IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 29, 2019, accepted August 19, 2019, date of publication August 26, 2019, date of current version September 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2937357

An Enhanced Electrocardiogram Biometric Authentication System Using Machine Learning

EBRAHIM AL ALKEEM[1], SONG-KYOO KIM[2], CHAN YEOB YEUN[1,2], MOHAMED JAMAL ZEMERLY[1], KIN FAI POON[3], GABRIELE GIANINI[3,4], AND PAUL D. YOO[5,6]

[1]Department of Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi 127788, UAE
[2]Center for Cyber-Physical Systems, Khalifa University of Science and Technology, Abu Dhabi 127788, UAE
[3]Emirates ICT Innovation Centre, Khalifa University of Science and Technology, Abu Dhabi 127788, UAE
[4]Dipartimento di Informatica Gianni Degli Antoni, Università degli Studi di Milano, 20122 Milano, Italy
[5]CSIS, Birkbeck College, University of London, London WC1E 7HX, U.K.
[6]Cranfield School of Defence and Security, Defence Academy of the United Kingdom, Shrivenham SN6 8LA, U.K.

Corresponding author: Chan Yeob Yeun (chan.yeun@ku.ac.ae)

This work was supported in part by the Center for Cyber-Physical Systems, Khalifa University, under Grant 8474000137-RC1-C2PS-T3, in part by the EU H2020 Research Programme Threat-Arrest under Grant 786890, and in part by the Concordia University under Grant 830927.

ABSTRACT Traditional authentication systems use alphanumeric or graphical passwords, or token-based techniques that require ''something you know and something you have''. The disadvantages of these systems include the risks of forgetfulness, loss, and theft. To address these shortcomings, biometric authentication is rapidly replacing traditional authentication methods and is becoming a part of everyday life. The electrocardiogram (ECG) is one of the most recent traits considered for biometric purposes. In this work we describe an ECG-based authentication system suitable for security checks and hospital environments. The proposed system will help investigators studying ECG-based biometric authentication techniques to define dataset boundaries and to acquire high-quality training data. We evaluated the performance of the proposed system and found that it could achieve up to the 92% identification accuracy. In addition, by applying the Amang ECG (*amgecg*) toolbox within MATLAB, we investigated the two parameters that directly affect the accuracy of authentication: the ECG slicing time (sliding window) and the sampling time period, and found their optimal values.

INDEX TERMS Authentication, biomedical signal processing, electrocardiogram signal (ECG), machine learning, multi-variable regression.

I. INTRODUCTION

Biometric authentication is replacing typical identification and access control systems to become a part of everyday life [1], [2]. The electrocardiogram (ECG) is one of the most recent traits to be explored for biometric purposes [3], [4]. ECGs report electrical conduction through the heart and can be used to recognize specific individuals [5]. The utilization of ECGs as a biometric trait was first proposed in a 1977 US military report [6]. Although much progress has been achieved over the last decades, many challenges remain to be overcome [5], including data acquisition, pre-processing for data enhancement, the assignment of authentication categories. However, the recent development of deep learning (DL) and other machine learning (ML) classification techniques [7] open new perspectives to this approach to authentication. ML techniques have recently been used to construct a verification model for identification based on live ECG data [8]–[11]. ML is a subfield of Artificial Intelligence: ML algorithms build a mathematical model based on training data; typical models are regression (predictions) models and decisions models (e.g. classification and pattern recognition) [12]. The diverse applications of ML include the analysis of videos, images, and sounds [13], as well as ECG data [11], [14], [15].

ECG research covers a wide range of disciplines with different requirements. Medical engineers set up electrocardiographs for the collection of rich ECG data [5], [16], [17], whereas electrical engineers use simpler sensors to detect ECG signals [18]–[21]. In a previous study [22] we defined three use cases that influence the setup of an ECG-based authentication system focusing the attention on aspects of the

The associate editor coordinating the review of this article and approving it for publication was Chi-Yuan Chen.

system that are relevant for external users [23]. The three use cases are security checks (SCK), hospitals (HOS) and wearable devices (WD). The analysis of these three use cases helps researchers in the field of biometric authentication to understand the conditions and setup the requirements for each scenario [22]. In this article, we consider the SCK and HOS use cases in more detail. In a typical SCK scenario, biometric authentication based on a simple ECG scan, would take place at a security checkpoint of an entrance to a building and would identify employees and visitors, while excluding unknown persons [22]. In contrast, the HOS use case involves complex medical equipment which collects detailed ECG data during the training and testing phases. This requires a longer sampling time period and multiple leads to attach a person to gather the data [22].

