig. 5 enlarges the dataset, increases the stability and optimizes performance through the introduction of variability. Scaling, rotation, flipping, and time-shifting are the techniques of diversification of the dataset. These approaches mainly address issues related with overfitting, boosting model accuracy and credibility, scalability, and, therefore, boosting the general performance of ECG-based biometrics. The figure displays the original signal (blue) alongside signals modified by three augmentation methods: noise addition (orange), time-shifting (green), and pitch-shifting (red).

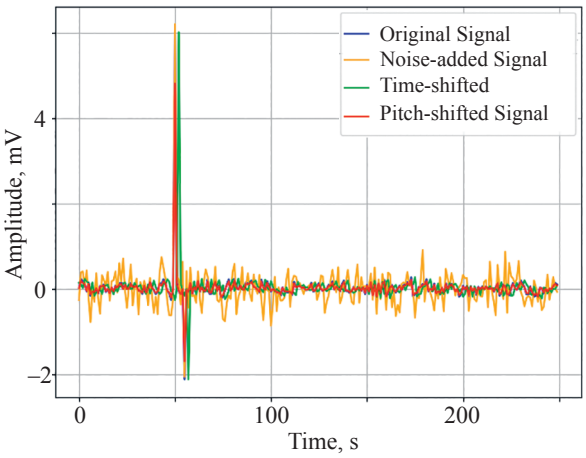

Fig. 5. Data augmentation techniques

Results

This section presents a detailed analysis and conclusions drawn from experimental evaluations, offering insights into the system performance across various scenarios. Both quantitative and qualitative data are thoroughly examined to highlight the system advantages, identify areas for improvement, and evaluate overall efficacy. The experiment utilized 1D ECG signals of length 256, with SNN and CNN models trained using a batch size of 64, a learning rate of 0.00001, and the Adam optimizer with decay.

Training Phase

During the training phase of SNN model, the ECG dataset underwent a preprocessing phase wherein the ECG segments were truncated to 700 per individual, resulting in a well-balanced distribution of classes. This step ensures an equal representation of different classes, providing a more robust foundation for subsequent analysis.

Following the truncation, the pre-processed data underwent normalization, transforming the values to a standardized range between 0 and 1. This normalization process is crucial for mitigating potential anomalies that could complicate signal analysis. By scaling the data to a uniform range, the impact of variations in magnitude is minimized, facilitating a more consistent and effective analysis of ECG signals.

The dataset includes signals from 90 individuals, resulting in a total of 63,000 segments (90 individuals × 700 segments), ensuring a balanced distribution across all individuals. This balance is particularly important for the SNN which compares pairs of ECG signals to verify if they belong to the same individual for human authentication, as it allows the model to learn a robust similarity metric by training on an equal number of positive pairs (same individual) and negative pairs (different individuals) for each class.

Subsequently, the normalized data is shuffled and organized into pairs. Each pair is categorized as either similar (Signal 1) if the segments belong to the same class, or dissimilar (Signal 0) if they pertain to different classes. This pairing strategy, illustrated in Fig. 6, sets the stage for training a classifier to distinguish between similar and dissimilar ECG segments.

Specifically, similar pairs (positive pairs) help the model learn the characteristics of matching signals within the same patient class, while dissimilar pairs (negative pairs) enable the model to identify clear differences between unrelated ECG segments. Fig. 6, *a* shows an example of a positive pair where both signals closely match, and Fig. 6, *b* displays a negative pair where the signals differ significantly. This approach improves the model ability to generalize and enhances classification performance.

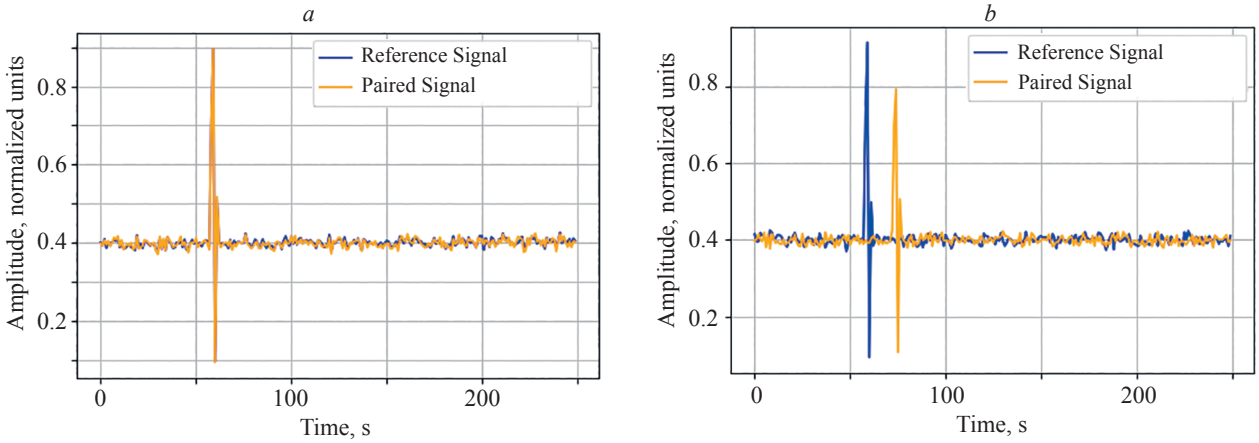

Fig. 6. Examples of pairs: positive (*a*) and negative (*b*)

To calculate the classifier's performance, the dataset is divided into training, validation, and test sets. The Sklearn selection model is utilized for this task, randomly assigning 60 % of the data to training, 20 % to validation, and 20 % to testing. The training set is used to design and fine-tune the classifier, while the test set is held out to assess the classifier's performance and accuracy.

This strategic division of the dataset into training, validation, and test sets not only facilitates robust training but also ensures an unbiased assessment of the classifier's generalization to new, unseen data. The allocation percentages are chosen to strike a balance between providing sufficient data for model training and maintaining an adequate portion for independent evaluation. This meticulous approach enhances the reliability and applicability of the classifier in real-world scenarios.

