 doi:10.20944/preprints202206.0223.v1

Article

An Intelligent Multimodal Biometric Authentication Model for Personalised Healthcare Services

Farhad Ahamed [1]*, Farnaz Farid [1], Basem Suleiman [2,],Zohaib Jan [3],Luay A. Wahsheh [4],Seyed Shahrestani [1]

[1] Western Sydney University; farhad.ahamed@westernsydney.edu.au,farnaz.farid@westernsydney.edu.au,s.shahrestani@westernsydney.edu.au
[2] The University of Sydney; basem.suleiman@sydney.edu.au
[3] University of South Australia; muhammad.jan@unisa.edu.au
[4] University of Tennessee at Chattanooga; luay-a-wahsheh@utc.edu
* Correspondence: farhad.ahamed@westernsydney.edu.au

Abstract: With the advent of modern technologies, the healthcare industry is moving towards a more Personalised smart care model. The enablers of such care models are the Internet of Things (IoT) and Artificial Intelligence. These technologies collect and analyse data from persons in care to alert relevant parties if any anomaly is detected in a patient's regular pattern. However, such reliance on IoT devices to capture continuous data extends the attack surfaces and demands high-security measures. Both patients and devices need to be authenticated to mitigate a large number of attack vectors. The biometric authentication method has been seen as a promising technique in these scenarios. To this end, this paper proposes an AI-based multimodal biometric authentication model for single and group-based users' device-level authentication that increases protection against the traditional single modal approach. To test the efficacy of the proposed model, a series of AI models are trained and tested using physiological biometric features such as ECG (Electrocardiogram) and PPG (Photoplethysmography) signals from five publicly available datasets from Physionet and Mendeley data repositories. The multimodal fusion authentication model shows promising results with 99.8% accuracy and an Equal Error Rate (EER) of 0.16.

Keywords: biometrics; ECG; Internet of Things; machine learning; Personalised Healthcare; PPG; Smart Aging

1. Introduction

In recent years, Personalised Healthcare (PH) has gone through promising advances with the potential to provide a customised type of care based on specific patient health and by using predictive analytic [1]. PH relies on data from patients' health records and measurements to predict unknown issues that might arise concerning the patient's health. For example, PH could help patients forecast how much weight they might gain in the coming two months, considering their daily diet. Daily habits, diets and other lifestyle-related factors can cause someone to get diabetes or dementia earlier than expected. Early prediction of potential health issues can help proactively address them and provide adequate therapy before it worsens. Consequently, PH can help to improve the quality of care and decrease its related costs.

A reliable PH system comprises several key components, as shown in Figure 1. In a PH system, various types of data about a patient are gathered through continuous monitoring of their health. The procedure includes utilising multiple devices, including the Internet of Things (IoT) sensors and smart devices. Patients discharged from hospitals, patients living remotely and the elderly living in residential care can take advantage of such remote health monitoring. By remote monitoring of health status through IoT devices, the patients' personal health data can be stored in a highly-secured cloud-based data source. The monitoring data can then be used to perform intelligent analysis, often using cloud-based

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

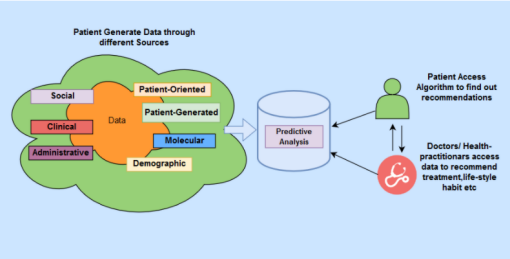

Figure 1. PH Healthcare Architecture

services, to predict potential health issues. In this model, the communication channel needs to be actively and continuously passing the data of the monitored patient to re-enforce the learning by the predictive analysis model. However, security and privacy concerns remain among the significant challenges, especially in PH systems, due to the reliance on IoT and cloud-based technologies [2]. In particular, the authentication challenges of these systems are unique because the IoT-based sensors and smart devices frequently produce a continuous stream of data and thus, require continuous authentication to ensure that the data belongs to a particular patient. Specifically, the device's legitimacy needs to be continuously verified in a sensor-based PH network (a network of connected devices and IoT sensors that monitor a patient's health).

Therefore, in such a context, it becomes challenging to verify that a set of sensors belong to the same PH network and they trust each other in providing and sharing patient data. Let us assume a PH network that belongs to a patient, Bob and has sensors A, B, C and D. Alice, on the other hand, has a PH network with three different sensors X, Y and Z. Assume there is a rouge sensor W which tries to impersonate Bob or Alice's network. In this case, the challenge is to employ a reliable method to verify that Bob's sensors should trust each other in sharing and communicating Bob's data but not Alice's and the rough sensors. Such settings stimulate the need for a *continuous authentication* method to verify that a set of sensors belongs to the same patient. Thus, it can trust that the data belongs to the same patient. Figure 2 depicts this scenario.

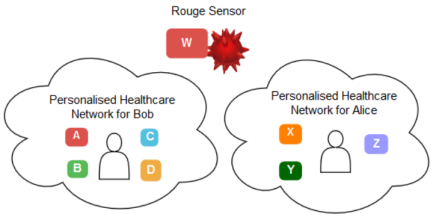

Figure 2. Scenario: Single User Authentication

The second type of scenario that instigates such an authentication method involves a PH network that belongs to a group of users instead of a single user. They might be from the same household sharing the same network. Figure 3 illustrates this scenario. Let us assume that Bob and Alice share the same PH network in this context. The sensors A, B, C, D adjunct to Bob and Alice. The intruder, Eve, tries to intrude the network using a rouge sensor W. In this case, the network should employ an authentication method to authenticate and verify Bob and Alice's devices continuously and reject the rough sensor from Eve. Such contexts also advocate for a robust *continuous authentication* method to scrutinise a group of persons and their sensors belonging to a specific network.