Our proposed authentication system uses multi-variable regression to break down the dataset into smaller subsets, then builds a decision tree (DT) model based on these variables to predict target values [24], [25].

With respect to competing techniques, such as DL techniques, we consider the following. The convoluted nature of popular deep-structured machine learning implies lack of transparency and interpretability. The knowledge obtained by more interpretable learners (such as decision trees) is critical in biometric software design. The deep learning methods [26]–[29] could be applied but the DT is more flexible for the input size of the samples and the changes in sampling frequency.

We use the time-sliced ECG method to build the training and testing datasets [22] and also investigate the optimum sliding window size. Time-sliced ECG data provides a sufficient number of samples and each sliced dataset can be used as the input for ML training. Although time-sliced ECG data offers sufficient flexibility to mix with other training inputs, we have used this source of data on its own. Previous research showed that the performance of ML is dependent on the ECG slicing time [7]–[10], we have therefore investigated this relationship. The minimum heartbeat interval within a typical heart rate [29] was chosen as the sliding window width. Representative time-sliced ECG data are shown in Fig. 1. We used the Amang ECG (*amgecg*) toolbox in MATLAB for ECG time slicing and to build the training input for the regression approach [22].

This paper is organized into four sections. Section II describes the new ML-based authentication system and evaluates its classification performance [32]. Section III considers the two most relevant parameters (slicing time and sampling time period) that directly affect authentication performance: their relationship and impact are evaluated. Finally, the new authentication system and its contributions are summarized in Section IV.

II. ECG-BASED AUTHENTICATION USING ML

This section describes the ECG-based authentication system using regression as a ML technique that particularly complements the security check, or SCK, use case. The sampling

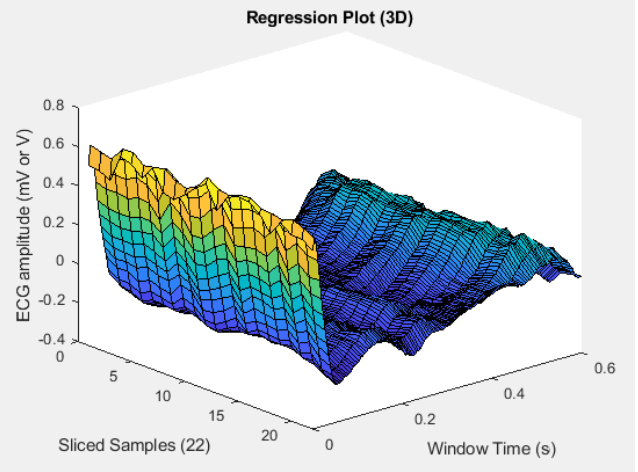

FIGURE 1. ECG time slicing with R-peak anchoring [31].

time period for the testing (validation) phase is relatively short: less than 20s. The system can identify the unknown entity within this short interval [22].

A. SECURITY CHECK CASE: EXPERIMENTAL SETUPS

Several ML approaches could be used to develop a regression model, however our previous studies showed that the DT method achieves the best performance with time-sliced ECG data [22]. We confirmed this by comparing the performance of the decision tree (a fine tree, with a rich structure, i.e. many nodes) and support vector machine (SVM) methods and the results are shown in Table 1. Based on these results, we selected the DT-based regression method for our authentication system. The performance comparison between DT and SVM have been analyzed by the *Regression Leaner* function in Matlab. The values in Table 1 is automatically generated by the Matlab function during training the dataset.

TABLE 1. Performance comparison between decision trees (dt) and support vector machines (SVM).

	DT (Fine Tree)	SVM (Fine Gaussian)
RMSE[1]	0.05817 mV	0.06011 mV
MAE[2]	0.00339 mV	0.00361 mV
Training Time	5.96 s	7554.3 s

[1] RMSE: Root Mean Square Error
[2] MAE: Mean Absolute Error

We therefore applied this method to the SCK use case based on 90 ECG data samples arbitrary collected in a HOS environment [22]. An ECG-based authentication system can be used to identify employees and exclude unknown persons assuming that employees have registered their identities and the ECG data are stable enough during both the training and testing phases. Out of the 90 samples used to construct the dataset for this experiment, 63 were sourced from the PhysioBank database [31], [33] and 27 from the Diabetes

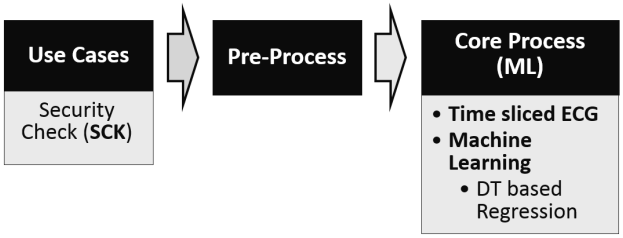

FIGURE 2. The training process for the SCK use case.