During the training phase of CNN model, the ECG dataset underwent a segmentation process resulting in 10,000 segments per individual, ensuring a balanced class distribution. This segmentation strategy aims to capture a comprehensive representation of each class, laying the groundwork for a more robust analysis.

Following segmentation, the pre-processed data underwent normalization, scaling the values to a standardized range between 0 and 1. This normalization step is pivotal in mitigating anomalies that might complicate signal analysis. By standardizing the data, variations in magnitude are minimized providing a more consistent foundation for subsequent analysis of ECG signals.

Subsequently, the normalized data is shuffled and partitioned into training and validation sets. This shuffling process is crucial for preventing the model from learning sequence patterns inherent in the data, ensuring a more unbiased evaluation. The division into training and validation sets enables a thorough assessment of the classifier's performance during development.

The dataset includes signals from 90 individuals, with each individual's 700 original segments augmented to create 10,000 segments, resulting in a total of 900,000 segments (90 individuals × 10,000 segments), ensuring a balanced distribution across all individuals. This balance is particularly important for the CNN which classifies ECG signals to identify individuals for human authentication, as it allows the model to learn robust features from an equal number of segments for each class, preventing bias toward overrepresented individuals and improving classification accuracy.

To achieve this partitioning, the Sklearn selection model was utilized, randomly allocating 60 % of the data to the training set, 20 % to the validation set, and 20 % for testing. The training set serves as the basis for designing and fine-tuning the classifier, while the validation set aids in monitoring the model performance and making adjustments to enhance generalization.

The remaining 20 % of the data is reserved for testing, serving as an independent set for the final evaluation of the classifier's performance and accuracy. This separation into distinct training, validation, and test sets ensures a comprehensive assessment of the classifier's ability to generalize to new, unseen data.

Testing Phase

For the verification task, the SNN was trained for 100 epochs, incorporating Model Checkpoint and early stopping mechanisms to monitor validation loss. Using Euclidean Distance, the SNN employed contrastive loss during training. This loss function evaluates the distance between outputs for positive and negative samples, ensuring the network effectively discriminates between these instances for accurate authentication. The training process typically required 20 to 25 minutes, with validation loss stabilizing at 0.3 %. Through experimentation, a decision threshold margin of 0.0009999 was established. If the similarity score equals or exceeds this threshold, the ECG segment is classified as a match with an enrolled template, resulting in successful verification. Some test samples from our experiment are illustrated in Fig. 7.

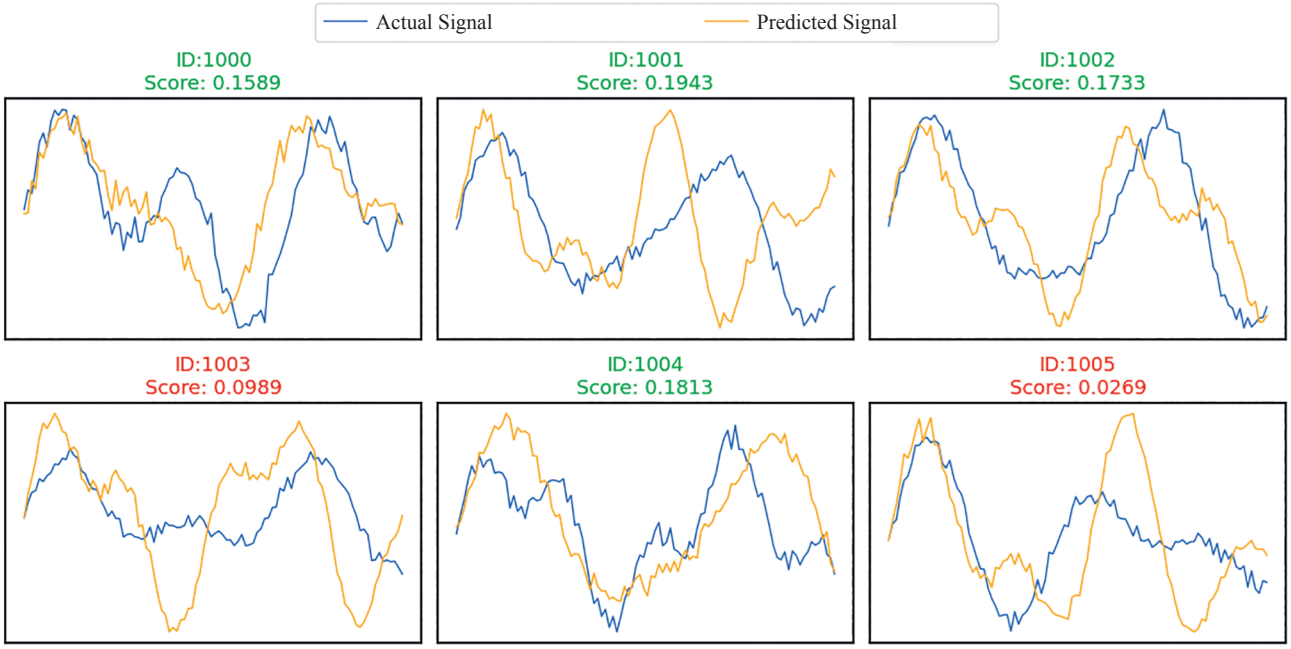

Fig. 7. Predicted samples from verification (SNN) model

For the authentication task, the CNN model underwent training for an average duration of 4 hours across 100 epochs. Early stopping and Model Checkpoint prevented the possibility of finishing after around 20–25 epochs on average. With an accuracy of 98.8 % and a validation loss of 0.32 %, as shown in Fig. 8, *a*, the rapid convergence of training and validation accuracy within the first 20 epochs are demonstrated, while Fig. 8, *b* shows a steady decrease in both training and validation loss, confirming effective learning with minimal overfitting.

