International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

DESIGNING SECURE AND EFFICIENT BIOMETRIC-BASED SECURE ACCESS MECHANISM FOR CLOUD SERVICES

G. SATHEESH KUMAR[1], MD SHABAZ PATEL[2], JILLELLA ABHISHEK PAUL[3], VALLAMKONDA SATHWIK[4], JOGINIPELLI SAI SREEJA[5]

[1]Assistant professor, Department of CSE, Malla Reddy College of Engineering Hyderabad, TS, India.
[2,3,4,5] UG students, Department of CSE, Malla Reddy College of Engineering Hyderabad, TS, India.

ABSTRACT:

This paper introduces a framework for how to appropriately adopt and adjust machine learning (ML) techniques used to construct electrocardiogram (ECG)-based biometric authentication schemes. The proposed framework can help investigators and developers on ECG-based biometric authentication mechanisms define the boundaries of required datasets and get training data with good quality. To determine the boundaries of datasets, use case analysis is adopted. Based on various application scenarios on ECG-based authentication, three distinct use cases (or authentication categories) are developed. With more qualified training data given to corresponding machine learning schemes, the precision on ML-basedECG biometric authentication mechanisms are increased in consequence. The ECG time slicing technique with the R-peak anchoring is utilized in this framework to acquire ML training data with good quality. In theproposed framework four new measure metrics are introduced to evaluate the quality of the ML training and testing data. In addition, a Matlab toolbox, containing all proposed mechanisms, metrics, and sample data with demonstrations using various ML techniques, is developed and made publicly available for further investigation. For developing ML-based ECG biometric authentication, the proposed framework can guide researchers to prepare the proper ML setups and the ML training datasets along with three identified user case scenarios. For researchers adopting ML techniques to design new schemes in other research domains,the proposed framework is still useful for generating the ML-based training and testing datasets with goodquality and utilizing new measure metrics.

Keywords: HITS, Hash tags, CNN, ML.

1. INTRODUCTION:

Most application systems support Internet access for general users, identifying persons with their

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

own body has become the trend for users to access application systems. In consequence, biometric authentication has become a hot research topic in recent years. Among various biometric authentication schemes such as fingerprint scanning and facial recognition, electrocardiogram authentication has the advantage of adopting live user body signals during authentication. In general, machine learning techniques are adopted to construct a verification model for user identification by getting user's live ECG data. Recently there are a number of state-of-art literatures on ECG based biometrics. However, several ECG biometrics challenges still require further investigation such as authentication categorization, pre-processing for data quality enhancement, data acquisitions, selection on Deep Learning (DL) and other Machine Learning classification approaches. This project introduces a ML framework for ECG based biometric authentication in order to mitigate identified challenges on ECG authentication. To better understand potential application environments for ECG authentication, it is necessary to identify basic application scenarios through use cases. In the proposed framework, application scenarios using ECG authentication are categorized into three general use cases: Hospital (HOS), Security Check (SCK) and Wearable Devices (WD). Furthermore, new data preprocessing techniques including the baseline adjustment of frequency artifacts in the ECG, the ECG data noise removal technique for Power Line Interference (PLI), and flipping mechanism for ECG signal due to the wrong placement of electrodes, are proposed. In addition, time slicing techniques are introduced in the framework to prepare ML-based training datasets along with new measure metrics developed for authentication precision evaluation. Four new measure metrics for data quality are introduced in the proposed framework. They are Mean Absolute Error Rate (MAER), Upper/Lower Range Control Limits (UCL/LCL), Accuracy Percentage within Ranges (APR), and Accuracy per UCL (APU).

2. LITERATURE SURVEY

In this session, we discuss about Biometric Authentication using Electrocardiogram by Machine learning Framework. Several ML techniques are adopted: Decision Tree (DT) and Support Vector Machine (SVM) for regression approach, and Artificial Neural Network (ANN) and Convolution Neural Network (CNN) for classification approach. Song-Kyoo (Amang) Kim received the M.S. degree in computer engineering from the Florida Institute of Technology, in 1999, and the Ph.D. degree in operations research, in 2002. He is

currently a Research Scholar with Khalifa University. He has been an Associate Professor of various universities in United Arab Emirates. Prior to joining in the Gulf regions, he was a Core Faculty Member of the Asian Institute of Management who taught Technology, Innovation, and Operations topics. Before joining the academy, he had been a Technical Manager with the Mobile Communication Division, Samsung Electronics, for over ten years and mainly dealt with technology management in IT industries. He has authored various research papers and patents focused on mobile industries. His research interests include artificial intelligent and ECG-based biometric securities. His current research interests include Block chain Governance Game. For developing ML-based ECG biometric authentication, the proposed framework can guide researchers to prepare the proper ML setups and the ML training datasets along with three identified user case scenarios. For researchers adopting ML techniques to design new schemes in other research domains, the proposed framework is still useful for generating the ML-based training and testing datasets with good quality and utilizing new measure metrics.