Complications Research Initiative [34]. The data from the PhysioBank [31], [33] have been downloaded and transforming into Matlab formats by using the WFDB toolbox [35] and the data from the other source [34] are originally supported as the Matlab format. Ten additional samples (indicated hereafter as 'unknown') were randomly selected from the dataset using the same sources but in different sampling time periods [31], [33], [34] and added during the testing phase [22]. Preprocessing for the HOS use case is still necessary even when dealing with the SCK scenario because the sources are not originally from the security check.

The authentication process began with use-case categorization and pre-processing, before training the dataset. All pre-processing steps recommended in our previous study [22] were applied (including baseline drift adjustment, power line interference (PLI) noise adjustment and checking the flipping signal) because the data were sourced from medical equipment (HOS use case). Although the pre-process for ECG signals by using various techniques has been widely studied [36]–[39], our system only follows the basic standard methods which have been suggested from the ML framework [22]. The polynomial curve fitting for the baseline drift adjustment and the Fourier Transform for the PLI noise cancellation have been applied in this research [22]. The ECG data were collected at two different times, resulting in two datasets, which were defined as the training and testing sets. The ECG data were trained using the DT regression method (Fig. 2).

Although many different measures and techniques are cited in the biometric literature for feature selection filters, we used mutual information in DT model as a measure to score and rank the features. Mutual information was proposed by Shannon [40] as part of this information theory, and was based in the concept of entropy, used to quantify the irreducible complexity of random signals (below which no lossless compression is possible). The entropy H of a random variable x with a probability mass function $p(x)$ is

$$H(x) = -\sum_{x \in X} p(x) \log_2 p(x) \tag{1}$$

where X is a set of all possible outcomes of x. From the above definition derive the definitions of: (i) conditional entropy,

$$H(x|y) = -\sum\nolimits_{x \in X} \sum\nolimits_{y \in Y} p(x, y) \log_2 [p(x|y)] \tag{2}$$

quantifying the entropy of a random variable x conditional upon the knowledge of another random variable y; and (ii) mutual information,

$$I(x; y) = \sum_{x,y} p(x, y) \log_2 \frac{p(x, y)}{p(x)\, p(y)} = H(x) - H(x|y) \tag{3}$$

denoting the amount of information gained about y as a result of knowing x. In terms of our mutual information theoretic feature selection filter, the random variables x and y can be used to represent features and class labels: x can be used to denote a feature within the dataset, and y can be used to denote a class label. The information theoretic measures help quantifying how likely the machine learner is to correctly predict the class label, for any given instance, as a result of learning a given feature. Once mutual information is estimated, one can rank the features based on their capability to predict the target and selected accordingly. We point out that this approach to feature selection inherently relies on the assumption that classifier performance is linked to the amount of mutual information shared between the class label and a feature, *i.e.* the greater the number of high-ranking features selected for classifier training, the better the classifiers perform in terms of correctly identifying the class label for any given instance. However, this approach disregards the potential for better subsets to exist, comprising features that are not sequentially ranked in terms of their mutual information values.

Computing the equations from (1) to (3) requires the knowledge of probability measures $p(x)$, $p(y)$ and $p(x, y)$. Since these quantities are frequently unknown *a priori* for any given datasets, we invoke a widely-used histogram-based approach [41] to estimate the probability distribution. Generally *histogramming* is known to introduce estimation bias due to sensitivity to bin size.

The sliced ECG time (sliding window) for this experiment is 0.6 s which is equivalent to the interval between heartbeats at a typical rate of 100 beats per minute [30]. However, the slice time can be changed, and may therefore affect the authentication performance, and this relationship is discussed in Section III. The detailed process flow for the training and testing phases is summarized in Fig. 3.