This study consolidates the performance of the proposed SNN-CNN framework for ECG-based authentication in IoT telehealth, highlighting its resource efficiency, accuracy, reliability, and adaptability, with results demonstrated through comprehensive figures.

The confusion matrix in Fig. 9 grounds the precision, recall, and F1-score to nearly 100 %. The confusion matrix shows patient information in a diagonal matrix form and denotes that the total person strength has been estimated correctly. It is used to visually represent the performance of the classification model by showing how well predicted labels match the actual person classes. A perfect or near-perfect diagonal pattern indicates the model accuracy in correctly identifying each class without confusion. Several samples predicted by the model are given in Fig. 10, which shows the applicability of the model for distinguishing between instances.

The Receiver Operating Characteristic (ROC) curve can then be used to evaluate the model effectiveness in user authentication with ECG data in terms of decision thresholds. The AUC is an estimate of the overall model performance. This indirectly provides a possibility of selecting an optimal decision point depending on the needs of a particular application having both sensitivity and specificity in trade off. If your model ROC curve is located near the top left corner, you have a strong model that is great at both high sensitivity and specificity. Fig. 11 shows performance of the proposed model at threshold value.

The performance of the proposed model is 98.8 % based on main parameters and significantly higher than

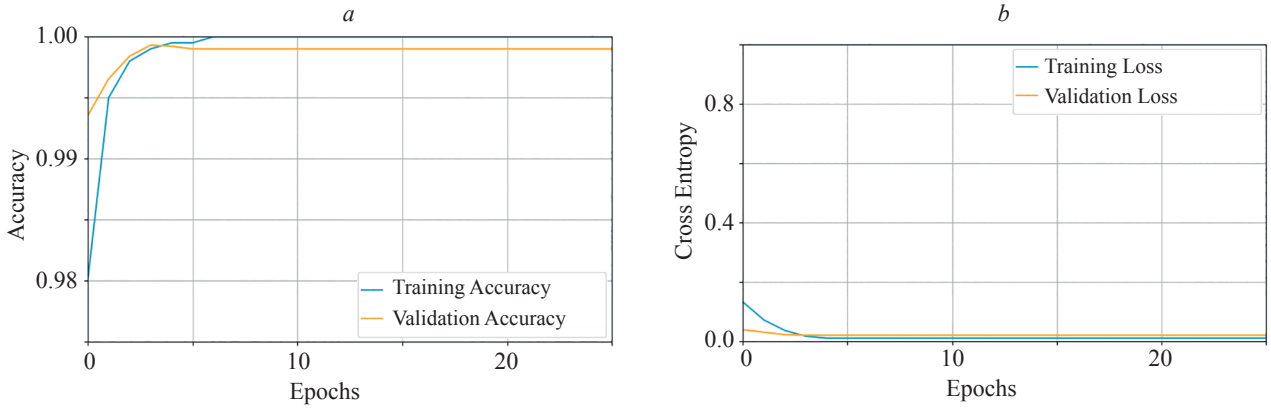

Fig. 8. Accuracy (*a*) and loss (*b*) scores for training and validation

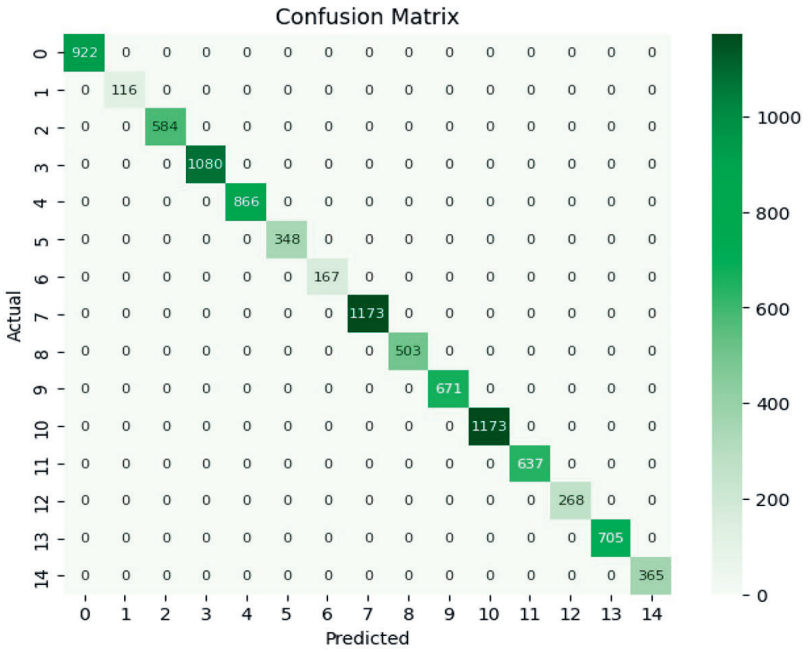

Fig. 9. Confusion Matrix of the proposed authentication model

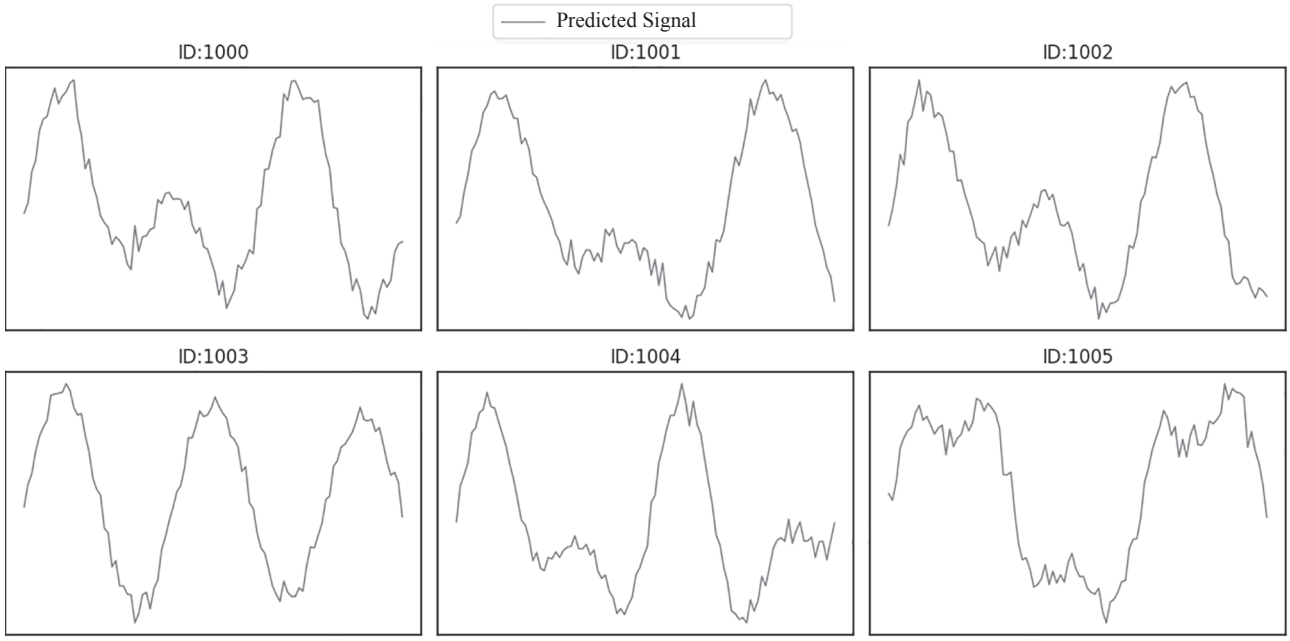

Fig. 10. Predicted samples from authentication (CNN) model

Table. Performance comparison of the proposed model and other models

Publication	Database	Methods	Accuracy, %
[38]	PhysioNet	Random Forest classifier	92.0
[39]	ECG-ID	Decision Curve Analysis	94.0
[40]	ptbdb, mitdb, nsrdb	Matching process	97.6
[20]	MIT-BIH	Feed-Forward Neural Network	95.0
[30]	ECG-ID	Euclidean detector	94.3
[41]	ECG-ID	CNN	96.6
