RES MILITARIS Social Science Journal

SECURING IOT CONFIGURATIONS WITH END-TO-END DATA AUTHENTICATION VIA DEEP LEARNING

[1]Dr P.Veeresh,[2]M.Rajeswaraiah
[1]Professor & HOD,[2]Assistant Professor
Department Of ECE
St. Johns College of Engineering & Technology, Errakota, Yemmiganur

Abstract

Electrocardiograms (ECGs) are widely accepted as a reliable method for verifying the presence of life in many security applications, particularly in new and developing technologies, when compared to other biometric methods. Our work exploits this crucial characteristic to enhance existing machine and deep learning ECG authentication solutions by using edge computing servers that provide connectivity to Internet of Things (IoT) devices while retaining access to computational and storage resources. In our proposed technique, we integrate the preprocessing, feature extraction, and classification routines into a single unit. We directly input individual ECG signals from the database into a convolutional neural network (CNN) model, which then classifies them as either accepted or rejected. In addition, we customize our authentication system to be cost-effective and prioritize minimizing latency, making it well-suited for applications on edge computing platforms. In order to verify the effectiveness of our proposed model, we tested it on standard ECG signals from the Physikalisch-Technische Bundesanstalt (PTB) database. The results showed accuracy, precision, recall, and F1-score rates of 99.50%, 99.73%, 100%, and 99.78% respectively. These high rates demonstrate the suitability of our technique for use in real-time authentication systems. In addition, we include insights on the model's performance compared to newer approaches that are based on conventional machine and deep learning methods.

Keywords: Deep Learning, Biometric Authentication, Electrocardiogram (ECG), Information Security, Internet of Things (IoT), Edge Computing, Industrial Data Integration

1. Introduction

In recent times, the rise in counterfeiting cases has led to a decrease in the effectiveness of conventional authentication techniques such security tokens, passwords, personal identification numbers (PINs), and so on. Currently, biometric authentication is widely used instead. However, typical biometric markers like fingerprints, face recognition, iris recognition, and ear recognition may be affected by several parameters such as universality, uniqueness, performance, measurability, acceptability, circumvention, etc. [1]. Unlike conventional biometric modalities like fingerprints, electrocardiogram (ECG) signals may be used as biometric markers to test for animateness. This is because ECG signals give a reliable measure of consciousness, making them a good balance in terms of accuracy and reliability.

An electrocardiogram (ECG) is used to assess the cardiac rhythm, which represents the movement of blood into and out of the heart [2]. Currently, there has been a reduction in the size of ECG sensors, making it more convenient to include them into wearable devices and linked cars [3]. Furthermore, the widespread use and practicality of ECGs in many sectors may be due to their modest computational requirements and compact template size [4, 5]. These features are used in [6] to securely identify drivers and passengers in vehicle access control.

Meanwhile, the electrocardiogram (ECG) is crucial in diagnosing a range of cardiac diseases, such as arrhythmias and coronary problems. An ECG signal consists of a P-wave, a QRS-complex, and a T-wave, which together make up a typical cardiac cycle [2]. Furthermore, there are three crucial parts or intervals referred to as ST-segment or ST-interval, PR-segment or PR-interval, and QT-interval. The P-wave represents the atrial depolarization resulting from atrial contraction, whereas the QRS-complex component indicates the ventricular depolarization or contraction. Subsequently, both ventricles return to a state of relaxation, referred to as the T-wave [7]. The PR-interval, sometimes referred to as the PR-segment, represents the duration between the onset of the P-wave and the Q-wave. On the other hand, the

QT-interval represents the duration between the starting point of the QRS-complex and the T-wave. The ST-interval, often referred to as the ST-segment, represents the line connecting the S-wave and T-wave. Figure 1 depicts a standard electrocardiogram (ECG) signal together with its peaks and intervals. These attributes have been used in many applications, including enhancing security in body-area network sensors (BANs) like smart wristbands and cardiac pacemakers. The user's text is "[8]".

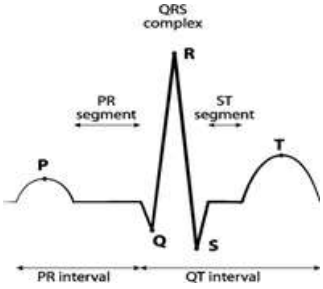

Fig. 1. Illustration of all peaks and intervals on an ECG signal [20].

Lately, there has been an upsurge in the use of these signals in applications across different medical Internet of Things (IoT) platforms [9]. However, there is still a shortage of such applications using ECG for authentication [10]. Meanwhile, whereas cloud computing approaches are more widespread for handling IoT applications, they are known to suffer from high latency to applications, impact of considerable traffic overhead, etc., all of which are detrimental to real-time and delay-sensitive applications [11]. Unlike these past efforts, our study presents a deep learning-based ECG authentication approach for edge computing platforms where, unlike in IoT, cloud resources and services are moved to edge nodes [12].

Broadly speaking, previous studies on ECG-based authentication can be classified as either conventional machine learning techniques [13–16] or deep learning-based approaches [17–23]. In the former, the ECG signals pass through many steps (typically for preprocessing of the ECG data, extracting and selecting the ECG features and classification) before the authentication is accomplished. These steps complicate and overburden the targeted authentication process. Moreover, most of these approaches reported below-par authentication performance when working on other databases as well as when evaluated on larger datasets that overfitting had been reported [13–16].

