Applied GIS

ISSN: 1832-5505
Vol-10 Issue-04 Oct 2022

Data Verification at Every Level A Deep Learning Framework for IoT Security Establishments

Dr.T.Vishnu Priya [1], Ms.N.Rama Priya [2],
Associate Professor [1], Assistant Professor [2],
Department of ECE, SRK INSTITUTE OF TECHNOLOGY ENIKEPADU VIJAYAWADA
Mail Id : Vishnu priya000@gmail.com, Mail id : Ramapriya442.ece@gmail.com,

Abstract

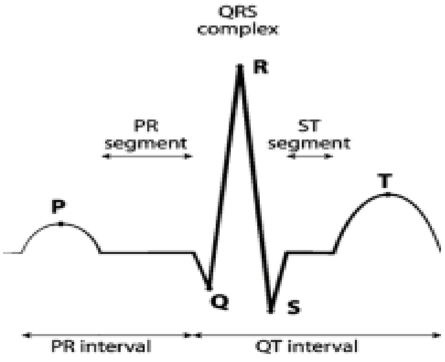
***Electrocardiograms (ECGs) have received universal acceptance as a medium for certifying animateness in several security applications, notably in new and developing technologies, compared to other biometrics. By using edge computing servers that provide connectivity to Internet of Things (IoT) devices while preserving access to computational and storage resources, our research helps to enhance existing machine and deep learning ECG authentication methods. Specifically, our suggested method integrates the pre-processing, feature extraction, and classification methods into a single module, and then feeds individual ECG signals from the database into a convolutional neural network (CNN) model for acceptance or rejection. Our authentication method is also optimised for usage with applications running on edge computing platforms, since it is both cost-effective and latency-conscious. We tested our proposed model on a database of standard ECG signals provided by the Physikalisch-Technische Unresistant (PTB), and the results showed that our approach is both accurate and precise enough for use in real-time authentication systems, with recall and F1-scores of 99.73%, 100%, and 99.78%, respectively. Further, we analyse how the model fares in comparison to more modern methods that are based on classic machine learning and deep learning architectures*.**

Keywords

Technologies like Deep Learning, Biometric Authentication, Electrocardiograms, Information Security, Internet of Things, Edge Computing, and Industrial Data Integration are becoming more important in today's world.