[42]	Low-cost sensors biometrics	One-class classifier density estimation	98.0
[43]	PTB	CNN-LSTM	98.0
Proposed Solution	ECG-ID	SNN-CNN	98.8

the performance of the previous models. It also shows high specificity of 0.99 %, sensitivity of 0.99 %, the AUC of 0.99 % and F1-score of 0.99 %. From the results, we see that it is efficient for ECG based authentication and could be better than other advanced algorithms. The reliability and accuracy of the model may radically change the existing ECG-based authentication systems, primarily in security fields. Table above indicates a comparison of the proposed model with other architectures.

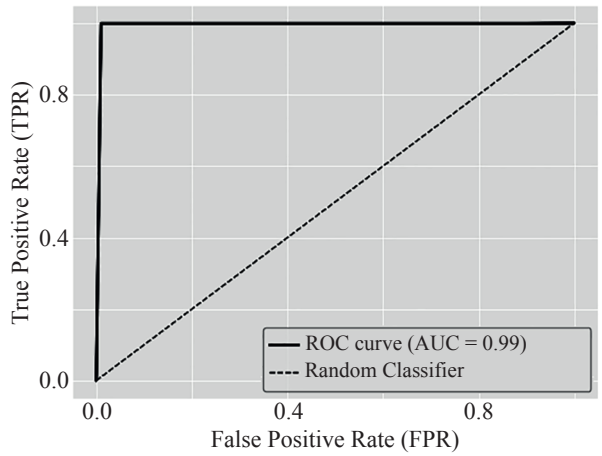

Fig. 11. Predicted samples from authentication (CNN) model

Conclusion

The proposed methodology introduces a significant advancement in Electrocardiogram (ECG)-based biometric systems for real-time authentication in IoT telehealth applications. By integrating a Siamese Neural Network for verification and a Convolutional Neural Networks for authentication, this hybrid approach enhances system reliability, security, and adaptability. Unique biometric signatures, resistant to replication or theft, offer superior security compared to traditional methods.

Separating authentication and verification models provides flexibility, scalability, and optimized performance across diverse scenarios. Lightweight models suit resource-

constrained settings, while advanced models cater to high-security environments. This modularity minimizes errors, supports targeted optimization, and facilitates continuous improvement.

Future research could explore handling noisy ECG signals, integrating multi-modal biometrics, implementing wearable sensors, and applying the model to secure governmental or military domains. Another key direction involves leveraging the two separate models for solving Open-Set Recognition challenges, ensuring accurate identification of known users while effectively rejecting unfamiliar subjects. Testing on a large ECG dataset demonstrated high accuracy, leveraging preprocessing techniques like filtering and normalization. Advanced architectures and expanded applications to other physiological signals, such as photoplethysmography and electroencephalography, could further enhance the model versatility.