In this paper, to address the challenges mentioned above, we propose a multimodal biometric-based authentication model that comprises continuous single and group user and device authentication in PH network environments. We utilise a person's unique physiological characteristics that are continuously monitored using various IoT sensors to classify real users and intruders. Our method aims to overcome the potential security flaws in such sensors by employing a person's biological features that can be very difficult to borrow,

 doi:10.20944/preprints202206.0223.v1

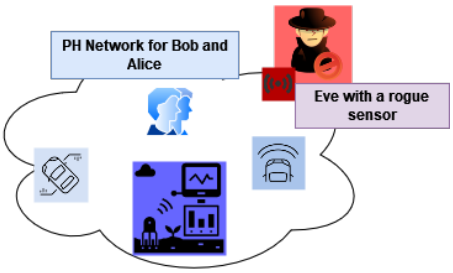

Figure 3. Scenario: Group User Authentication

buy or forge. To achieve this, the performance of the multimodal authentication method over a single modal is empirically investigated and analysed. Single modal authentication utilises and considers a user's single biometric trait (e.g., ECG), which is still feasible to be compromised given the advancement in computation [3]. Unlike single signal modal, multimodal authentication considers more than one characteristic of the human body while processing an authentication scheme. Such approaches can result in higher accuracy and a higher security level, making spoofing, device impersonation and replay attacks harder to occur [4]. Therefore, we devise a multimodal individual and group-based biometric authentication, which will combine the features among a few common biometric traits such as ECG and PPG. The systematic approach investigates both user and device authenticity. Furthermore, we employ various machine learning algorithms and empirically evaluate the performance of our proposed method. The objectives and novel contributions of our work are:

- We propose the first comprehensive deep learning-based multimodal authentication model applying ECG and PPG signals fusion. Our objective is to prevent user impersonation and device spoofing in the personalised healthcare network, heavily dependent on IoT based sensors.
- Our model incorporates a two-level authentication to detect intruding users and devices. The developed approach first enrols the authorised users using their multiple biometric traits. It then attaches IoT sensors using those traits to an individual. Such methods prevent the impersonation of both users and devices. It can easily detect the presence of an intruder in IoT-based healthcare services.
- We have conducted extensive experiments over multiple public datasets, demonstrating the model's efficiency for biometric authentication purposes, compared to the previous research works that have used most of these datasets for clinical research perspectives.
- To the best of the authors' knowledge, very few works have addressed the device-level authentication and audit mechanisms of IoT- based personal healthcare services.

The rest of this paper is organised as follows. In section 2, we present background and motivation for multimodal continuous authentication method. The related works are also described with a concise view. In section 3, the overall system architecture and relevant algorithms and models are narrated. In section 4, multiple types of attack scenarios are discussed in relation to biometric-based authentication. In section 5, details of the dataset, experiments and the results are presented, followed by a discussion on the findings in section 6. Finally, 7 illustrates the limitation of our work and 8 section summarises the objective, outcome, and future direction of this work.

2. Background and Related Works

Biometric authentication has grown in popularity with the effective use and adoption of IoT networks, especially in PH [2]. Many continuous authentication techniques have recently emerged to offer more reliable solutions to the growing challenges. In continuous authentication, users are monitored with a high frequency to validate their authority for a particular session [5]. Compared with the traditional authentication process, continuous

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

authentication mechanisms are equipped with a higher level of security and are well-known for enhanced Quality of Experience (QoE) [6]. Continuous authentication incorporates behavioural and physiological signal-based biometric authentication, which can make the IoT networks more secure, which are prone to impersonation and injection attacks [7].

The use of IoT sensors in any system poses serious security challenges [2]. The PH systems which are heavily dependent on such sensors are not exceptional. Figure 4 summarises the main security threats that IoT device layer authentication techniques can face in such contexts.

1. **Device impersonation attack:** The attacker impersonates a device pretending to be an authenticated user [8].
2. **Injection attack:** The attacker deploys malicious nodes to monitor or control the data flows in the network [9].
3. **Side-channel attack:** The attacker reads the leaked signals from a device to collect and analyse sensitive data [10].
4. **Eavesdropping and interference:** This type of attack is caused by a weakened connection between an IoT device and the server. The intruder takes advantage of such a vulnerable connection to intercept network traffic [11].
5. **Sleep deprivation attack:** The attacker keeps the targeted node out of its sleep mode to reduce its lifetime [12].
6. **DDoS attack:** The attackers generate a large amount of traffic from compromised devices to make services unavailable [2].
7. **Replay attack:** The imposter produces a signal to control IoT devices [2].
8. **Man in the middle attack:** The attacker hacks the communication channel between two nodes and spoofs or interrupts communications [2].