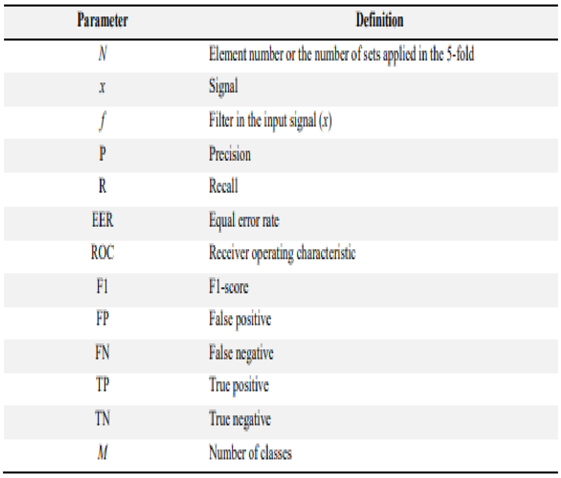
Introduction

Traditional authentication techniques, including security tokens, passwords, PINs, etc., have recently seen a decline in popularity due to rising instances of counterfeiting. Instead, biometric authentication is often used nowadays. Still, conventional biometric identifiers like fingerprints, faces, irises, and ears are affected by a broad variety of parameters, including their universality, uniqueness, performance, measurable accuracy, acceptance, and vulnerability to fraud and evasion. The use of electrocardiogram (ECG) signals as biometric markers gives a good test of animateness in addition to giving a good compromise in these parameters, and this is in contrast to the conventional biometric modalities, such as fingerprints, which do not necessarily indicate awareness. The electrocardiogram (ECG) detects irregularities in the heart's electrical activity [2]. Size-wise, currently available ECG sensors have been shrinking, facilitating their incorporation into wearable devices and linked cars [3]. The ease of use and versatility of ECGs have contributed to their widespread use in a variety of settings [4, 5]. In [6], these features are used to ensure the safety of vehicle access control identification procedures for both drivers and passengers. In the meanwhile, the electrocardiogram (ECG) is regarded as critical in the identification of a number of heart problems, including arrhythmias and other coronary illnesses. The P-wave, QRS complex, and T-wave are the three components of an ECG signal that make up a typical cardiac cycle [2]. Additionally, the ST-segment, the PR-segment, and the QT-interval are all very important segments or intervals. The P-wave represents the atrial depolarization that occurs during atrial contraction, while the QRS-complex section represents the ventricular depolarization that occurs during ventricular contraction. T-wave relaxation states are thereafter restored in both ventricles [7]. The QT-interval is the distance from the beginning of the QRS complex to the beginning of the T-wave, whereas the PR-interval is the distance from the beginning of the P-wave to the beginning of the Q-wave (also known as the PR-segment). The ST-segment or ST-interval is the portion of an electrocardiogram that separates the S-wave and the T-wave. You can see the peaks and valleys of a typical ECG signal in Fig. 1. These properties have found use in a broad variety of contexts, including the enhancement of security in body-area network sensors (BANs) such smart wristbands and cardiac pacemakers [8].



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].

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

Companion Pieces

Previous research on ECG-based authentication may be roughly categorised as either conventional machine learning (CLM)-based methods [1316, 42] or DLM-based approaches [1723, 4347], as we mentioned in the introduction. A summary of current research in these fields is provided below.Traditional Approaches to Machine Learning the term "classical machine learning" (CLM) is used to describe methodologies that use the whole machine learning pipeline. The ECG signals in such a system go through many processing stages before authentication is complete. Initially, the incoming ECG data are cleaned up by excluding unwanted background activity and strengthening weaker signals. This is the "pre-processing" stage of a project. The second phase involves picking out the most salient aspects of the pre-processed ECG data for extraction. The process of identifying these traits is known as the feature extraction stage, and it is important that they be distinct for each signal. Authentication is performed at the last phase, classification, by feeding the characteristics into the classifier. The aforementioned structures form the basis of the majority of CLM methods. For instance, the authors of [13] proposed one-dimensional multi-resolution local binary patterns (1DMRLBP) and sequential sampling feature extraction for one-dimensional signals, both of which contribute to a new feature extraction and continuous authentication approach, respectively. This system dynamically adjusts cut-off values and sample sizes while running. Read more about how it handles the quantization error required to tolerate noise and how it recovers local and global signal morphology in [13].

The authors claimed to have used data from 290 patients from the Physikalisch-Technische Unresistant (PTB) database for validation, and they reported an equal error rate (EER) for ECG signal authentication of 10.10%. Also, utilising ECG fiducial points as a feature vector, Safi et al. [14] introduced a feature extraction method they dubbed pulse active ratio (PAR) for ECG-based authentication. By using the Euclidean distance as the similarity metric, this method compares each feature vector in the test dataset to each feature vector in the training database to determine how well they match. A successful authentication is indicated by a match between the feature vectors of the test dataset and the training dataset. Using the PTB dataset, they conducted studies on 112 people, reporting that 98 of them had arrhythmia beats while the other 30 were healthy. Furthermore, they found that the EER for regular heartbeats was 9.89% and that of arrhythmia was 19.15%. An ECG-based human authentication expert system was created by Hoshiarpur and Goshvarpour [42].