References

1. Suran Melissa. Increased use of medicare telehealth during the pandemic. *JAMA*, 2022, vol. 327, no. 4, pp. 313. https://doi.org/10.1001/jama.2021.23332
2. Marquez G., Astudillo H., Taramasco C. Security in telehealth systems from a software engineering viewpoint: a systematic mapping study. *IEEE Access*, 2020, vol. 8, pp. 10933–10950. https://doi.org/10.1109/access.2020.2964988
3. Watzlaf V.J.M., Zhou L., DeAlmeida D., Hartman L.M. A systematic review of research studies examining telehealth privacy and security practices used by healthcare providers. *International Journal of Telerehabilitation*, 2017, vol. 9, no. 2, pp. 39–59. https://doi.org/10.5195/IJT.2017.6231
4. Yousuf T., Mahmoud R., Aloul F., Zualkernan I. Internet of Things (IoT) Security: current status, challenges and countermeasures. *International Journal for Information Security Research*, 2015, vol. 5, no. 4, pp. 608–616. https://doi.org/10.20533/ijisr.2042.4639.2015.0070
5. Zhou L., Thieret R., Watzlaf V., Fahima., Dealmeida D., Parmanto B. A telehealth privacy and security self-assessment questionnaire for telehealth providers: development and validation. *International Journal of Telerehabilitation*, 2019, vol. 11, no. 1, pp. 3–14. https://doi.org/10.5195/ijt.2019.6276
6. Sodhro A.H., Sennersten C., Ahmad A. Towards cognitive authentication for smart healthcare applications. *Sensors*, 2022, vol. 22, no. 6, pp. 2101. https://doi.org/10.3390/s22062101
7. Khan H., Jan Z.H., Ullah I., Alwabli A., Alharbi F., Habib S., Islam M., Shin B.J., Lee M.Y., Koo J. A deep dive into AI integration and advanced nanobiosensor technologies for enhanced bacterial infection monitoring. *Nanotechnology Reviews*, 2024, vol. 13, no. 1, pp. 20240056. https://doi.org/10.1515/ntrev-2024-0056
8. Barros A., Rosário D., Resque P., Cerqueira E. Heart of IoT: ECG as biometric sign for authentication and identification. *Proc. of the 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019, pp. 307–312. https://doi.org/10.1109/iwcmc.2019.8766495
9. Kim S.-K., Yeun C.Y., Damiani E., Lo N.W. A machine learning framework for biometric authentication using electrocardiogram. *IEEE Access*, 2019, vol. 7, pp. 94858–94868. https://doi.org/10.1109/access.2019.2927079
10. Rehman I.U., Ullah I., Khan H., Guellil M.S., Koo J., Min J., Habib S., Islam M., Lee M.Y. A comprehensive systematic literature review of ML in nanotechnology for sustainable development. *Nanotechnology Reviews*, 2024, vol. 13, no. 1, pp. 20240069. https://doi.org/10.1515/ntrev-2024-0069
11. Ibtehaz N., Chowdhury M.E.H., Khandakar A., Kiranyaz S., Rahman M.S., Tahir A., Qiblawey Y., Rahman T. EDITH: ECG biometrics aided by deep learning for reliable individual authentication. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2022, vol. 6, no. 4, pp. 928–940. https://doi.org/10.1109/tetci.2021.3131374
12. Asadifam S., Talebi M.J., Nikougoftar E. ECG-based authentication systems: a comprehensive and systematic review. *Multimedia Tools and Applications*, 2024, vol. 82, no. 9, pp. 27647–27701. https://doi.org/10.1007/s11042-023-16506-3
13. Shdefat, A.Y., Mostafa, N., Saker, I., Topcu, A. 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*, 2021. vol. 9, no. 2, pp. 394–416. https://doi.org/10.52549/ijeei.v9i2.2890
14. Li L., Chen C., Pan L., Zhang L.Y., Wang Z.F., Zhang J., Xiang Y. A survey of PPG's application in authentication. *Computers & Security*,

Литература

1. Suran Melissa. Increased use of medicare telehealth during the pandemic // JAMA. 2022. V. 327. N 4. P. 313. https://doi.org/10.1001/jama.2021.23332
2. Marquez G., Astudillo H., Taramasco C. Security in telehealth systems from a software engineering viewpoint: a systematic mapping study // IEEE Access. 2020. V. 8. P. 10933–10950. https://doi.org/10.1109/access.2020.2964988
3. Watzlaf V.J.M., Zhou L., DeAlmeida D., Hartman L.M. A systematic review of research studies examining telehealth privacy and security practices used by healthcare providers // International Journal of Telerehabilitation. 2017. V. 9. N 2. P. 39–59. https://doi.org/10.5195/IJT.2017.6231
4. Yousuf T., Mahmoud R., Aloul F., Zualkernan I. Internet of Things (IoT) Security: current status, challenges and countermeasures // International Journal for Information Security Research. 2015. V. 5. N 4. P. 608–616. https://doi.org/10.20533/ijisr.2042.4639.2015.0070
5. Zhou L., Thieret R., Watzlaf V., Fahima., Dealmeida D., Parmanto B. A telehealth privacy and security self-assessment questionnaire for telehealth providers: development and validation // International Journal of Telerehabilitation. 2019. V. 11. N 1. P. 3–14. https://doi.org/10.5195/ijt.2019.6276
6. Sodhro A.H., Sennersten C., Ahmad A. Towards cognitive authentication for smart healthcare applications // Sensors. 2022. V. 22. N 6. P. 2101. https://doi.org/10.3390/s22062101
7. Khan H., Jan Z.H., Ullah I., Alwabli A., Alharbi F., Habib S., Islam M., Shin B.J., Lee M.Y., Koo J. A deep dive into AI integration and advanced nanobiosensor technologies for enhanced bacterial infection monitoring // Nanotechnology Reviews. 2024. V. 13. N 1. P. 20240056. https://doi.org/10.1515/ntrev-2024-0056
8. Barros A., Rosário D., Resque P., Cerqueira E. Heart of IoT: ECG as biometric sign for authentication and identification // Proc. of the 15th International Wireless Communications & Mobile Computing Conference (IWCMC). 2019. P. 307–312. https://doi.org/10.1109/iwcmc.2019.8766495
9. Kim S.-K., Yeun C.Y., Damiani E., Lo N.W. A machine learning framework for biometric authentication using electrocardiogram // IEEE Access. 2019. V. 7. P. 94858–94868. https://doi.org/10.1109/access.2019.2927079
10. Rehman I.U., Ullah I., Khan H., Guellil M.S., Koo J., Min J., Habib S., Islam M., Lee M.Y. A comprehensive systematic literature review of ML in nanotechnology for sustainable development // Nanotechnology Reviews. 2024. V. 13. N 1. P. 20240069. https://doi.org/10.1515/ntrev-2024-0069
11. Ibtehaz N., Chowdhury M.E.H., Khandakar A., Kiranyaz S., Rahman M.S., Tahir A., Qiblawey Y., Rahman T. EDITH: ECG biometrics aided by deep learning for reliable individual authentication // IEEE Transactions on Emerging Topics in Computational Intelligence. 2022. V. 6. N 4. P. 928–940. https://doi.org/10.1109/tetci.2021.3131374
12. Asadifam S., Talebi M.J., Nikougoftar E. ECG-based authentication systems: a comprehensive and systematic review // Multimedia Tools and Applications. 2024. V. 82. N 9. P. 27647–27701. https://doi.org/10.1007/s11042-023-16506-3
13. Shdefat, A.Y., Mostafa, N., Saker, I., Topcu, A. 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. 2021. V. 9. N 2. P. 394–416. https://doi.org/10.52549/ijeei.v9i2.2890
14. Li L., Chen C., Pan L., Zhang L.Y., Wang Z.F., Zhang J., Xiang Y. A survey of PPG's application in authentication // Computers &