To overcome these limitations, we propose a deep learning model (DLM) approach to human authentication system using ECG signals. As one of its many upsides, DLM techniques subsume many of the earlier mentioned steps of traditional machine learning approaches. Deep learning is a class of machine learning where networks are capable of unsupervised learning from unstructured or unlabeled data. These networks facilitate the gradual extraction of higher-level features from raw input data. The most widespread used DLM method, known as convolutional neural network (CNN), has its origins and best performance in image analysis [24]. Recently, CNN-based DLMs have become popular across many fields including medicine [25–28], computer vision [29–32], remote sensing [33, 34], and many other interesting applications [35–38].

To encapsulate, whereas the use of DLMs in biometric authentication, particularly CNN [39] is not new, very few of these methods are based on ECG authentication [17–23]. Even so, they are encumbered by the following shortcomings.

- Temporal and resource overhead associated with the need for preprocessing, segmentation and, QRS detection stages (as in [13–16]).
- Sensitivity to quality of ECG signals (as in [17–19]).
- Need for a separate classifier for authentication, which complicates the already complex process [20–23].

- Working on more than one lead ECG, which imposes additional hardware susceptibility (as in [17, 20]).

To ameliorate the enumerated deficiencies of both the machine and deep learning approaches, our proposed method presents the following contributions.

- An efficient CNN-based DLM is proposed to automatically authenticate the ECG signals for efficient identity validation.
- Since ECG data suffer from various noise artifacts due to unconstrained signaling environments and considering the challenges of collecting all in one environment, this study employs an end-to-end DLM to eliminate the need for a preprocessing stage.
- An edge-computing framework is integrated into the proposed model as a cost-efficient remedy to lower latency wherein storage and processing capabilities are provided at the edge of the radio access network that is in close proximity to mobile users. Consequently, our strategy facilitates real-time and delay-sensitive applications for execution.

As noted earlier, there has been a recent surge in the integration of IoT and wireless technologies into a wide range of systems such as healthcare, pattern recognition, industry [39–41]. These devices including sensors are infused in automatic car tracking adapters, Google Glass, blood glucose monitors, ECGs, continuous glucose monitors, oximeters, insulin pens, temperature monitors, etc. Correspondingly, numerous applications and multimedia services that require supplementary computations and high data communication are increasing rapidly. Nevertheless, these applications are still resource-limited with restricted computational power and energy. Edge computing, which is described as a network architecture that provides computing and data storage at edge server nodes [12], is considered a solution that can address the limitations of individual devices. Moreover, it is known to offer lower latency and high bandwidth [12], which supports its implementation in real-time applications. Consequently, computationally intensive services of IoT devices can be offloaded and executed on this server through a wireless channel. This will mitigate the load demand while also helping to extend battery life [12].

Our study advances previous machine and deep learning ECG authentication efforts by leveraging the use of edge computing servers that can be connected to IoT devices while maintaining access to computational and storage resources. Fig. 2 illustrates the integration of ECG authentication in a car control system which is considered a daily life application. First, the user's ECG signal is acquired and sent to the edge computing server through mobile devices where the proposed model is trained, and relevant data are stored. Next, if the user is authenticated, the edge server will send an automated signal to the car sensor which transfers further control to the user. Otherwise, the edge server will reject the user's request and subsequently alert appropriate authorities to prevent the vehicle from being stolen. Therefore, the overall performance of these systems is improved since computationally-intensive operations of the model are processed at the edge server. Table 1 presents a definition of parameters used in this example and subsequent sections of this study.

Fig. 2. Integration of ECG authentication in a car control system.

The rest of this paper is structured as follows. In Section 2, we present the outline and other details of our proposed CNN model whose validation via a range of performance evaluation experiments are presented in Section 3. These results are subsequently analyzed and discussed alongside related work in Sections 4 and 5, respectively.

Table 1. Definition of parameters

Parameter	Definition
N	Element number or the number of sets applied in the 5-fold
x	Signal
f	Filter in the input signal (*x*)
P	Precision
R	Recall
EER	Equal error rate
ROC	Receiver operating characteristic
F1	F1-score
FP	False positive
FN	False negative
TP	True positive
TN	True negative
M	Number of classes

2. Related Works

As highlighted in our introduction, previous studies on ECG-based authentication can be broadly classified as either classical machine learning (CLM)-based techniques [13–16, 42] or DLM-based approaches [17–23, 43–47]. This section provides an overview of recent studies in both categories.

2.1 Classical Machine Learning-based Techniques

Classical machine learning (CLM) refers to techniques that pass through all steps of the machine learning pipeline [48]. In this kind of system, the ECG signals pass through many steps before the authentication is accomplished. The first stage entails removal of noise and other artifacts while also enhancing the input ECG signals in order to make them suitable for further processing. This step is usually called the preprocessing step. The second step is focused on extracting and selecting the prominent features from the preprocessed ECG signal. These features should be unique for each signal and this step is called feature extraction step. Finally, the features are fed into the classifier in the classification step where the authentication is done.