The training phase generates the reference regression functions for each sample (i.e., entity) using the DT technique and stores all functions as a database. This database is then used to compare the ECG data when new ECG data are detected during the testing phase. The sampling time period for the training data was set to 50s. The sampling time period for the testing data should be shorter due to the properties of the SCK use case category. The detection of the ECG testing data should be faster because the SCK use case considers a scenario in which employees are entering a company building. Accordingly, the sampling time period for testing was set to 15s. The core process generates reference regression functions for each set of ECG training data. Some of the trained reference functions are shown in Fig. 4 and these can be compared with the ECG testing data without fixing the sampling frequency.

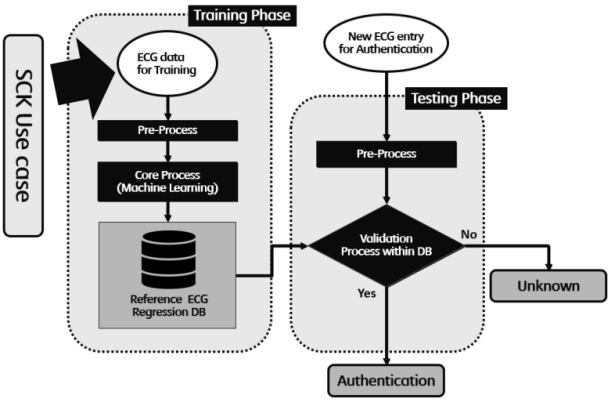

FIGURE 3. Process flow for ECG-based authentication in the SCK use case.

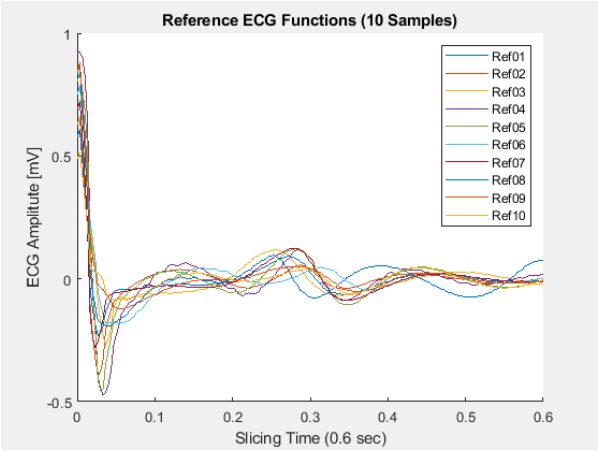

FIGURE 4. The reference ECG regression functions for the SCK use case.

TABLE 2. Authentication confusion matrix for SCK use case I.

122		Actual ECG data	
		Known	Unknown
Predicted ECG data	Known	84	2
	Unknown	30	6

TABLE 3. Authentication confusion matrix for SCK use case II.

82		Actual ECG data	
		Known	Unknown
Predicted ECG data	Known	76	5
	Unknown	1	0

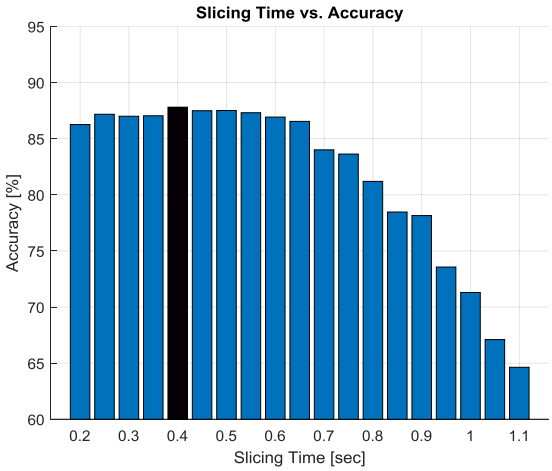

FIGURE 5. Authentication accuracy based on slicing time.

B. EXPERIMENTAL RESULTS

Authentication performance was evaluated by means of standard metrics [32] such as accuracy and recall a.k.a. sensitivity). Given the characteristics of the SCK use case, the authentication process focuses on the detection of unknown entities, thus the recall is defined as the ratio of the detected unknown and the total of unknown entities. We also applied a data quality measure based on the mean square error (MSE) before starting to detect the testing ECG data. The experiment was performed 150 times using 100 samples, with a sampling time period of 15s for the authentication testing and the confusion matrix. Notably, 28 out of the 150 ECG datasets (17.61%) were rejected because they did not meet the data quality criteria [22]. The resulting dataset consisted in 122 samples. The confusion matrix resulting from the experiment is shown in Table 2.