2023, vol. 135, pp. 103488. https://doi.org/10.1016/j.cose.2023.103488
15. Pereira T.M.C., Conceição R.C., Sencadas V., Sebastião R. Biometric recognition: a systematic review on electrocardiogram data acquisition methods. *Sensors*, 2023, vol. 23, no. 3, pp. 1507. https://doi.org/10.3390/s23031507
16. Hammad M., Plawiak P., Wang K.Q., Acharya U.R. ResNet-Attention model for human authentication using ECG signals. *Expert Systems*, 2021, vol. 38, no. 6, pp. e12547. https://doi.org/10.1111/exsy.12547
17. Labati R.D., Muñoz E., Piuri V., Sassi R., Scotti F. Deep-ECG: convolutional neural networks for ECG biometric recognition. *Pattern Recognition Letters*, 2019, vol. 126, pp. 78–85. https://doi.org/10.1016/j.patrec.2018.03.028
18. Tirado-Martín P., Sanchez-Rello R. BioEcg: Improving ECG biometrics with deep learning and enhanced datasets. *Applied Sciences*, 2021, vol. 11, no. 13, pp. 5880. https://doi.org/10.3390/app11135880
19. D'angelis O., Bacco L., Vollero L., Merone M. Advancing ECG biometrics through vision transformers: a confidence-driven approach. *IEEE Access*, 2023, vol. 11, pp. 140710–140721. https://doi.org/10.1109/ACCESS.2023.3338191
20. Alduwaile D., Islam M.S. Single heartbeat ECG biometric recognition using convolutional neural network. *Proc. of the International Conference on Advanced Science and Engineering (ICOASE)*, 2020, pp. 145–150. https://doi.org/10.1109/ICOASE51841.2020.9436592
21. Ivanciu L., Ivanciu I.A., Farago P., Roman M., Hintea S. An ECG-based authentication system using siamese neural networks. *Journal of Medical and Biological Engineering*, 2021, vol. 41, no. 4, pp. 558–570. https://doi.org/10.1007/s40846-021-00637-9
22. Albuquerque S.L., Misoso C.J., da Rocha A.F., Gondim P.R.L. Authentication based on electrocardiography signals and machine learning. *Engineering Research Express*, 2021, vol. 3, no. 2, pp. 023504. https://doi.org/10.1088/2631-8695/abffa6
23. Al Alkeem, E., Yeun C.Y., Yun J., Yoo P.D., Chae M., Rahman A., Asyhari A.T. Robust deep identification using ECG and multimodal biometrics for industrial internet of things. *Ad Hoc Networks*, 2021, vol. 121, pp. 102581. https://doi.org/10.1016/j.adhoc.2021.102581
24. Ahmad I., Yao C., Li L., Chen Y., Liu Z., Ullah I., Shabaz M., Wang X., Huang K., Li G., Zhao G., Samuel O.W., Chen S. An efficient feature selection and explainable classification method for EEG-based epileptic seizure detection. *Journal of Information Security and Applications*, 2024, vol. 80, pp. 103654. https://doi.org/10.1016/j.jisa.2023.103654
25. Jamin A., Humeau-Heurtier A. (Multiscale) cross-entropy methods: a review. *Entropy*, 2019, vol. 22, no. 1, pp. 45. https://doi.org/10.3390/e22010045
26. Domínguez-Bolaño T., Campos O., Barral V., Escudero C.J., García-Naya J.A. An overview of IoT architectures, technologies, and existing open-source projects. *Internet of Things*, 2022, vol. 20, pp. 100626. https://doi.org/10.1016/j.iot.2022.100626
27. Pourghebleh B., Wakil K., Navimipour N.J. A comprehensive study on the trust management techniques in the Internet of Things. *IEEE Internet of Things Journal*, 2019, vol. 6, no. 6, pp. 9626–9337. https://doi.org/10.1109/jiot.2019.2933518
28. Sharma P., Jain S., Gupta S., Chamola V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Networks*, 2021, vol. 123, pp. 102685. https://doi.org/10.1016/j.adhoc.2021.102685
29. Dogo E.M., Afolabi O.J., Nwulu N.I., Twala B., Aigbavboa C.O. A comparative analysis of gradient descent-based optimization algorithms on convolutional neural networks. *Proc. of the International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, 2018, pp. 92–99. https://doi.org/10.1109/ctems.2018.8769211
30. Tyagi P.K., Agrawal D. Automatic detection of sleep apnea from single-lead ECG signal using enhanced-deep belief network model. *Biomedical Signal Processing and Control*, 2023, vol. 80, part 2, pp. 104401. https://doi.org/10.1016/j.bspc.2022.104401
31. Bento N., Belo D., Gamboa H. ECG biometrics using spectrograms and deep neural networks. *International Journal of Machine Learning and Computing*, 2020, vol. 10, no. 2, pp. 259–264. https://doi.org/10.18178/ijmlc.2020.10.2.929
32. Zhou D.-X. Deep distributed convolutional neural networks: Universality. *Analysis and Applications*, 2018, vol. 16, no. 6, pp. 895–919. https://doi.org/10.1142/s0219530518500124