Most CLM techniques adopt basic frameworks outlined above. For instance, in [13], the authors introduced a feature extraction and a continuous authentication method by proposing one-dimensional multi-resolution local binary patterns (1DMRLBP) and sequential sampling feature extraction for one-dimensional signals. This system updates decision thresholds and sample sizes during run-time. As reported in [13], it accounts for the quantization error needed to tolerate noise and extracts local and global signal morphology. For validation, the authors reported using data from 290 subjects from the Physikalisch-Technische Bundesanstalt (PTB) database and recorded an equal error rate (EER) of

10.10% for ECG signal authentication. Similarly, Safi et al. [14], presented a feature extraction approach that they called pulse active ratio (PAR) for ECG-based authentication using ECG fiducial points as a feature vector. In this scheme, each feature vector from the test dataset is compared to all feature vectors in the training database with Euclidean distance set as the similarity measurement to generate matching scores. If the feature vectors from the test and training dataset are the same, the authentication is considered successful. They reported experiments involving 112 individuals from the PTB dataset of which they reported that 98 individuals exhibited arrhythmia beats while the remainder were healthy. They also recorded an EER of 9.89 % and 19.15% for normal and arrhythmia beats, respectively. In their contribution, Goshvarpour and Goshvarpour [42], developed an expert system for human authentication based on ECG signals. They executed their authentication protocol by combining the ECG characteristics with information theoretic (IT) considerations. In the last step, using 5-fold cross-validation, they applied k-nearest neighbor (kNN) to identify individuals and reported an average accuracy of 97.6%. In their contribution, Ivanciu et al. [49], presented an ECG-system based on Siamese neural networks for authentication. They used the Siamese network to simplify the training process. In addition, they deployed the system on private cloud to ensure its security and scalability. They reported a sensitivity of 87.3% and overall accuracy of 86.47%. In [50], the authors introduced an ECG authentication system based on incremental learning to identify the ECG signal of each subject under several conditions. They employed support vector machine (SVM) for authentication and reported the best accuracy of 99.4%. Similarly, in [51], the authors presented an ECG authentication system based on nonlinear normalization according to various physiological conditions. They reported an accuracy of 99.05% and 88.14% for resting and non-resting conditions, respectively.

To conclude, we also note that despite the performance recorded, authentication performance in most of the highlighted CLM studies, are below-par when working on other databases or when assessed on large datasets, which also leads to overfitting. Exploiting their potency, nowadays, DLMs have been proposed to overcome most of the problems faced by CLM methods across different domains and applications as highlighted in the sequel.

2.2 Security Scenarios with CNN-based DLMs

Deep learning is widely regarded as the advanced solution to most machine learning problems. As reviewed earlier, most DLM are built on CNNs, and they are credited with some of the stellar performance recorded in various fields including biometric authentication. For example, in [17], the authors used CNN to deploy an authentication algorithm based on more than one ECG lead. Their algorithm recorded an EER of 1.36% for authentication using the PTB database. In [18], the authors presented a CNN-based multi-modal authentication system based on ECG and fingerprints. Their technique used a pre-trained VGG-Net model and transfer learning technique by using the output of the last fully connected layer as features for the input ECG image. Following this, an improved version of bio-hashing strategy [16] was employed to protect the features. Finally, an external classifier called Q-Gaussian multiclass support vector machine (QG-MSVM) was used for authentication. They reported an EER of 3.20% for the PTB database.

Furthermore, in [19] the authors used CNN to generate ECG features that they protected using matrix operations [16]. In the end, they employed a separate classifier (QG-MSVM) for authentication and reported an EER of 3.5% using images in the PTB database. In another effort, Hammad et al. [20] combined machine learning features with deep learning features of ECG for human authentication using CNN. They employed scan and removal techniques to extract the ECG features and CNN for classification. They recorded an EER of 1.63% for ECG authentication. In their contribution, Chu et al. [23] used the parallel multi-scale one-dimensional residual network for ECG authentication. Specifically, in the preprocessing step, they located the R-peak and used it with the whole ECG signal to extract the

feature. After that, they used a residual network with a new loss function to extract the features and train the network. They used all records in the PTB database and reported an EER of 0.59%.

Similarly, Zhang et al. [43] presented a wavelet domain multiresolution CNN (MCNN) for ECG identification. The first step of their technique used blind segmentation to process the data and process first blind segmentation and applied an auto-correlation operation on the transformed data to remove the difference resulting from the use of randomly chosen signal segments. They reported an average identification accuracy of 93.5%. Similar to that effort, Abdeldayem and Bourlai [44], presented a human identification system based on ECGs where the input signal was segmented to enrich its original informational content. Subsequently, they generated spectral correlation images that were fed to the CNN for identification. They reported an accuracy of 95.6% with false acceptance and rejection rates of 0.2% and 0.1%, respectively. Similarly, in [45], the authors presented a CNN protocol for human identification based on ECG. They employed two CNN models, one for feature extraction and another for identification a combination that recorded an average identification accuracy of 94.3%.

In their contribution, Abd El-Rahiem and Hammad [52] presented a multi-fusion ECG authentication system based on internal deep fusion algorithm. Transfer learning technique is used to extract the deep features of ECG signals in this system. After that, they used SVM as a separate classifier for authentication and reported final authentication accuracy of 99.4%. Finally, AlDuwaile and Islam [53] employed CNN and a single heartbeat to develop an ECG recognition system. They reported accuracy of 99.90%, 98.20%, and 94.18% for different databases. Unlike most of the enumerated DLMs, our proposed approach is built on an end-to-end structure that eliminates the need for different machine learning stages while recording better accuracy. Details of this proposed model are presented in the next section.