Utilizing both ECG features and information theoretic (IT) factors, they developed their authentication technique. Finally, they used k-nearest neighbour (in) to identify people using 5-fold cross-validation and found an average accuracy of 97.6 percent. Ivanciu et al. [49] introduced a Siamese neural network-based ECG-system for authentication. With the Siamese network, they were able to streamline the learning process. In order to guarantee the system's safety and scalability, they had it set up on a private cloud. Their stated sensitivity was 87.3%, and their total accuracy was 86.47. The authors of [50] presented an incremental-learning-based ECG authentication system that could distinguish each subject's ECG signal across a range of experimental settings. When it came to authentication, they used a support vector machine (SVM), and claimed it was 99.4 percent effective. Similarly, in [51], the authors introduced a nonlinear normalization-based ECG authentication method that takes into account different physiological situations. At rest, they recorded an accuracy of 99.05%, but in active states, it dropped to 88.14%.

A Look at the Stuff You'll Need

Our suggested CNN-based deep learning method (or CDM for short) streamlines the several steps typically performed by traditional machine learning methods (pre-processing, feature extraction, and classification) into a single procedure. Using biometric data from the PTB database [54], this research used the same methodology as the majority of the featured studies in the preceding section. Our proposed CNN model is trained using a dataset [54] consisting of 290 participants' ECG signals. Finally, the proposed model assigns an acceptance or rejection classification to the obtained ECG data. In our prior presentation of ECG-authenticated vehicle access control systems (see Fig. 2), we showed how the system provides access depending on the driver's identity, i.e., whether or not the driver is approved as an authorised user. For a high-level overview of how the DLM fits within the ECG authentication system.

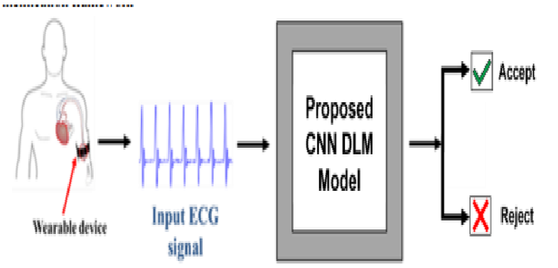


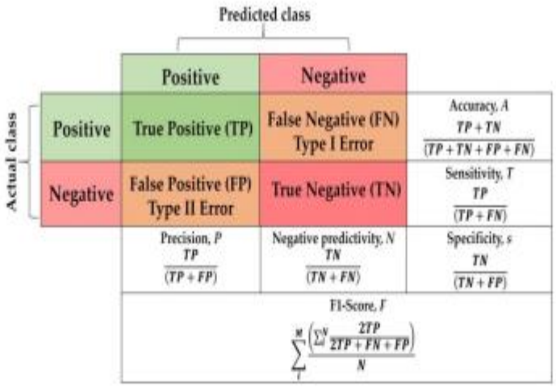
Fig. 1. Block diagram outlining implementation of the proposed model.

Verification Through Experiment

For testing purposes, we used a workstation with a 16 GB RAM Intel Core i7-6800K CPU, NVIDIA GTX 1080ti GPU, and MATLAB R2018a open-source Deep Learning toolbox to run our proposed model. The CNN model took half an hour to train, yet could make a prediction in only 0.03 seconds.

Indices of Performance

We used common metrics for evaluating performance, including accuracy (A), precision (P), recall (R), expected error rate (EER), ROC curve, and F1-score (F1), all of which are dependent on the rates of false positives (FP), false negatives (FN), true positives (TP), and false negatives (TN) as defined in the equation matrix in Fig. 1 [26], where N and M stand for the number of sets used in the 5-fold validation and the number of classes, Keep in mind that the ROC curve is a graph used to display the efficiency of a statistical model with two output classes (like the Accept or Reject result of our model). Classifiers with a high degree of accuracy have curves that are closer to the left corner of the graph, providing a trade-off between specificity and sensitivity [58].