Security. 2023. V. 135. P. 103488. https://doi.org/10.1016/j.cose.2023.103488
15. Pereira T.M.C., Conceição R.C., Sencadas V., Sebastião R. Biometric recognition: a systematic review on electrocardiogram data acquisition methods // Sensors. 2023. V. 23. N 3. P. 1507. https://doi.org/10.3390/s23031507
16. Hammad M., Plawiak P., Wang K.Q., Acharya U.R. ResNet-Attention model for human authentication using ECG signals // Expert Systems. 2021. V. 38. N 6. P. e12547. https://doi.org/10.1111/exsy.12547
17. Labati R.D., Muñoz E., Piuri V., Sassi R., Scotti F. Deep-ECG: convolutional neural networks for ECG biometric recognition // Pattern Recognition Letters. 2019. V. 126. P. 78–85. https://doi.org/10.1016/j.patrec.2018.03.028
18. Tirado-Martín P., Sanchez-Rello R. BioEcg: Improving ECG biometrics with deep learning and enhanced datasets // Applied Sciences. 2021. V. 11. N 13. P. 5880. https://doi.org/10.3390/app11135880
19. D'angelis O., Bacco L., Vollero L., Merone M. Advancing ECG biometrics through vision transformers: a confidence-driven approach // IEEE Access. 2023. V. 11. P. 140710–140721. https://doi.org/10.1109/ACCESS.2023.3338191
20. Alduwaile D., Islam M.S. Single heartbeat ECG biometric recognition using convolutional neural network // Proc. of the International Conference on Advanced Science and Engineering (ICOASE). 2020. P. 145–150. https://doi.org/10.1109/ICOASE51841.2020.9436592
21. Ivanciu L., Ivanciu I.A., Farago P., Roman M., Hintea S. An ECG-based authentication system using siamese neural networks // Journal of Medical and Biological Engineering. 2021. V. 41. N 4. P. 558–570. https://doi.org/10.1007/s40846-021-00637-9
22. Albuquerque S.L., Misoso C.J., da Rocha A.F., Gondim P.R.L. Authentication based on electrocardiography signals and machine learning // Engineering Research Express. 2021. V. 3. N 2. P. 023504. https://doi.org/10.1088/2631-8695/abffa6
23. Al Alkeem, E., Yeun C.Y., Yun J., Yoo P.D., Chae M., Rahman A., Asyhari A.T. Robust deep identification using ECG and multimodal biometrics for industrial internet of things // Ad Hoc Networks, 2021, V. 121. P. 102581. https://doi.org/10.1016/j.adhoc.2021.102581
24. Ahmad I., Yao C., Li L., Chen Y., Liu Z., Ullah I., Shabaz M., Wang X., Huang K., Li G., Zhao G., Samuel O.W., Chen S. An efficient feature selection and explainable classification method for EEG-based epileptic seizure detection // Journal of Information Security and Applications. 2024. V. 80. P. 103654. https://doi.org/10.1016/j.jisa.2023.103654
25. Jamin A., Humeau-Heurtier A. (Multiscale) cross-entropy methods: a review // Entropy. 2019. V. 22. N 1. P. 45. https://doi.org/10.3390/e22010045
26. Domínguez-Bolaño T., Campos O., Barral V., Escudero C.J., García-Naya J.A. An overview of IoT architectures, technologies, and existing open-source projects // Internet of Things. 2022. V. 20. P. 100626. https://doi.org/10.1016/j.iot.2022.100626
27. Pourghebleh B., Wakil K., Navimipour N.J. A comprehensive study on the trust management techniques in the Internet of Things // IEEE Internet of Things Journal. 2019. V. 6. N 6. P. 9626–9337. https://doi.org/10.1109/jiot.2019.2933518
28. Sharma P., Jain S., Gupta S., Chamola V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications // Ad Hoc Networks. 2021. V. 123. P. 102685. https://doi.org/10.1016/j.adhoc.2021.102685
29. Dogo E.M., Afolabi O.J., Nwulu N.I., Twala B., Aigbavboa C.O. A comparative analysis of gradient descent-based optimization algorithms on convolutional neural networks // Proc. of the International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS). 2018. P. 92–99. https://doi.org/10.1109/ctems.2018.8769211
30. Tyagi P.K., Agrawal D. Automatic detection of sleep apnea from single-lead ECG signal using enhanced-deep belief network model // Biomedical Signal Processing and Control. 2023. V. 80. Part 2. P. 104401. https://doi.org/10.1016/j.bspc.2022.104401
31. Bento N., Belo D., Gamboa H. ECG biometrics using spectrograms and deep neural networks // International Journal of Machine Learning and Computing. 2020. V. 10. N 2. P. 259–264. https://doi.org/10.18178/ijmlc.2020.10.2.929
32. Zhou D.-X. Deep distributed convolutional neural networks: Universality // Analysis and Applications. 2018. V. 16. N 6. P. 895–919. https://doi.org/10.1142/s0219530518500124