3. Materials and Methods

Structurally, our proposed CNN-based DLM (or simply CDM) combines the hitherto separate stages (i.e., preprocessing, feature extraction and classification) of conventional machine learning techniques into a compact unit. Like most of the studies highlighted in the previous section, ECG biometric data from the PTB database [54] was employed for all stages of this study. This dataset [54] comprises of ECG signals from 290 subjects, which are separately fed into our proposed CNN model. Finally, the proposed model classifies the acquired ECG signal as an accepted or unaccepted (i.e., rejected) class. For example, in our earlier demonstration of vehicle access control systems based on ECG authentication in Fig. 2, the system grants access depending on the identification of the driver, i.e., whether he/she is accepted as an authorized driver or not. Fig. 3 presents a general outline depicting the integration of the DLM in the ECG authentication framework

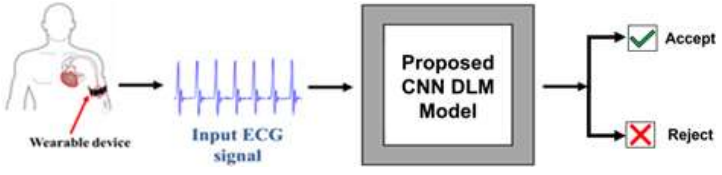

Fig. 3. Block diagram outlining implementation of the proposed model.

3.1 Dataset and Implementation Framework

As mentioned earlier, the PTB dataset [54] is used throughout this study. This is a widely used multi-session dataset made up of 549 records from 290 subjects whose ages range from 17 to 87 years of which

28% were female and 72% were male. Each subject has signal duration of between 1 to 5 records. Each recording consists of 15 measured signals: 12 regular leads and 3 Frank ECG leads with a sampling frequency of 1,000 Hz. The specifications of the PTB recorder are as follows:

- ±16 mV as an input voltage with 16 input channels and 100 Ω input resistance
- 16-bit resolution with 0 to 1 kHz bandwidth.
- Maximum noise voltage of 10 μV (pp).
- The noise level recording during signal collection. Furthermore, the diagnostic classes of the subjects in the dataset are summarized in Table 2 [54].

Additionally, we used two-second Lead II ECG signals made up of 2,000 sample pulses in total. Finally, we normalized each record using Z-score normalization with standard deviation and mean set at 1 and 0, respectively.

Results emanating from the implementation of our proposed model are compared alongside standard studies published in the literature as reported later in Section 4 and discussed in Section 5.

Table 2. PTB classes

Class	Number of subjects
Myocardial infarction	148
Myocardial hypertrophy	7
Myocarditis	4
Heart failure	18
Dysrhythmia	14
Bundle branch block	15
Valvular heart disease	6
Miscellaneous	4

3.2 Proposed CNN-based Deep Learning Model

CNN has been credited for the remarkable success of DLMs. Since its debut for applications in pattern recognition and computer vision, it has been deployed in numerous fields, including biometrics, authentication, etc. Typically, a CNN consists of different layers: convolutional, fully connected, and pooling. The convolutional layer is used to extract features from the input that are fed into the pooling layer where some parameters may be reduced. Finally, the fully connected layer converts the features matrix to a vector and combined, these features together to create a model.

Fig. 4 depicts details of the CNN architecture for our proposed model comprising of five convolution processes that consist of three maxpooling, three dropout, two fully connected layers as well as a softmax layer that is employed in the authentication stage, whose output is the final decision, i.e., accept or reject.

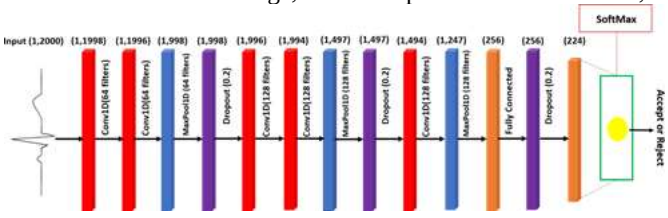

Fig. 4. CNN operation of the proposed model.

Probing further, we now note that in our model, each ECG record (with 2,000 samples) is fed to our network for training and testing. The proposed CNN model comprises of five 1D convolutional layers that are actuated using a rectified linear unit (ReLU) activation function [54] and three maxpooling layers

that are followed by two fully connected layers and a softmax activation function, which is used to transform the outputs of the classifier into probabilities for each class of the two classes (i.e., accept or reject). In accomplishing this, the convolution operation is executed using (1).

$$Y_p = \sum_{k=0}^{N-1} x_k f(n-k) \quad (1)$$

where N, x, and f are the element number, signal, and filter in the input signal (x), respectively and the vector y represents the output signal. We start with the 1D convolutional layers with 64 filters whose size increases sequentially to 128 filters in the last layers (to extract more features from the input). The filter size is set at 3 with a step-wise stride. We also pool the output of every convolutional layer output at a stride of 2. Further, a dropout with a 0.2 probability rate is used to prevent the network from overfitting [55] by ignoring some randomly selected neurons during the training. It is noteworthy that the dropout is important in large networks that have complex fitting but few labeled samples. In addition to serving as a classifier, the fully connected layer maps the dimensions, i.e., high to low, as presented in Table 3. For authentication, we employed the softmax function defined in (2) because it is differentiable, and it optimizes the cost function, and its outcome produces the final decision as presented in Fig. 3.

$$\sigma(Z^{\rightarrow})i = \frac{e^{Z_i}}{\sum_{i=1}^{k} e^{Z_j}} \quad (2)$$

where Z_i is the input vector to the softmax function, k is the number of classes and $\sum_{j=1}^{k} e^{Zj}$ is a normalization term.

3.3 Training

Stochastic gradient descent with momentum [56] is used for training our model with a batch size of 10 samples. Furthermore, hyper-parameters comprising of weight decay, learning rate and number of epochs were set at 0.00005, 0.0001 and 100, respectively. Subsequently, these parameters were adjusted iteratively to obtain optimum performance.