The values of the performance metrics are the following: overall accuracy 90/122 (73.77%); recall (proportion of unknown actually detected) 6/8 (75%).

The acceptance criteria for validation could be strengthened based on the quality of the training data (according to the upper control limit of the MSE). When these higher data quality criteria were used, the samples were reduced to 82. The corresponding confusion matrix is shown in Table 3.

The accuracy of this biometric authentication system was 76/82 (92.7%). However, the recall was 0. Notably, the values could vary because the ECG testing data were randomly selected for each trial to make the SCK use case more realistic.

III. SLICING AND SAMPLING TIME PERIOD DEPENDENCIES

Some ML performance measures depend on the ECG slicing time (sliding window). We gathered 70 samples from the various sources discussed above [31], [33], [34] and the HOS use case was addressed to find a relationship between the authentication performance and two key parameters: the sliding window size (i.e., ECG slice time) and the ECG data sampling time period. The relationship between the slicing time and authentication accuracy is shown in Fig. 5, revealing that the optimal slicing time is approximately half the average interval between heartbeats (0.4s).

We also investigated the relationship between sampling time period and authentication accuracy (Fig. 6). Although there was no clear relationship between these parameters, the

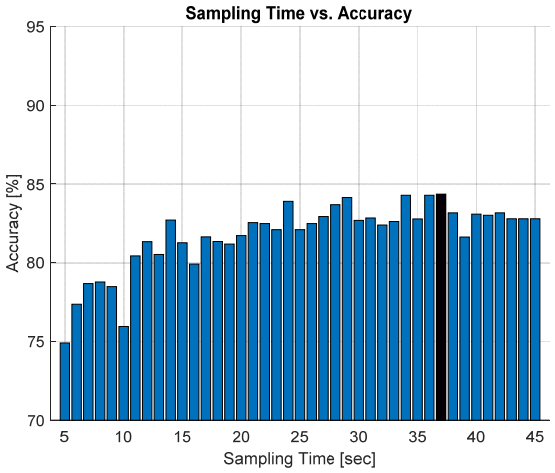

FIGURE 6. **Authentication accuracy based on sampling time period.**

optimal sliding time was 37 seconds in our experiment. The optimal slicing and sampling time periods may not remain the same if different datasets are used. However, our experiments clearly demonstrated that optimal values for these parameters exist and can be used to improve performance.

IV. CONCLUSION

In this paper, we proposed an enhanced ECG-based biometric authentication system for the SCK use case in which a regression-based interpretable ML approach was used to define the dataset boundaries and to acquire good-quality training data. We trained on a total of 90 ECG data samples to generate the reference function database. The reference function for each ECG data entity (i.e., identification) was then generated using a mutual-information-based DT regression approach. The authentication performance of the proposed system was evaluated not only with a confusion matrix but also by using the *amgecg* toolbox in MATLAB to analyze two key parameters: the ECG slicing time (sliding window) and the sampling time period. We found that a sliding window of 0.4s achieved the best performance and that the optimal sampling duration is 37s. In conclusion, using these optimized parameters, the proposed authentication system is able to achieve accurate results.

APPENDIX

The *amgecg* toolbox v.0.5 [22] and WFDB toolbox v0.10.0 [35] were used to design our authentication system. The corresponding MATLAB codes are available on GitHub[1] for users to try the demonstrations.