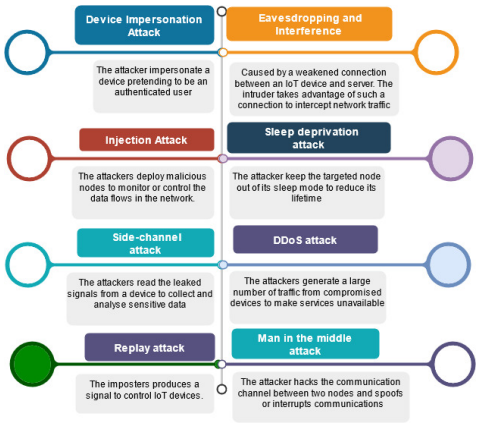

Figure 4. IoT Network Attacks

Many studies have focused on biometric behavioural and physiological authentication in IoT healthcare networks since wearables and inertial sensors are gaining popularity. One of the critical advantages of physiological signals over physiological features is their sense of life [13]. ECG-based authentication has also gained growing interest, particularly for continuous authentication scenarios [14]. For instance, the work in [15] proposed an ECG-based cancelable biometric scheme that mitigates replay attacks. In [16], the authors proposed a continuous authentication mechanism that incorporates sequential sampling and One-Dimensional Multi-Resolution Local Binary Patterns extraction to identify users over using ECG signals. The work in [17] defined a unified sparse representation framework that uses joint and specific ECG signal patterns.

ECG-based authentication mechanisms can be further classified based on feature extraction techniques. For instance, studies such as [1,18] have applied fiducial feature extraction in their identification algorithms. Many other studies [19,20], on the other hand, have used non-fiducial feature extraction techniques. Other studies, such as [21,22], have

 doi:10.20944/preprints202206.0223.v1

combined the benefits of fiducial and non-fiducial extraction to form a hybrid approach for ECG-based authentication.

Some work, such as [23] focused on investigating various classification algorithms to identify the best performing one for ECG-based authentication. Out of eight algorithms, the study concluded that linear discriminant analysis (LDA), k-nearest neighbour, and neural networks are best for ECG-based identification. Furthermore, it also concluded that principal components analysis (PCA) has no noticeable impact on the classification process performance but can lead to accuracy reduction.

A few studies have proposed PPG-based authentication methods. For example, In [13], the authors studied the feasibility of using PPG data for authentication. They concluded that the results heavily depend on the quality of data.

In [24], the authors combined both behavioural and physiological biometric features for user identification. Specifically, they employed Gait and PPG as the biometric trait. Their experimental results showed that Support Vector Machine (SVM) has superior performance to KNN and Autoencoder Neural Network, although KNN achieved the fastest performance. Furthermore, they noticed that with sample size increment, the gap between KNN and Linear SVM accuracy becomes smaller.

Besides the above studies, some research work considered multimodal authentication approaches. In [25], the authors implemented a multimodal biometric authentication method integrating face and iris based on score level fusion. The performance excels the performance of the unimodal biometric identification method and the previous fused face-iris methods.

In [26], the authors adopted a SVM based multimodal approach for identification. They applied a score level fusion approach, and k means clustering to classify a multi SVM machine. A nonlinear classifier is used to allow the SVM to perform a 'two-dimensional' classification of a set of originally one-dimensional data.

In [27], a multimodal authentication model is proposed. The work applies a combination of ECG and fingerprint to authenticate the users and reports an EER of 0.1%. However, the ECG only authentication method denotes a 90% accuracy.

The authors in [28] designed a PPG based nonfiducial biometric authentication method. They apply Continuous Wavelet Transform (CWT) and Direct Linear Discriminant Analysis (DLDA) and attained an EER of 0.5%-6%.

The study in [29] uses ECG and finger vein for multimodal authentication. The researchers report an EER of 0.12% and 1.40% with feature and score fusion. They apply Multi-Canonical Correlation Analysis (MCCA) with a range of classifiers, namely: Support Vector Machine (SVM), K-Nearest Neighbors (KNNs), Random Forest (RF), Naive Bayes (NB), and Artificial Neural Network (ANN).

The authors in [30] propose two multimodal authentication systems, which are sequential and parallel system and uses a combination of ECG and Fingerprint. They apply Convolution Neural Network (CNN) and Q-Gaussian multi-support vector machine (QG-MSVM). They attained an EER of 0.14% and 0.10% for the sequential systems using two datasets. The parallel system achieves an EER of 0.40% and 0.32% for respective datasets.

Table 1 presents the overview of similar works to our study. Many studies have focused on multimodal biometric authentication. However, only a few studies have comprehensively experimented with ECG and PPG signals. For example, the study [31] was one of the few to use both ECG and PPG signals to detect spoof detection and authentication. However, the method uses ECG and PPG signals separately. As a result, the processing time for this model is 85.31 ms with an accuracy of 98.9%. The other prominent work in this sense is the one reported in [28]. The authors denote an EER of 0.05 while combining ECG, PPG and GSR with 25 subjects. However, the EER and details results in the case of fused ECG and PPG have not been precisely reported. Additionally, the research did not scrutinise the in-depth study of the applied classification algorithms and feature extraction methods. Another recent work that has used ECG and PPG for biometric authentication is [32]. The study uses ECG and PPG signals separately for authentication. The MATLAB

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

functions applied for feature extraction and classification are not explained explicitly. As a result, it is hard to reproduce the reported results.

Compared to other studies, our work proposes a novel biometric-based continuous model that takes advantage of ECG and PPF fusion. We also consider user impersonation and device spoofing by incorporating continuous authentication with biometric signal fusion. Apart from this, our model also considers single-user and multi-user mode authentication. We converse a series of machine learning and deep learning algorithms such as SVM, KNN, Naive Bays, Ensemble, Generalised Additive Model (GAM), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM) to address user and device level continuous authentication in PH networks. We test our models with a range of publicly available datasets. We have also made our code publicly available so that the other researchers can reproduce the results and propose further improvements.