Table 3. Composition of different layers of proposed model

Layer number	Layer name	Size of filter	Stride	Number of kernels	Size of output
1	Convolution	3	1	64	1998×64
2	Convolution	3	1	64	1996×64
3	Maxpooling	2	2		998×64
4	Dropout		Rate=0.2		998×64
5	Convolution	3	1	128	996×128
6	Convolution	3	1	128	994×128
7	Maxpooling	2	2		497×128
8	Dropout		Rate=0.2		497×128
9	Convolution	3	1	128	494×128
10	Maxpooling	2	2		247×128
11	Fully connected			512	256
12	Dropout		Rate=0.2		256
13	Fully connected			448	224
14	Softmax			2	2

3.4 Testing

Testing was performed after each run of the training epoch on our model. We divided the data into three parts: 60% for training, 30% for validation, and 10% for testing. Additionally, a 5-fold cross-validation approach [57] is employed for training and testing sets during authentication. In this approach, the ECG data are randomly shuffled and divided into five equally-sized subsets. After that, we ran five experiments where 90% of the data was reserved for training and validation and the remaining 10% for testing. Finally, we evaluated the final performance of the method by calculating the mean of all folds.

To ascertain the performance of our CNN model, we considered two factors: evaluating the impact of the proposed model using a 5-fold approach [57] and the authentication performance of the proposed method relative to established ECG authentication methods. Algorithm 1 outlines the execution of the above procedure while Algorithm 2 summarizes steps for the execution of the CNN model.

Algorithm 1. Execution of proposed protocol

1: **Input**: Raw input data $x = x_1, x_2, \ldots, x_n$; % with 2000 samples for each record
2: CNN ← x; % the input data are directly fed into the CNN network to retrieve the extracted feature vectors
3: $F = F_1, F_2, \ldots, F_n$; % the extracted feature vectors are mapped into high-dimensional space
4: **for** each ECG signal starting from $i = 1$ to the length of ECG signal (2000 samples)
5: **extract** CNN features → F;
6: **end for**
7: $F_{train}, F_{test}, L_{train}, L_{test} \leftarrow F, L$; % split features and labels into train and test subsets
8: **Output**: F to SoftMax activation function; % transform the outputs of the classifier into probabilities for each output of the two classes (Accept or Reject)

Algorithm 2. Execution of proposed CNN model

Function CNN (x):
x ← set the input data.
Conv 1 ← RELU_Activation_Func (Conv1D)
Conv 2 ← RELU_Activation_Func (Conv1D)
Conv 2 ← Max_Pool1D (Conv 2)
Conv 2 ← Dropout (0.2)
Conv 3 ← RELU_ Activation_Func (Conv1D)
Conv 4 ← RELU_ Activation_Func (Conv1D)
Conv 4 ← Max_Pool1D (Conv 4)
Conv 4 ← Dropout (0.2)
Conv 5 ← RELU_ Activation_Func (Conv1D)
Conv 5 ← Max_Pool1D (Conv 5)
Fully connected ← Reshape (Conv 5)
Fully connected ← Dropout (0.2)
Fully connected ← RELU_ Activation_Func (Fully connected)
***Output** ← Softmax_Func (Fully connected)*
Return Output
End Function

4. Experimental Validation

Our proposed model was executed on an Intel Core i7-6800K CPU with NVIDIA GTX 1080ti GPU and 16 GB RAM workstation equipped with MATLAB R2018a open-source Deep Learning toolbox. The

training time of the CNN model was 0.5 hour while the prediction lasted 0.03 seconds.

4.1 Performance Metrics

For performance assessment, we employed standard metrics, such as accuracy (A), precision (P), recall (R), EER, receiver operating characteristic (ROC) curve and F1-score (F1) that depend on false positive (FP), false negative (FN), true positive (TP), and true negative (TN) rates as defined in the equation matrix in Fig. 5 [26] where *N* and *M* represent the number of sets applied in the 5-fold validation and the number of classes, respectively. We note that the ROC curve is a graph used to show the performance of a statistical model with two output classes (such as the Accept or Reject) outcome of our model. It provides a trade-off between specificity and sensitivity and classifiers with high accuracy tend to have curves closer to the left corner [58].

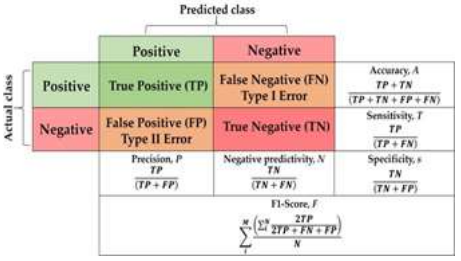

Fig. 5. Equation matrix for binary quality metrics. Adapted from [26].

4.2 Authentication Results

Using the performance metrics presented in Fig. 5, in this subsection an overview of the outcomes of the authentication process is presented and subsequently discussed in the next section. Table 4 presents the authentication results for the proposed system per fold for the PTB database by computing the accuracy, precision, recall and F1-score in each fold. Furthermore, these outcomes are presented as confusion matrices for each fold in Fig. 6 from where an average accuracy of 99.50% is reported. Based on this figure, 99.4% of the genuine classifications are correctly verified (i.e., true positive) while a meagre 0.04% of impostor cases are wrongly verified as genuine classifications, i.e., false positive classifications (or type II error).