REFERENCES

[1] F. Agrafioti, J. Gao, D. Hatzinakos, and J. Yang, "Heart biometrics: Theory, methods and applications," in *Biometrics*, J. Yang, Ed. Rijeka, Croatia: InTech, 2011, pp. 199–216.
[2] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*. New York, NY, USA: Springer, 2011.
[3] F. Agrafioti, F. M. Bui, and D. Hatzinakos, "Secure telemedicine: Biometrics for remote and continuous patient verification," *J. Comput. Netw. Commun.*, vol. 2012, Oct. 2012, Art. no. 924791.
[4] M. Li and S. Narayanan, "Robust ECG biometrics by fusing temporal and cepstral information," in *Proc. 20th Int. Conf. Pattern Recognit. (ICPR)*, Istanbul, Turkey, Aug. 2010, pp. 1326–1329.
[5] J. R. Pinto and J. S. Cardoso, "Towards a continuous biometric system based on ECG signals acquired on the steering wheel," *Sensors*, vol. 17 no. 10, p. 2228, 2017.
[6] G. E. Forsen and M. R. Nelson, "Personal attributes authentication techniques," Rome Air Develop. Center, Pattern Anal. Recognit. Corp., Rome, NY, USA, Tech. Rep. RADC-TR-77-333, 1977.
[7] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Cao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018.
[8] 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.
[9] 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.
[10] 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.
[11] H. Kim and S. Y. Chun, "Cancelable ECG biometrics using compressive sensing-generalized likelihood ratio test," *IEEE Access*, vol. 7, pp. 9232–9242, 2019.
[12] J. R. Koza, F. H. Bennett, D. Andre, and M. A. Keane, "Automated design of both the topology and sizing of analog electrical circuits using genetic programming," in *Artificial Intelligence in Design*. Dordrecht, The Netherlands: Springer, 1996, pp. 151–170.
[13] F. Camastra and A. Vinciarelli, *Machine Learning for Audio, Image and Video Analysis: Theory and Applications*, 2nd ed. New York, NY, USA: Springer, 2015.
[14] A. Mincholé and B. Rodriguez, "Artificial intelligence for the electrocardiogram," *Nature Med.*, vol. 25, no. 1, pp. 22–23, 2019.
[15] E. Tatara and A. Cinar, "Interpreting ECG data by integrating statistical and artificial intelligence tools," *IEEE Eng. Med. Biol. Mag.*, vol. 21, no. 1, pp. 36–41, Jan. 2002.
[16] H. J. Kim and J. S. Lim, "Study on a biometric authentication model based on ECG using a fuzzy neural network," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 317, no. 1, 2018, Art. no. 012030.
[17] 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, 2013.
[18] 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.
[19] 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 IC-TSP*, Vienna, Austria, Jun. 2016, pp. 656–659.
[20] 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," 2017, *arXiv:1708.08189*. [Online]. Available: https://arxiv.org/abs/1708.08189
[21] B. E. Manjunathswamy, A. M. Abhishek, J. Thriveni, K. R. Venugopal, and L. M. Patnaik, "Multimodal biometric authentication using ECG and fingerprint," *Int. J. Comput. Appl.*, vol. 111, no. 13, pp. 33–39, 2015.
[22] S. K. Kim, C. Y. Yeun, E. Damiani, and N. W. Lo, "A machine learning framework for biometric authentication using electrocardiogram," *IEEE Access*, vol. 7, pp. 94858–94868, 2019.
[23] *Use Cases*. Accessed: Feb. 1, 2019. [Online]. Available: https://www.usability.gov/how-to-and-tools/methods/use-cases.html
[24] P. Gupta. *Decision Trees in Machine Learning*. Accessed: Feb. 1, 2019. [Online]. Available: https://towardsdatascience.com/decision-trees-in-machine-learning-641b9c4e8052
[25] J. R. Quinlan, "Induction of decision trees," *Mach. Learn.*, vol. 1, no. 1, pp. 81–106, 1986.
[26] M. van Gerven and S. Bohte, "Artificial neural networks as models of neural information processing," *Frontiers Comput. Neurosci.*, vol. 11, p. 114, Dec. 2017. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fncom.2017.00114/full