Table 1. Comparisons with other Machine Learning-based Biometric Authentication Studies

Study	Signal type	Method	Results
[27]	ECG, Fingerprint	Score Fusion	Accuracy: ECG: 90.0%, ECG+Fingerprint: EER: 0.1%
[29]	ECG, Finger Vein	SVM, KNNs, RF,NB and ANN	EER: 0.12%, 1.40%
[28]	PPG	CWT and DLDA	EER: 0.5%-6%
[30]	ECG and Finger print	CNN and QG-MSVM	EER: 0.14%, 0.10%, 0.40% and 0.32%
[32]	ECG, PPG	Cross-Correlation Function (CCF)	Accuracy: PPG: 99.98%, ECG: 88.79%
[33]	PPG	Naïve Bayes classifier	Achieved a recognition rate of 98.65%, 97.76%, and 99.69%
[34]	PPG	Decision Tree, KNN, Random Forest	Achieved accuracy rate of 93%, 98%, and 99% respectively
[35]	PPG	Gradient boosting tree (GBT)	Accuracy: over 90% and false detection rate: 4%
[31]	Fused ECG and PPG	CNN	Accuracy: 98.9%
[36]	PPG	CNN	AUC of 78.2% and 83.2%
[37]	ECG, PPG, GSR	Classifiers	Equal Error Rate (EER): 0.05 for 25 subjects

2.1. Machine Learning Algorithms

In this part, to brief the readers, we present some concise pieces of background information on the classification and deep learning algorithms used in our work.

2.1.1. SVM

We have used SVM along with other classification algorithms. It constructs a hyperplane in multidimensional space to differentiate different classes [38]. In this work, we have two classes, AUTH to indicate the data of authenticated users and NAUTH, to indicate the signal data of intruder SVM generates optimal hyperplane in an iterative manner that is used to minimise any error in estimation. The core idea of using SVM is to find a maximum marginal hyperplane that best divides the signal dataset into AUTH and NAUTH classes. The SVM applies a decision function $f(X) > 0$ or $f(X) < 0$, to separate the input examples into two classes, where $X = (x^1..., x^d)$ with d being the dimension. The size of the training set N can be derived as y^i, x^i, with $i = 1, ..., N, x^i \in R^n$ as the input part for the *i-th* example,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

and the class label of $y^i \in -1,1$. SVM maps X^i to a higher dimensional feature space that depends on a nonlinear function $\phi(X)$, optimising the separated hyperplane through maximisation of the margin with the following quadratic equation:

$$Maximise : \sum_{i=1}^{n} \alpha_i - \frac{1}{2} \sum_{j=1}^{n} \alpha_i y_i K(K_i, X_j) \alpha_j y_j \tag{1}$$

$$Subject\ to : \sum_{i=1}^{n} \alpha_i y_i = 0, 0 <= \alpha_i <= C(i = 1, ..., n) \tag{2}$$

where $\alpha >= 0$ and it will be equal to 0 after optimisation. C expresses a degree of losing constraint where it is a positive constant that was chosen by the user. This mean that having a large value number of C would result in more accurate classification during the learning phase. If $K(x, X^{'})$ is the kernel function which is inner a product defined by $K(x, X^{'}) = \phi(X)$, Then the SVM decision function is narrated as:

$$f(x) = \sum_{x_i \in SV} \alpha_i y_i K(X_i, X) \tag{3}$$

with a common polynomial kernel that can be defined as follows:

$$K(X, X^{'}) =< \phi(X), \phi(X^{'}) > \tag{4}$$

2.1.2. Naive Bayes

Naive Bays classifiers are one of the most popular families of machine learning algorithms formulated on the simple probabilistic theorem. All Naive Bayes algorithms are based on the principle that all features are independent for any given classes [39].

Assume that $F_1, F_2, ..., F_m$ are m feature variables, a test instance t can be represented by a feature vector $< f_1, f_2, \ldots, f_m >$, where f_i is the value of F_i. Let V represent the class variable and v represent the value.

Assume that all features are fully independent given the class, NB uses the following equation to classify t.

$$v(t) = \arg\max_{v \in V} P(v) \prod_{i=1}^{m} P(f_i|v). \tag{5}$$

where $v(t)$ class value of t, prior probability $P(v)$ and the conditional probability $P(v_i|c)$.

2.1.3. KNN

KNN is a simple supervised algorithm that relies on the assumption that data with similar attributes will most likely have similar outcomes [40]. In KNN, the decision is taken based on the similarity between a given training and test sets. The training examples are asserted using a number n of attributes, and each of these attributes denotes a point in n-dimensional space using distinct classes. To predict the unknown data set, it calculates the closest distance between the K training sets. A given dataset DS, where D is a matrix of features from a data point, and L is a class label. KNN then will estimate the conditional distribution of L given D and classify a data point to the class with the highest probability. Given a positive integer k, KNN looks at the k observations closest to a test data point d_0 and estimates the conditional probability that it belongs to class c using the following formula:

$$P(L = c|D = d_0) = \frac{1}{k} \sum_{i \in S_0} I(l_i = c) \tag{6}$$

where S_0 is the set of k-nearest observations and $I(l_i = c)$ is an indicator variable that is equal to 1 if a given data point d_i, l_i in S_0 is a member of class c, and 0 if otherwise. After

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

estimating these probabilities, KNN classifies the data point d_0 under the class in which the previous possibility is the greatest.