Table 4. Authentication results per fold on PTB database

Number of folds	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
1	99.3	99.6	99.98	99.7
2	98.7	98.9	99.98	99.4
3	100	100	100	100
4	99.5	99.7	99.99	99.8
5	100	100	100	100

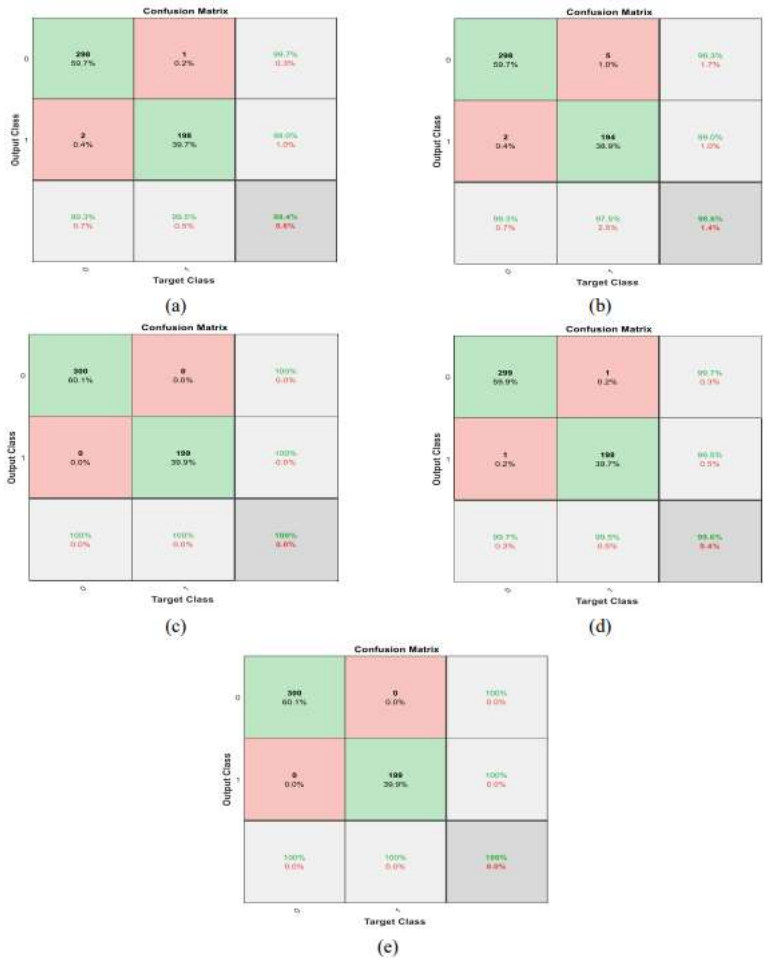

Fig. 6. Confusion matrix for each fold of proposed model: (a) 1-Fold, (b) 2-Fold, (c) 3-Fold, (d) 4-Fold, and (e) 5-Fold.

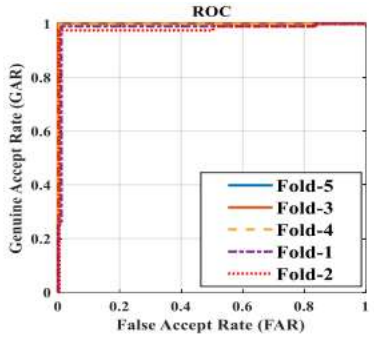

Fig. 7. ROC curves of each fold of proposed model.

Additionally, Fig. 7 presents the ROC curves for the proposed CNN model in each fold, while the variation in the EER (computed as a percentage rate when FP=FR) for our proposed model during the 5-fold validation is presented in Fig. 8. Here, it is noteworthy that an average EER of 0.47% is reported for the proposed model, while, as presented in Fig. 9 (i.e., plots of accuracy and logarithmic loss), it can be deduced that the model converges after 50 training epochs. Consequently, this setting is adopted for the remaining experiments that are reported.

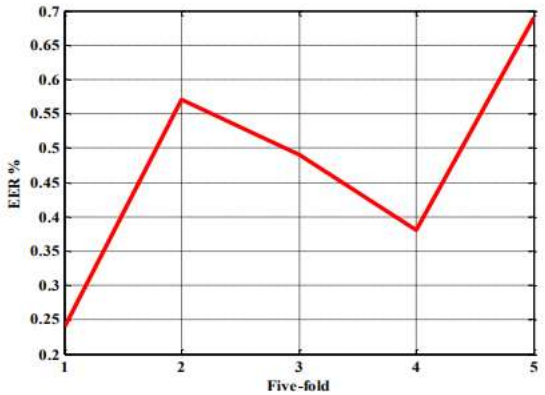

Fig. 8. Variation in EER (%) for different number of folds in proposed model.

5. Discussion of Results

Whereas analysis of the results presented earlier in Section 4 can provide deductions regarding the efficiency and robustness of the proposed authentication method, in this section we present an analysis of such outcomes. From the authentication results in Table 4 and the confusion matrices in Fig. 6, we can observe that the proposed method attained high accuracy in each fold (i.e., in some cases maximum accuracy of 100% was reported), which, as previously reviewed in Section 2, manifests the robustness of the proposed model and its capacity to overcome overfitting that is ascribed to CLM models,. Additionally, the ROC curves reported in Fig. 7 present evidence that the proposed model has high authentication in each fold as exhibited by the number of genuine acceptance rate relative to the number of false acceptance rate in each fold. Finally, the variations in EER reported in Fig. 8 support our claims regarding the accuracy of the proposed model since low EER is recorded in each fold.