[1] https://github.com/amangkim/ECGRegreSec

[27] L. Yann. *LeNet-5, Convolutional Neural Networks*. Accessed: Feb. 1, 2019. [Online]. Available: http://yann.lecun.com/exdb/lenet/
[28] W. Yu, K. Yang, Y. Bai, H. Yao, and Y. Rui, "Visualizing and comparing convolutional neural networks," Jun. 2019, *arXiv:1412.6631*. [Online]. Available: https://arxiv.org/abs/1412.6631
[29] R. D. Labati, E. Muñoz, V. Piuri, R. Sassi, and F. Scotti, "Deep-ECG: Convolutional neural networks for ECG biometric recognition," *Pattern Recognit. Lett.*, to be published. doi: 10.1016/j.patrec.2018.03.028.
[30] American Heart Association. *All About Heart Rate (Pulse)*. Accessed: Feb. 1, 2019. [Online]. Available: https://www.heart.org/en/health-topics/high-blood-pressure/the-facts-about-high-blood-pressure/all-about-heart-rate-pulse
[31] A. Taddei, G. Distante, M. Emdin, P. Pisani, G. B. Moody, C. Zeelenberg, and C. Marchesi, "The European ST-T database: Standard for evaluating systems for the analysis of ST-T changes in ambulatory electrocardiography," *Eur. Heart J.*, vol. 13, pp. 1164–1172, Sep. 1992.
[32] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, 2005.
[33] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, Jun. 2000. [Online]. Available: http://circ.ahajournals.org/content/101/23/e215.full
[34] M. H. Imam, C. K. Karmakar, H. F. Jelinek, M. Palaniswami, and A. H. Khandoker, "Detecting subclinical diabetic cardiac autonomic neuropathy by analyzing ventricular repolarization dynamics," *IEEE J. Biomed. Health Inform.*, vol. 20, no. 1, pp. 64–72, Jan. 2016.
[35] I. Silva and G. B. Moody, "An open-source toolbox for analysing and processing physionet databases in MATLAB and octave," *J. Open Res. Softw.*, vol. 2, no. 1, p. e27, Sep. 2014. doi: 10.5334/jors.bi.
[36] Y.-W. Bai, W.-Y. Chu, C.-Y. Chen, Y.-T. Lee, Y.-C. Tsai, and C.-H. Tsai, "Adjustable 60 Hz noise reduction by a notch filter for ECG signals," in *Proc. IEEE Instrum. Meas. Technol. Conf.*, Como, Italy, May 2004, pp. 1706–1711.
[37] A. R. Verma and Y. Singh, "Adaptive tunable notch filter for ECG signal enhancement," *Procedia Comput. Sci.*, vol. 57, pp. 332–337, Jan. 2015.
[38] E. Ebrahimzadeh, M. Pooyan, S. Jahani, A. Bijar, and S. K. Setaredan, "ECG signals noise removal: Selection and optimization of the best adaptive filtering algorithm based on various algorithms comparison," *Biomed. Eng., Appl. Basis Commun.*, vol. 27, no. 4, pp. 1–13, Jul. 2015.
[39] P.-Y. Chen, M.-J. Chang, K.-C. Tu, S.-S. Yu, and C.-C. Liu, "Study of using Fourier transform to capture the ECG signals between awakeness and dozing," in *Proc. IS3C*, Xian, China, Jul. 2016, pp. 1055–1058.
[40] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–426, 1948.
[41] G. Egnal, "Image registration using mutual information," Univ. Pennsylvania, Philadelphia, PA, USA, Tech. Rep. MS-CIS-00-05, 1999.

EBRAHIM AL ALKEEM received the bachelor's degree in communication engineering and the master's degree in information security from Khalifa University of Science and Technology, where he is currently pursuing the Ph.D. degree. He is a Global Digital Leader specializing in the effects of artificial intelligence and other rapidly developing technologies on the economy, healthcare, and society, focusing on threats and opportunities created by these new developments. During his 13 years in the cybersecurity industry, he has worked with many technologies in various technical and management positions. He currently manages the ENEC Information Security Department as the acting Chief Information Security Officer. He has presented many international and domestic seminars. He has published many articles in the field of security. In 2015, he has received the Tamayaz Excellence Award in recognition of his work and inventions in the field of information technology and smart services. He is an active member of many of engineering associations across the world.

SONG-KYOO (AMANG) KIM received the M.S. degree in computer engineering and the Ph.D. degree in operations research from the Florida Institute of Technology, in 1999 and 2002, respectively. He is a Research Scholar with the Khalifa University of Science and Technology. He has been an Associate Professor with several UAE universities. Before moving to the Gulf region, he was a core Faculty Member of the Asian Institute of Management, providing courses in technology, innovation, and operations. Before his academic career, he was the Technical Manager of the Mobile Communications Division, Samsung Electronics, for more than ten years and mainly dealt with technology management in the information technology industry. He has been an Invited Speaker with many international conferences concerning technology management and innovation process. He is the author of over 70 research articles. He holds ten patents relating to the mobile technology industries. His current research area include artificial intelligence and ECG-based biometric security. He is also an External Reviewer of the IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING.