		Predicted class		
		Positive	Negative	
Actual class	Positive	True Positive (TP)	False Negative (FN) Type I Error	Accuracy, A $\frac{TP+TN}{(TP+TN+FP+FN)}$
	Negative	False Positive (FP) Type II Error	True Negative (TN)	Sensitivity, T $\frac{TP}{(TP+FN)}$
		Precision, P $\frac{TP}{(TP+FP)}$	Negative predictivity, N $\frac{TN}{(TN+FN)}$	Specificity, s $\frac{TN}{(TN+FP)}$
		F1-Score, F $\sum_{i}^{M}\frac{\left(\sum_{i}^{N}\frac{2TP}{2TP+FN+FP}\right)}{N}$		

Fig. 2. Equation matrix for binary quality metrics. Adapted from [26].

Evaluation of Outcomes

Here we offer an analysis of the findings reported in Section 4, which may be used to draw conclusions about the effectiveness and reliability of the suggested authentication technique. Table 1 and Fig. 2 show that the proposed method achieved high accuracy in each fold of authentication (i.e., in some cases maximum accuracy of 100% was reported), which, as discussed in Section 2, demonstrates the robustness of the proposed model and its capacity to overcome overfitting that is ascribed to CLM models. In addition, as shown by the genuine acceptance rate compared to the false acceptance rate in each fold, the ROC curves provided in Fig. 7 provide further evidence that the proposed model has good authentication in each fold. Finally, low EER is recorded in each fold, as seen by the fluctuations in EER presented in Fig. 2. This lends credence to our statements about the precision of the suggested model.

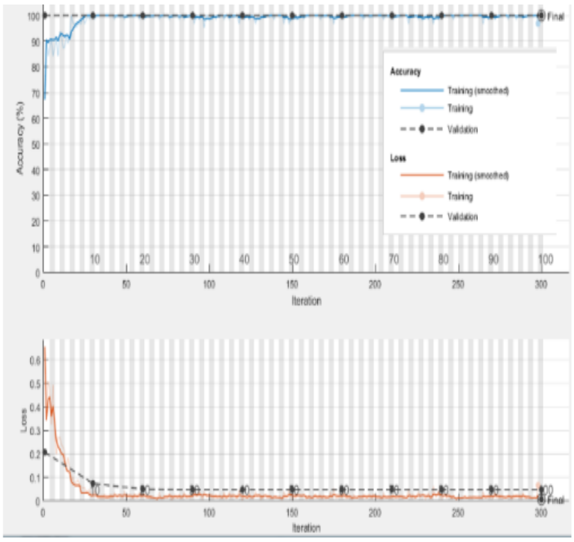


Fig. 3. Accuracy and loss curves for the proposed CNN technique.

Conclusion

By using edge computing servers that may be linked to IoT devices while preserving access to computational and storage resources, our research improves upon earlier machine and deep learning approach for ECG-based human authentication. To reduce the computational complexity of the system, the proposed approach uses a CNN-based DLM to provide a full pipeline that does all pre-processing, feature extraction, and classification automatically. As a result, our model shows the possibilities of integrating the edge computing frameworks to improve cost effectiveness and efficiency in terms of reduced authentication time. Experimental results using the PTB ECG database corroborate assertions that the suggested technique achieves much lower authentication EER than state-of-the-art classical machine and deep learning models. These results suggest that our suggested technique is more generalizable and stable than previously thought. Some intriguing avenues to apply the suggested research include in real-world applications of the proposed model, such as a vehicle access control system, customer authentication for the banking system, and applications in various medical systems. Negative aspects of the proposed model include its inability to cancel, i.e., to safeguard the ECG feature templates [59, 60], despite its promise. One of our immediate priorities is to address these limitations of the proposed model, and down the road, we want to include template protection measures to defend the system against spoof attempts and investigate the model's potential use in other biometrics contexts. In addition, we will evaluate potential dangers, provide countermeasures for assaults, and discuss their potential uses in cutting-edge IoT networks [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-toauthenticate-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-carmodels.

[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 IoTbased 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 multiresolution 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.