2.1.4. Ensemble Bagged Tree

Ensemble methods combine several machine learning methods in a single predictive model to minimise variance and bias or maximise prediction probability. Bootstrap aggregating (Bagging) [41] is one of the earliest ensemble methods which create and integrate multiple classification modes to solve a specific classification problem. This method has been widely applied in biometric signal processing [42,43].

2.1.5. GAM

The generalised additive model applies shape functions to capture the nonlinear relationship between a predictor and the response variable. These are interpretable models that explain class scores using single and bi-variate shape functions of predictors [44]. The standard GAM uses a univariate shape function for each predictor.

$$y \sim Binomial(n, \mu) \tag{7}$$

$$g(\mu) = log\frac{\mu}{(1-\mu)} = c + f_1(x_1) + f_2(x_2) + ... + f_p(x_p) \tag{8}$$

where y is a response variable that follows the binomial distribution with the probability of success (probability of positive class) μ in n observations. $g(\mu)$ is a logic link function, and c is an intercept (constant) term. $f_i(x_i)$ is a univariate shape function for the ith predictor, which is a boosted tree for a linear term for the predictor (predictor tree).

2.1.6. CNN

CNN is a particular type of neural network that can extract spatial and temporal dependencies from data, and this method is widely applied to digital images. More about CNN can be found here [45].

2.1.7. LSTM

LSTM is a particular type of deep neural network that can capture repetitive features in the data [46]. It is widely used for time series data to extract features in the time domain.

2.2. Feature Extraction

We have applied both time domain and joint time-frequency domain feature extraction methods to the physiological signals in this work. These features improved the accuracy and EER of the ML model from the processed signals. Wavelet Packet Transform (WPT), a joint time-frequency domain method, has been applied with the time-domain extraction method based on the AutoRegressive (AR) model. The justification for using these methods is detailed in the consequent subsections. We extracted Shanon's Entropy values, Wavelet variances, and AR coefficients from the signals. Figure 5 depicts the role of feature extraction process in the proposed intrusion detection model.

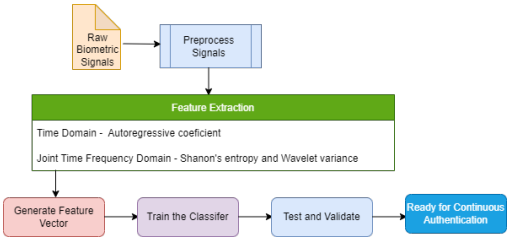

Figure 5. Feature Extraction for the Proposed Model

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

2.2.1. Wavelet Packet Transform

Wavelet packet transform (WPT) is an extension of wavelet decomposition (WD)[47]. This method is chosen for its efficiency for non-stationary signal denoising, compression and classification. It also allows the features to have more discrimination power than the features from discrete wavelet transform.

The wavelet packet transform function of a signal $f(x)$ can be defined as[48]:

$$W_s f(x) = f(x) * \Psi_s(x) = \frac{1}{s} \int_{-\infty}^{+\infty} f(t)\Psi(\frac{x-t}{s})dt \tag{9}$$

where s is a scale factor.$\Psi_s(x) = \frac{1}{s}\Psi(\frac{x}{s})$ is the dilation of a basic wavelet $\Psi(x)$ by the scale factor s.

The scale factor acts as a linear operator and divides the signals into two components: approximation and detail. The approximation then can split itself into another approximation and detail. The process can be repeated till the signal that correlates well with the frequencies required for the classification of the signal is retained in the wavelet coefficients [49]. Figure 6 shows the wavelet tree for the ECG signal from one of the datasets.

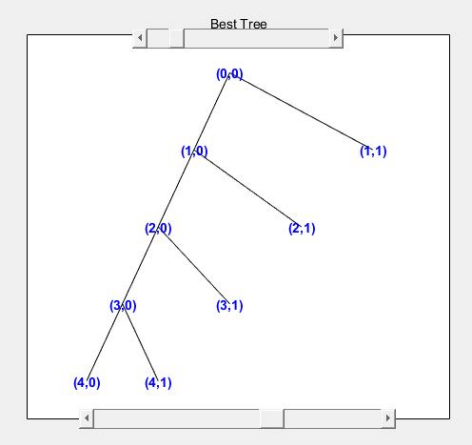

Figure 6. ECG Wavelet Tree

However, with wavelet packet decomposition, the massive size of the decomposed coefficient can be a hurdle for classification. Entropy has been introduced to tackle such issues in WPD. It is prevalent in measuring the uncertainty of data in signal processing. There are different types of entropy. Some of them are Shannon's entropy (SE), Log Energy Entropy (LEE), Renyi Entropy (RE), and Tsallis entropy (TE) [50].

The entropy function is defined is as follows:

$$E_{ij} = \sum_{k=1}^{N} E_{ijk} \tag{10}$$

$$E_{ij} =< x(i), x(j), x(k) >= |d_{jk}|^2 \tag{11}$$

where k is the number of coefficients, j is the number of nodes and i is the level on the node. The probability of the coefficients can be calculated as follows:

$$Px_i = \frac{E_{ijk}}{E_{ij}} \tag{12}$$

The entropy can be defined as follows:

$$H(X) = -\sum_{i=1}^{n} Px_i log_2 Px_i \tag{13}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

where P represents the probability, $x_i = 1, ..., i$ represents the possible outcomes, being:

$$0 < Px_i < 1, \sum_{i=1}^{n} Px_i = 1 \tag{14}$$

2.2.2. Autoregressive Model (AR)

The Autoregressive model is a time series model that analyses the values from the previous time steps using a linear combination of past values of the variables to predict future values. Here autoregression refers to a regression of the variable against itself. Implementing the AR model includes some levels of randomness and uncertainty, where future values can be predicted based on the past value. In most cases, the AR Model predicts a trend close to accuracy to be useful for the given problem.