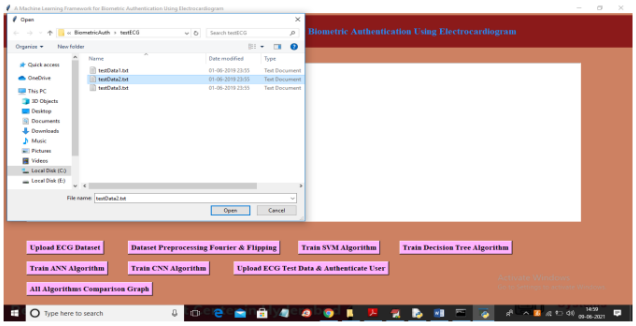
3. METHODOLOGY

Traditionally, a patient will take an ECG test to diagnose whether a heart disease or a heart stress is occurred. The equipment for gathering ECG signals from a patient is usually elaborated and complicated for gathering the high quality for medical diagnostics. Therefore, the sampling time for getting ECG data is relatively long (from couple of minutes to hours dependent on the type of ECG test) and multiple leads are used during an ECG test. A new use case for ECG test is to identify patients in a hospital (Category 1; HOS use case). The assumption is that those patients have to register their identities (i.e., their names or legal identity numbers) along with their historical ECG data in advance. In addition, it is assumed that the measured ECG signals from the same patient are stable enough (i.e., the measured ECG signal values within a normal range) for both registration (training) and verification (testing) phases of an ECG based authentication scheme. Then the hospital can identify those patients with ECG based biometric authentication scheme next time the patients enter the hospital. Notice that a well trained ECG user authentication model (or scheme) can identify a patient by evaluating live ECG signals in a very short period of time (less than a couple of seconds) in comparison with questioning for the patient's name and his/her legal identity number by a nurse (it may take a couple of minutes). For patients losing consciousness in an emergency room, ECG based user (or patient) authentication

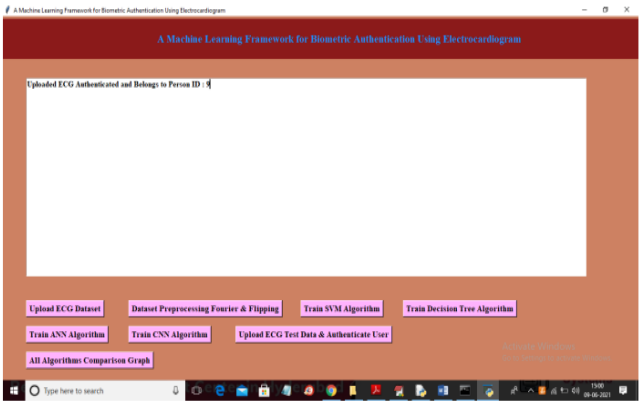
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal
2581-4575

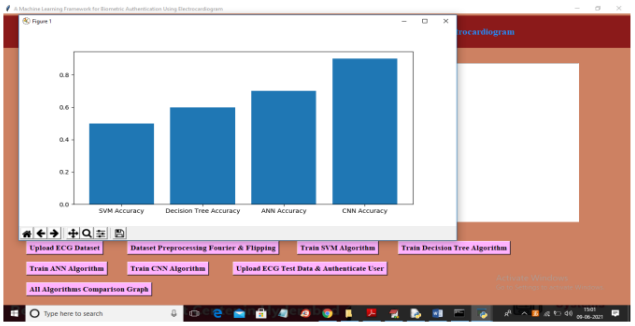
can easily identify those patients. In general, a patient authentication in hospitals may be one of the major application environments for ECG based authentication schemes. This HOS use case is the most widely applied research environment in healthcare and medical industry. There are a lot of public available databases containing historical ECG data such as the PhysioBank database.