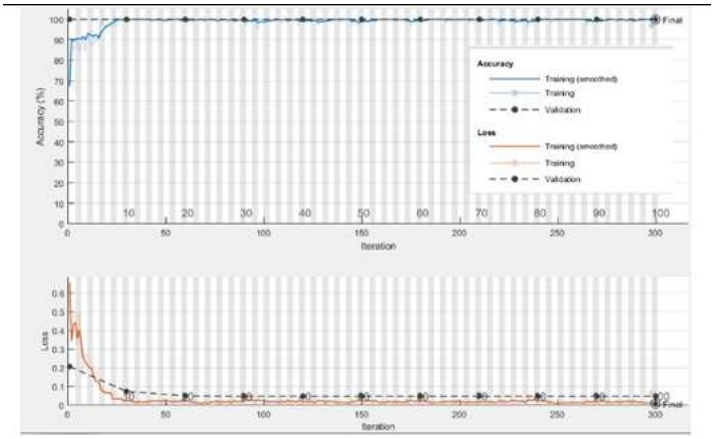

Fig. 9. Accuracy and loss curves for the proposed CNN technique.

To undertake an effective performance analysis, the authentication performance obtained using the PTB database based on [13–16] and deep learning techniques [17–23] highlighted earlier in Section 2 (presented in Table 5), alongside outcomes from our proposed model. Therefrom, we note the better performance (in bold) of out technique. Moreover, for a balanced discussion, we start by highlighting the key features of the methods used in the assessment (i.e., as presented in Table 5).

Unlike the deep learning approaches mentioned in Table 5 [17–20, 23], our proposed approach is built on an end-to-end structure that eliminates the need for different machine learning stages. Furthermore, our system is less complex than other systems because only one ECG lead was used. Additionally, unlike the enormous size of the filters in the convolutional layers (e.g., 5×1 and 8×1) employed by the model in [17], which increases the computational cost, our model utilizes a reasonable number of filters throughout the network (i.e., 3×1 filters). Moreover, unlike methods (such as [18, 20, 21]) that recorded low accuracy using noisy data, as an end-to-end structure, our model can manage such noisy signals. This eliminates the need for a preprocessing stage, and it works directly on the input ECG signal instead. Furthermore, unlike our proposed model, previous studies in [17–20, 22, 23] reported the use of separate classifiers, which exacerbates computational complexity and cost.

As noted earlier in Section 3, the use of edge computing servers to execute and evaluate the proposed deep learning model, provides access to radio networks to enhance computational and storage capabilities. Therefore, the overall performance of these systems is improved since computationally-intensive operations of the model are processed on the edge server. In this regard, edge computing models are considered prominent solutions that can offer lower latency and high bandwidth to support their implementation in real-time applications.

We conclude our discussion by once again highlighting the contributions of our study vis-à-vis its merits as highlighted in the reported discussions in this section:

- As demonstrated throughout the study, our model is less complex than other authentication approaches because it is conceived and built as a completely end-to-end structure.
- This end-to-end structure supports direct application on the ECG signal, thus circumventing the need for any preprocessing stage. This facilitates dealing with noisy ECG signals.
- Finally, compared to previous DLMs, our proposed model exhibits better robustness and effectiveness in overcoming traditional drawbacks, such as overfitting.

Table 5. Comparison of different authentication algorithms based on PTB database (see text for further details)

ECG authentication framework	Study	Methodology	Performance (EER, %)
Machine learning methods	Louis et al. [13]	Local binary patterns Sequential sampling and bagging	10.10
	Safie et al. [14]	Pulse active ratio Euclidean distance	9.89 (for normal class) 19.15 (for abnormal class)
	Gürkan et al. [15]	Autocorrelation/Discrete cosine transform Mel-frequency cepstrum coefficients Linear discriminant analysis Three-nearest-neighbor	2.84
	Hammad et al. [16]	Improved bio-hashing Matrix operation Feed forward neural network	32 14
Deep learning models	Labati et al. [17]	CNN	2.90
	Hammad et al. [18]	Two-dimensional CNN	3.20
	Hammad and Wang [19]	One-dimensional CNN	3.50
	Hammad et al. [20]	Scanning and removing techniques CNN	1.63
	Hammad et al. [22]	CNN Residual CNN (ResNet)	1.53 (using CNN) 1.39 (using ResNet)

	Chu et al. [23]	Parallel multi-scale one-dimensional residual network	0.59
	Proposed	**1D convolutional neural network**	**0.47**

6. Concluding Remarks

Our research enhances the existing machine and deep learning methods for ECG-based human identification by using edge computing servers that can connect to IoT devices and yet have access to computational and storage resources. The suggested model utilizes a Convolutional Neural Network (CNN) based Deep Learning Model (DLM) to achieve a complete structure that avoids the need for any manually designed preprocessing, feature extraction, and classification techniques, which are known to affect the computational complexity of the system. Therefore, our model demonstrates the capabilities of using edge computing frameworks to improve cost efficiency and effectiveness by reducing authentication time. The findings of studies using the PTB ECG database provide evidence that the suggested technique surpasses current conventional machine and deep learning models in terms of authentication Equal Error Rate (EER). These results demonstrate enhanced ability to apply our suggested method to a wide range of situations and its ability to withstand variations and uncertainties.

By making suitable adjustments, the suggested model may be used to many practical scenarios. For instance, it can be used to develop a vehicle access control system, enhance client identification in the banking system, and improve various medical systems. These applications provide intriguing opportunities to apply the proposed research. Although the suggested model has promise, it does have certain shortcomings, such as the absence of cancellability, which means it cannot preserve the ECG feature templates [59, 60]. Our short-term aims include addressing the limitations of the proposed model. In the future, we want to use template protection approaches to enhance the system's security against spoof attacks. Additionally, we aim to investigate the potential applications of the model in other biometric systems. In addition, we will evaluate security risks and provide countermeasures for assaults, as well as explore the use of sophisticated IoT infrastructures [46].