In an AR process of order p, the signal X_t with the time instant t will be represented as a linear combination of p previous values of the same signal. The AR process is modelled as:

$$X_t = \sum_{i=1}^{p} \varphi_i X_{t-1} + \epsilon_t \tag{15}$$

where ϵ_t represents the white noise with a zero mean, var ϕ_i represents the i-th coefficient of the model. It uses the authentication model's coefficients as the feature input of the classifier. We tune various "AR process order" to tune the accuracy and precision of the best classification model for a scenario.

2.2.3. Instantaneous Frequency (IF)

The IF is a property of a non-stationary signal such as ECG that has a time-varying parameter relating to the average of the frequencies present in the signal as it evolves. Further details regarding the IF can be found in [51]. The IF features of the ECG and PPG signals are used to train and test the CNN and LSTM models.

2.2.4. Spectral Entropy (SE)

SE is a property of a signal measured from the spectral power distribution. The SE treats the signal's normalized power distribution in the frequency domain as a probability distribution, and calculates the Shannon entropy of it. Further details of SE can be found in [52]. The SE feature values of the ECG and PPG signals are used for CNN and LSTM models.

3. System Design

This section elaborates on our designed physiological biometric-based device authentication system based on continuous authentication techniques. Figure 7 illustrates our system. The system uses two phases to verify a legitimate device - the enrolment phase and the constant authentication phase. The enrolment phase includes both user and device registration. The preliminary step of device registration is user registration.

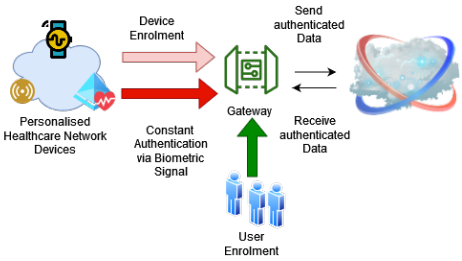

Figure 7. High-level Overview of the Proposed Authentication

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

At first, a range of biometric signals s_i where $i = 1, 2, 3, ..., n$ signifies a series of biometric signals. These are collected from a valid user u_i. The system is trained using a machine learning model to recognise legitimate users. The model has training and testing phases. In the training phase, the manager will use the right signal to make the model recognise the correct user. In the testing phase, the manager uses the reference dataset to test the success rate of the recognition.

The system progresses to the device registration after the user registration phase. In this stage, the PH manager instructs the device to send biometric signals such as ECG and PPG for a specific time window from the attached user. The manager then uses the previously created model to authenticate and register the device in the system.

In the authentication phase, a device is asked to log in using the biometric signal of the attached user. If the model can recognise the signal, the device is authenticated. Otherwise, the system will request a higher privilege to reset the sensor or data to be passed or lock the device to prevent further access. On the other hand, continuous authentication makes sure that the device is constantly audited. This prevents session impersonation. After the device is authenticated, it will continuously send the biometric signal maintaining a short interval (every 20 seconds), and the manager will monitor the transmitted data. If the sensor starts to send the wrong data at any point in time, the device will be locked out from the network.

Figure 8 illustrates the flow.

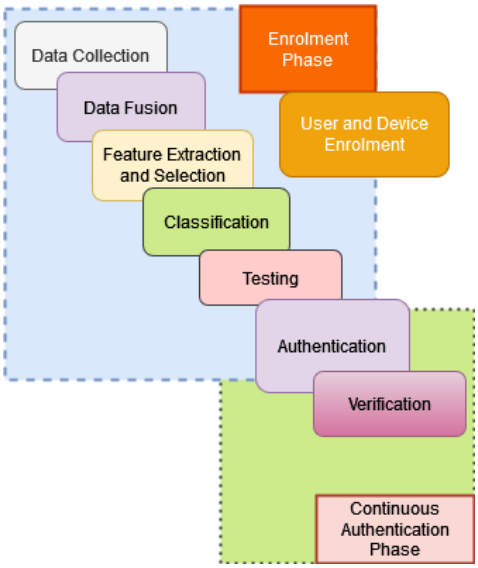

Figure 8. The Workflow of the Proposed Authentication

3.1. Algorithm Details

Let s_i be a set of signals from a user u_i. In our case, s_i is a set of multiple signals such as ECG_i and PPG_i.

$$s_i = (ECG_i, PPG_i) \tag{16}$$

The signal is collected for a time period w_i from a user u_i. A device d_i is trained with the signal for a time period $trnw_i$. The device is tested with the signal for a time period $tstw_i$. Then horizontal concatenation is performed on the signals to derive a single metric.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

Algorithm 1 User Registration

Input : An array $[s_i]$, $i = 1, 2, \cdots, n$, where each element is a biometric signal
Output: Registration Notification
`/* The device manager collects biometric signals from` $[u_i]$ `legitimate users */`
while *Input Signals from* $[u_i]$ *user r number of records=true* **do**
  The manager trains the system with authenticated and non-authenticated signals;
  for *r=0; r<=n; r++* **do**
    Feature Selection;
    Divide into Train and Test data;
    Train=TrainData;
    Test=TestData;
    End train the system;
    Test;
  end
  if *Test successful* **then**
    register user $[u_i]$;
    go to the next user;
  end
end