33. Sainath T.N., Kingsbury B., Saon G., Soltau H., Mohamed A.R., Dahl G., Ramabhadran B. Deep convolutional neural networks for Large-scale speech tasks. *Neural Networks*, 2015, vol. 64, pp. 39–48. https://doi.org/10.1016/j.neunet.2014.08.005
34. Khan A., Sohail A., Zahoora U., Qureshi A.S. A survey of the recent architectures of deep convolutional neural networks. *Artificial Intelligence Review*, 2020, vol. 53, no. 8, pp. 5455–5516. https://doi.org/10.1007/s10462-020-09825-6
35. Lodhi B., Kang J. Multipath-DenseNet: A Supervised ensemble architecture of densely connected convolutional networks. *Information Sciences*, 2019, vol. 482, pp. 63–72. https://doi.org/10.1016/j.ins.2019.01.012
36. Kanatov M., Atymtayeva L., Mendes M. Improved Facial Expression Recognition with xception deep net and preprocessed images. *Applied Mathematics & Information Sciences*, 2019, vol. 13, no. 5, pp. 859–865. https://doi.org/10.18576/amis/130520
37. Zhang Y., Wu J. Practical human authentication method based on piecewise corrected Electrocardiogram. *Proc. of the 7th IEEE International Conference on Software Engineering and Service Sciences (ICSESS)*, 2016, pp. 300–303. https://doi.org/10.1109/icsess.2016.7883071
38. Nwankpa C., Ijomah W., Gachagan A., Marshall S. Activation Functions: Comparison of Trends in Practice and Research for Deep Learning. *arXiv*, 2018, arxiv.org/abs/1811.03378v1. https://doi.org/10.48550/arXiv.1811.03378
39. Barros A., Resque P., Almeida J., Mota R., Oliveira H., Rosário D., Cerqueira E. Data improvement model based on ECG biometric for user authentication and identification. *Sensors*, 2020, vol. 20, no. 10, pp. 2920. https://doi.org/10.3390/s20102920
40. Su K., Yang G., Wu B., Yang L., Li D., Su P., Yin Y. Human identification using finger vein and ECG signals. *Neurocomputing*, 2019, vol. 332, pp. 111–118. https://doi.org/10.1016/j.neucom.2018.12.015
41. Zhao Z., Zhang Y., Deng Y., Zhang X. ECG authentication system design incorporating a convolutional neural network and generalized S-Transformation. *Computers in Biology and Medicine*, 2018, vol. 102, pp. 168–179. https://doi.org/10.1016/j.compbiomed.2018.09.027
42. Blasco J., Peris-Lopez P. On the feasibility of low-cost wearable Sensors for multi-modal biometric verification. *Sensors*, 2018, vol. 18, no. 9, pp. 2782. https://doi.org/10.3390/s18092782
43. Agrawal V., Hazratifard M., Elmiligi H., Gebali F. Electrocardiogram (ECG)-based user authentication using deep learning algorithms. *Diagnostics*, 2023, vol. 13, no. 3, pp. 439. https://doi.org/10.3390/diagnostics13030439

33. Sainath T.N., Kingsbury B., Saon G., Soltau H., Mohamed A.R., Dahl G., Ramabhadran B. Deep convolutional neural networks for Large-scale speech tasks // Neural Networks. 2015. V. 64. P. 39–48. https://doi.org/10.1016/j.neunet.2014.08.005
34. Khan A., Sohail A., Zahoora U., Qureshi A.S. A survey of the recent architectures of deep convolutional neural networks // Artificial Intelligence Review. 2020. V. 53. N 8. P. 5455–5516 https://doi.org/10.1007/s10462-020-09825-6
35. Lodhi B., Kang J. Multipath-DenseNet: A Supervised ensemble architecture of densely connected convolutional networks // Information Sciences. 2019. V. 482. P. 63–72. https://doi.org/10.1016/j.ins.2019.01.012
36. Kanatov M., Atymtayeva L., Mendes M. Improved Facial Expression Recognition with xception deep net and preprocessed images // Applied Mathematics & Information Sciences. 2019. V. 13. N 5. P. 859–865. https://doi.org/10.18576/amis/130520
37. Zhang Y., Wu J. Practical human authentication method based on piecewise corrected Electrocardiogram // Proc. of the 7th IEEE International Conference on Software Engineering and Service Sciences (ICSESS). 2016. P. 300–303. https://doi.org/10.1109/icsess.2016.7883071
38. Nwankpa C., Ijomah W., Gachagan A., Marshall S. Activation Functions: Comparison of Trends in Practice and Research for Deep Learning // arXiv. 2018. arxiv.org/abs/1811.03378v1. https://doi.org/10.48550/arXiv.1811.03378
39. Barros A., Resque P., Almeida J., Mota R., Oliveira H., Rosário D., Cerqueira E. Data improvement model based on ECG biometric for user authentication and identification // Sensors. 2020. V. 20. N 10. P. 2920. https://doi.org/10.3390/s20102920
40. Su K., Yang G., Wu B., Yang L., Li D., Su P., Yin Y. Human identification using finger vein and ECG signals // Neurocomputing. 2019. V. 332. P. 111–118. https://doi.org/10.1016/j.neucom.2018.12.015
41. Zhao Z., Zhang Y., Deng Y., Zhang X. ECG authentication system design incorporating a convolutional neural network and generalized S-Transformation // Computers in Biology and Medicine. 2018. V. 102. P. 168–179. https://doi.org/10.1016/j.compbiomed.2018.09.027
42. Blasco J., Peris-Lopez P. On the feasibility of low-cost wearable Sensors for multi-modal biometric verification // Sensors. 2018. V. 18. N 9. P. 2782. https://doi.org/10.3390/s18092782
43. Agrawal V., Hazratifard M., Elmiligi H., Gebali F. Electrocardiogram (ECG)-based user authentication using deep learning algorithms // Diagnostics. 2023. V. 13. N 3. P. 439. https://doi.org/10.3390/diagnostics13030439

Author

Mohamed Abdalla Elsayed Azab — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0009-0000-1748-0029, mohamed.a.azab@itmo.ru

Автор

Азаб Мохамед Абдалла Эльсейд — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0009-0000-1748-0029, mohamed.a.azab@itmo.ru

Received 14.12.2024
Approved after reviewing 30.04.2025
Accepted 26.05.2025

Статья поступила в редакцию 14.12.2024
Одобрена после рецензирования 30.04.2025
Принята к печати 26.05.2025