Because of complexity for data collecting operations, the received ECG data could be flipped or contain certain noises caused by PLI or wrong position placement of electrodes. Therefore, it is necessary to perform data pre-processing mechanisms onto these ECG data to further improve data quality before using them to train evaluation model for user (or patient) authentication purpose.



In above screen person ID is Authenticated or Identified as ‘Person ID 9’ and similarly you can upload any other test data and authenticate user. Now click on ‘All Algorithms Comparison Graph’ button to get accuracy graph of all algorithm.





CONCLUSION

As new ECG detection devices become portable, lightweight, embeddable with smart phones and wearable devices, and connectable with remote servers through wireless technologies in the near future, ECG based biometric authentication will be deployed on massive application systems all over the world. To get high accuracy on user authentication, ML techniques are generally adopted to build a more robust evaluation model for ECG based biometric authentication. In this paper a generalized machine learning framework

for ECG based biometric authentication is introduced. The proposed framework describes the general data processing flow of a ML-based ECG authentication mechanism along with various function features to help researchers easily design and evaluate a ML-based ECG user authentication scheme. Those functions include three general authentication categories for ECG user authentication, three new data pre-processing techniques, a time slicing technique to generate high quality ECG datasets, four new data quality metrics, and a publicly available Matlab Toolbox (i.e., amgecg Toolbox). For people using ML technologies to investigate other topics instead of ECG based biometric authentication, several data pre-processing techniques and newly defined measure metrics offered by the proposed framework are still useful and can help researchers accelerate the development of their ML-based schemes.

REFERANCES

[1] Q. Zhang, D. Zhou, and X. Zeng, ‘‘HeartID: A multiresolution convolutional neural network for ecg-based biometric human identification in smart health applications,’’ IEEE Access, vol. 5, pp. 11805–11816, 2017.

[2] J. R. Pinto, J. S. Cardoso, and A. Lourenço, ‘‘Evolution, current challenges, and future possibilities in ECG biometrics,’’ IEEE Access, vol. 6, pp. 34746–34776, 2018.

[3] E. J. da Silva Luz, G. J. P. Moreira, L. S. Oliveira, W. R. Schwartz, and D. Menotti, ‘‘Learning deep off-the-person heart biometrics representations,’’ IEEE Trans. Inf. Forensics Security, vol. 13, no. 5, pp. 1258–1270, May 2018.

1https://github.com/amangkim/amgecg_toolbox

2http://youtu.be/texyM7Gzz3c

[4] H. Kim and S. Y. Chun, ‘‘Cancelable ECG biometrics using compressive sensing-generalized likelihood ratio test,’’ IEEE Access, vol. 7, pp. 9232–9242, 2019.

[5] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, ‘‘Machine learning and deep learning methods for cybersecurity,’’ IEEE Access, vol. 6, pp. 35365–35381, 2018.

[6] H. J. Kim and J. S. Lim, ‘‘Study on a biometric authentication model based on ECG using a fuzzy neural network,’’ Proc. IOP Conf. Ser., Mater. Sci. Eng., vol. 317, Mar. 2018, Art. no. 012030.

[7] J. R. Pinto, J. S. Cardoso, A. Lourenço, and C. Carreiras, ‘‘Towards a continuous biometric system based on ECG signals acquired on the steering wheel,’’ Sensors, vol. 17 no. 10, p. 2228, 2017.

[8] M. Sansone, R. Fusco, A. Pepino, and C. Sansone, ‘‘Electrocardiogram pattern recognition and analysis based on artificial neural networks and support vector machines: A review,’’ J. Healthcare Eng., vol. 4, no. 4, pp. 465–504, Jun. 2013.

[9] A. E. Saddik, J. S. A. Falconi, and H. A. Osman, ‘‘Electrocardiogram (ECG) biometric authentication,’’ U.S. Patent 9 699 182 B2, Jul. 4, 2017.

[10] S. Y. Chun, J.-H. Kang, H. Kim, C. Lee, I. Oakley, and S.-P. Kim, ‘‘ECG based user authentication for wearable devices using short time Fourier transform,’’ in Proc. 39th Int. Conf. Telecommun. Signal Process. (TSP), Jun. 2016, pp. 656–659.

[11] A. F. Hussein, A. K. AlZubaidi, A. Al-Bayaty, and Q. A. Habash, ‘‘An IoT real-time biometric authentication system based on ECG fiducial extracted features using discrete cosine transform,’’ Aug. 2017, arXiv:1708.08189. [Online]. Available: https://arxiv.org/abs/1708.08189