Algorithm 2 Device Registration

Input : An array $[s_i]$, $i = 1, 2, \cdots, n$, where each element is a biometric signal
Output: Device Registration Notification
`/* The device manager compares the device signal` $[s_i]$`, with the user signal` $[u_i]$ `*/`
while *Input Signals from* $[d_i]$ *matches the signal of* $[u_i]$ **do**
  register device $[d_i]$;
  go to the next device;
end

Algorithm 3 Authentication

`/* A PH device sends data to manager */`
if *Valid Device* **then**
  Let the device send data;
end
else
  Reject entry;
end

Algorithm 4 Continuous Verification

`/* In every 5 minutes Time Window */`
if *The device signal matches with the stored signal* **then**
  Let the device send data;
end
else
  Ask to re-login to the system;
end

3.2. Data Fusion

We have applied a few early fusion methods to process multimodal signals. This section provides a brief description of each of these methods.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

- **Horizontal concatenation:** As part of horizontal concatenation, the data is stored as a form of a matrix at first. As a result, we get two matrices for ECG, and PPG signal consecutively:

$$M_{ECG} = \begin{bmatrix} x_1^{ECG} \\ x_2^{ECG} \\ . \\ . \\ . \\ x_n^{ECG} \end{bmatrix} \tag{17}$$

$$M_{PPG} = \begin{bmatrix} x_1^{PPG} \\ x_2^{PPG} \\ . \\ . \\ . \\ x_n^{PPG} \end{bmatrix} \tag{18}$$

The resultant concatenate matrix is as follows:

$$C_{EPG} = \begin{bmatrix} x_1^{ECG} + x_1^{PPG} \\ x_2^{ECG} + x_2^{PPG} \\ . \\ . \\ . \\ x_n^{ECG} + x_n^{PPG} \end{bmatrix} \tag{19}$$

- **Root Mean Square (RMS):** The RMS denotes the statistical measure of the mean square root of a set of data points. For a set of D number of data points and d_i data items, the RMS is calculated as:

$$RMS = \sqrt{\frac{1}{D}\sum_{i=1}^{D} d_i^2} \tag{20}$$

- **Geometric Mean (GM):** The GM implies a type of mean that calculates the central tendency of a set of numbers. It uses the root of the product of the observed items. For a set of D number of data points and d_i data points under observation, the GM is expressed as:

$$GM = \prod_{i=1}^{D} d_i = \sqrt[D]{d_1 d_2 \dots d_{ND}} \tag{21}$$

- **Arithmetic Mean (AM):** The AM denotes the central tendency of a set of numbers that applies the sum of observed items. For a set of D number of data points and d_i items under observation, formally the AM can be calculated as:

$$GM = \prod_{i=1}^{D} d_i = \sqrt[D]{d_1 d_2 \dots d_{ND}} \tag{22}$$

- **Harmonic Mean (HM):** The harmonic mean denotes the reciprocal of AM of a given set of data points. It inverses each data points in a given set, sums those data points and then the sum is divided by the total number of data points.

$$GM = \prod_{i=1}^{D} d_i = \sqrt[D]{d_1 d_2 \dots d_{ND}} \tag{23}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

4. Security Analysis

This section verifies the informal security analysis of our proposed model to ensure that it can defend against numerous prevalent attacks that persist in sensor-based PH systems. The following scenarios assume that an imposter tries to control the whole PH network through several well-known security breaches.

- **Impersonation and Spoofing Attack:** IoT sensors are prone to impersonation and spoofing attacks. The device, which is attached to patients, is usually verified at the beginning of any session. During the ongoing session, if the intruder inherits the device and pretends to be the user, the patient's data privacy is at risk. However, continuous authentication prevents the system from such an attack. Also, using multimodal biometric signals to authenticate instead of unimodal prevents a spoofing attack from device and user perspectives.
- **Injection and Tampering Attack:** The network that adopts the proposed authentication approach is also secure from an injection attack. If attackers want to implant a node in the patient's PH network, they will not be able to do so as the biometric trait will not match. Node tampering attack is also prevented as even if the intruders intrude on the node and implant a new biometric authentication signal, the network will reject the device.
- **Registration Phase Attack:** An imposter can register a rough device into the PH network during the registration phase. However, to mitigate this attack in our model, we use two-step registration: user registration and device registration. As a result, a device is only registered if it is attached to any previously registered legitimate user.

5. Experiment Design and Results Analysis

We have used a few publicly available datasets to experiment with the proposed authentication algorithm detailed in this section. We have implemented our model using MATLAB. The design and implementation are done in a few steps: data acquisition and pre-procession, feature extraction and selection, and finally, classification. The workflow diagram of the authentication ML model is presented in Figure 9.