References

[1] A. S. Alghamdi, K. Polat, A. Alghoson, A. A. Alshdadi, and A. A. Abd El-Latif, “A novel blood pressure estimation method based on the classification of oscillometric waveforms using machine-learning methods,” *Applied Acoustics*, vol. 164, article no. 107279, 2020. https://doi.org/10.1016/j.apacoust.2020.107279

[2] K. A. Abuhasel, A. M. Iliyasu, and I. N. Alquaydheb, “Reappraising the Impact of environmental stresses on the useful life of electronic devices,” *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol. 20, no. 4, pp. 640-651, 2016. https://doi.org/10.20965/jaciii.2016.p0640

[3] A. S. Alghamdi, K. Polat, A. Alghoson, A. A. Alshdadi, and A. A. Abd El-Latif, “Gaussian process regression (GPR) based non-invasive continuous blood pressure prediction method from cuff oscillometric signals,” *Applied Acoustics*, vol. 164, article no. 107256, 2020. https://doi.org/10.1016/j.apacoust.2020.107256

[4] A. Savvas, “Halifax Bank trials heart rate technology to authenticate customers,” 2015 [Online]. Available: https://www.computerworld.com/article/3556854/halifax-bank-trials-heart-rate-technology-to-authenticate-customers.html.

[5] A. Alghamdi, M. Hammad, H. Ugail, A. Abdel-Raheem, K. Muhammad, H. S. Khalifa, and A. Ahmed, “Detection of myocardial infarction based on novel deep transfer learning methods for urban healthcare in smart cities,” *Multimedia Tools and Applications*, 2020. https://doi.org/10.1007/s11042-020-08769-x

[6] C. Burt, “EKG biometrics from B-Secure to be featured in 2020 car models.,” 2019 [Online]. Available: https://www.biometricupdate.com/201905/ekg-biometrics-from-b-secur-to-be-featured-in-2020-car-models.

[7] M. Hammad, A. Maher, K. Wang, F. Jiang, an M. Amrani, “Detection of abnormal heart conditions based

on characteristics of ECG signals," *Measurement*, vol. 125, pp. 634-644, 2018. https://doi.org/10.1016/j.measurement.2018.05.033

[8] C. L. Chen and C. T. Chuang, "A QRS detection and R point recognition method for wearable single-lead ECG devices," *Sensors*, vol. 17, no. 9, article no. 1969, 2017. https://doi.org/10.3390/s17091969

[9] P. Huang, L. Guo, M. Li, and Y. Fang, "Practical privacy-preserving ECG-based authentication for IoT-based healthcare," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9200-9210, 2019.

[10] C. L. P. Lim, W. L. Woo, S. S. Dlay, D. Wu, and B. Gao, "Deep multiview heartwave authentication," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 777-786, 2018.

[11] I. A. Elgendy, W. Z. Zhang, C. Y. Liu, and C. H. Hsu, "An efficient and secured framework for mobile cloud computing," *IEEE Transactions on Cloud Computing*, vol. 9, no. 1, pp. 79-87, 2018.

[12] M. A. Jan, W. Zhang, M. Usman, Z. Tan, F. Khan, and E. Luo, "SmartEdge: an end-to-end encryption framework for an edge-enabled smart city application," *Journal of Network and Computer Applications*, vol. 137, pp. 1-10, 2019.

[13] W. Louis, M. Komeili, and D. Hatzinakos, "Continuous authentication using one-dimensional multi-resolution local binary patterns (1DMRLBP) in ECG biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2818-2832, 2016.

[14] S. I. Safie, J. J. Soraghan, and L. Petropoulakis, "Electrocardiogram (ECG) biometric authentication using pulse active ratio (PAR)," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1315-1322, 2011.

[15] H. Gurkan, U. Guz, and B. S. Yarman, "A novel biometric authentication approach using electrocardiogram signals," in *Proceedings of 2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Osaka, Japan, 2013, pp. 4259-4262.

[16] M. Hammad, G. Luo, and K. Wang, "Cancelable biometric authentication system based on ECG," *Multimedia Tools and Applications*, vol. 78, no. 2, pp. 1857-1887, 2019.

[17] R. D. Labati, E. Munoz, 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.

[18] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 26527-26542, 2018.

[19] M. Hammad and K. Wang, "Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network," *Computers & Security*, vol. 81, pp. 107-122, 2019.

[20] M. Hammad, S. Zhang, and K. Wang, "A novel two-dimensional ECG feature extraction and classification algorithm based on convolution neural network for human authentication," *Future Generation Computer Systems*, vol. 101, pp. 180-196, 2019.

[21] M. G. Kim and S. B. Pan, "Deep learning based on 1-D ensemble networks using ECG for real-time user recognition," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5656-5663, 2019.

[22] 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, article no. e12547, 2021. https://doi.org/10.1111/exsy.12547

[23] Y. Chu, H. Shen, and K. Huang, "ECG authentication method based on parallel multi-scale one-dimensional residual network with center and margin loss," *IEEE Access*, vol. 7, pp. 51598-51607, 2019.

[24] A. Sedik, M. Hammad, F. E. Abd El-Samie, B. B. Gupta, and A. A. Abd El-Latif, "Efficient deep learning approach for augmented detection of coronavirus disease," *Neural Computing and Applications*, 2021. https://doi.org/10.1007/s00521-020-05410-8

[25] M. Amrani, M. Hammad, F. Jiang, K. Wang, and A. Amrani, "Very deep feature extraction and fusion for arrhythmias detection," *Neural Computing and Applications*, vol. 30, no. 7, pp. 2047-2057, 2018.