CHAN YEOB YEUN received the M.Sc. degree in information security from Royal Holloway, in 1996, and the Ph.D. degree in information security from the University of London, in 2000. After the Ph.D. degree, he joined Toshiba TRL, Bristol, U.K., and later became the Vice President of LG Electronics, Mobile Handset R&D Center, in Seoul, South Korea, in 2005. He was responsible for developing mobile TV technologies and related security. He left LG Electronics, in 2007, and joined KAIST, South Korea, until August 2008, and then the Khalifa University Science and Technology, in September 2008. He is currently a Researcher in cybersecurity including the IoT/USN security, cyber-physical system security, cloud/fog security, and cryptographic techniques. He is also an Associate Professor with the Department of Electrical Engineering and Computer Science Department and an active member of the Center for Cyber-Physical Systems (C2PS). He also enjoys lecturing for the M.Sc. degree students information security and the Ph.D. degree engineering courses with the Khalifa University of Science and Technology. He has published over 100 journal articles and conference articles and seven book chapters. He held ten international patent applications. He also serves on the editorial board of multiple international journals and on the steering committee of international conferences.

MOHAMED JAMAL ZEMERLY received the M.Sc. degree from University College Cardiff, Wales, and the Ph.D. degree from The University of Birmingham, U.K., in 1986 and 1989, respectively. Since 1989, he was with various U.K. universities, such as UCL, Warwick, and Westminster, and then moved to Khalifa University of Science and Technology, in 2000, where he is currently an Associate Professor. He was the Research Program Chair (and ex-Computer Engineering Program Chair) of the Electrical and Computer Science Department for the M.Sc. degree. He has published over 100 journal and conference papers as well as eight book chapters. He is also the Co-Editor-in-Chief of the IJRFIDSC journal of the Infonomics Society. His research interests include ubiquitous computing, augmented reality, image processing and computer vision, context aware mobile systems, and information security. He was the Co-Program Chair of the ICITST Conference Series for the years 2011 and 2012. He was also the Co-Chair of the same conference, from 2014 to 2015.

KIN FAI POON received the bachelor's degree from the University of Sunderland, in 1995, and the master's degree in digital systems engineering, and the Ph.D. degree, in 2002. He is currently a Chief Researcher, leading the network optimization theme with Emirates ICT Innovation Centre (EBTIC), Khalifa University of Science and Technology, setting out research and development directions to downstream research activities to EBTIC partners. He won the IET outstanding Student Prize. He has contributed numerous technical articles and published four book chapters. He has filed five patents. Prior to joining EBTIC, he was a member of the Intelligent Systems Research Centre, working as a Network Optimization Consultant with British Telecom (BT), U.K. He was responsible for the design and implementation of new algorithms to solve telecom network problems. In 2003, he left BT and became the co-founder of evolved networks working as a research and development principle to commercialize some of the BT software applications. His main interests include network planning, graph theory, hardware and software development, and optimization techniques, in particular evolutionary algorithms.

GABRIELE GIANINI received the M.Sc. degree in physics, in 1992, and the Ph.D. degree in physics, in 1996. Since 2005, he has been an Assistant Professor with the Department of Computer Science, Università degli Studi di Milano, Italy. Since 2017, he has been a Senior Research Fellow of EBTIC/Khalifa University of Science and Technology. He has held visiting positions at a number of international institutions, including INSA de Lyon, France, and the University of Passau, Germany, CERN, Geneva, Switzerland, Fermilab, Chicago, USA, and CBPF, Brazil. From 2005 to 2012, he was an Adjoint Professor with the Free University of Bolzano, Italy. Since 1992, he has coauthored about 200 articles published in internationally refereed journals and conferences. His research interests include statistical and soft computing techniques for machine learning and big data, quantitative modeling of processes, and game theoretic applications to networking and to security.

PAUL D. YOO is currently with the CSIS, Birkbeck College, University of London, and leading the Data-Driven Cyber Security Laboratory under the Birkbeck Institute of Data Analytics (BIDA). He is also affiliated with the University of Sydney and the Korea Advanced Institute of Science and Technology (KAIST) as a Visiting Professor. Prior to this, he held academic/research posts with the Defence Academy, Cranfield, U.K., Sydney (USyd), and South Korea (KAIST). In his career, he has amassed more than 70 prestigious journal and conference publications. He has been awarded more than 2.3 million US$ in project funding and a number of prestigious international and national awards for his work in advanced data analytics, machine learning, and secure systems research, notably the IEEE Outstanding Leadership Award, the Capital Markets CRC Award, the Emirates Foundation Research Award, and the ICT Fund Award. Most recently, he won the prestigious Samsung Award for research to protect the IoT devices. He serves as an Editor for the IEEE COMML and the *Journal of Big Data Research* (Elsevier). He is a Fellow of the HEA.