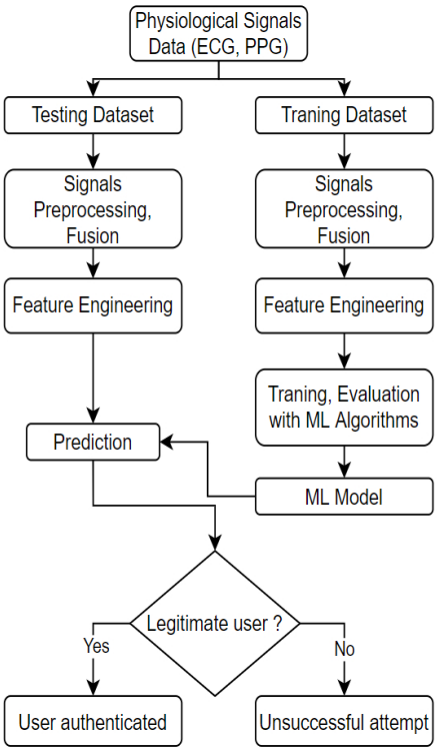

Figure 9. The workflow of creating ML based authentication model

 doi:10.20944/preprints202206.0223.v1

The notable elements of the workflow are as follows:

1. **Physiological Signals:** The signals are classified as authenticated and non-authenticated signals. As the name suggests, authenticated signals refer to signals registered into the database that are collected from a trusted source. The non-authenticated signals attribute to the signals from an unknown source/user that needs identification/authentication.
2. **Data Preparation:** As the physiological data being obtained are mostly raw sensor data, data pre-processing is required. Some of the techniques that are used in this stage are band-pass and noise filtering to remove the noise and artefacts from the collected signal.
3. **Feature Engineering:** For single signal experiments, the features are directly extracted using the feature extraction algorithm. For multimodal experiments, we apply early fusion and then extract and select features from the fused signals.
4. **Identification:** The unknown signal is processed, and features are extracted from the signal in this stage. Then the authentication algorithm is run to check the authenticity against the stored patterns of the authenticated users.

In this research work, we have used five datasets. All the signals in each dataset have been grouped in a single mat file. The signals are labelled as AUTH for authenticated users and NAUTH for non-authenticated signals.

We use the work from [53] as a reference point to design our feature extraction part. We extract between 18 to 34 features for each experiment. Then the most important features are selected based on the chi-square test. All derived features are concatenated into a feature vector. The detail of our code is available in Github [54].

The classification algorithms described previously are used to train and test the model. The parameters for each classification algorithm are selected based on the optimal performance. We define this performance benchmark by tuning several parameters and running each experiment at least five times. For example, when using the SVM algorithm, we have chosen the polynomial kernel function for SVM to classify each trial to estimate the misclassification rate and the confusion matrix. We selected the polynomial kernel function since our model is parametric. The polynomial function also works better if the model uses fewer data. Since we are training our model with authenticated user data, we do not expect a lot of data for this type of PH system.

We have used multiple metrics to evaluate our model. Ten-fold cross-validation is used to estimate the misclassification rate and construct the confusion matrix. Then we have derived the accuracy precision rate, recall rate, F1 score, model loss and Equal Error Rate (EER) for each of our experiments. Each of these metrics is calculated using True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN). We have a range of specific settings for unimodal and multimodal signal experiments. The following subsections detail the experiment settings and results, including the dataset details.

5.1. Dataset Details

Our research work focuses on two different physiological signals: ECG and PPG, to detect any network intruder. Most of the published research works primarily focus on a single physiological signal, ECG being the dominant one. We have used five datasets for our study based on their diversity and vastness.

BIDMC PPG and Respiration Dataset [55] This dataset is available at Physionet [56]. The collected data was from the admitted patients to the intensive care unit. The dataset consists of 53 patients' recordings. Each of the recorded signal is 8 minutes long in duration. Each recording contains:

- ECG and PPG signals, both of these signals are sampled at 125Hz.
- Some of the physiological parameters such as heart rate and respiratory rate and blood oxygen saturation level. These are sampled at 1Hz.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

MIT-BIH Arrhythmia Database [57] This dataset is also available at Physionet [56]. It is a clinical dataset of 47 participants of 48 half-hour excerpts of two channels ambulatory ECG recordings. Twenty-three recordings were randomly selected from a set of 4000 24-hour ambulatory ECG recordings. These recordings are from a mixed population of inpatients and outpatients of the hospital. The rest of the records were picked from the same group to include less common but clinically significant arrhythmia, however, in this experiment we will use the samples for biometric purposes.

MIT-BIH Normal Sinus Rhythm Database This dataset is extracted from Physionet [56]. The ECG data were collected at Boston's Beth Israel Hospital from 18 subjects. The subjects include five males between 26 and 45 years old and 13 females between 20 and 50 years old.

The BIDMC Congestive Heart Failure Database [58] This database contains ECG recordings from 15 subjects. Each record has 20 hours of recording. The dataset details are available at [59].

Real-World PPG dataset [60] This dataset contains PPG signals from 35 healthy subjects. Each recording has 300 samples (6 seconds) with a 50 sample/seconds sampling rate. Each subject has 50 to 60 recordings. The dataset details are available at [60].

5.2. Performance Benchmarking

To utilize the secure personalised healthcare network and usable authentication, performance benchmark of the system needs to be drawn from the following conditions,

- Using shorter training data (5 minutes or less amount of physiological signal) to develop a highly accurate authentication model.
- ML model accuracy needs to be close to 100% to prevent intrusive unauthorised access to sensors.
- The ML model training and validation should be power and processing efficient and highly accurate.

5.3. Experiments and Results

This section illustrates our experiment design and results. We have conducted three sets of experiments that involve ECG, PPG and fusion signal combining ECG and PPG. We run a series of single and group user authentication involving multiple classification algorithms for each type of signal. A set of experiments focused on single signal mode authentication with selected features, and other sets of experiments used multimodal mode and IF and SE features to address group user authentication. AR coefficients, Shannon's entropy and wavelet variance features are extracted for all signals. The most optimal parameters are chosen after running each experiment five times. Table 2 illustrates the parameters we set for our first set of experiments.

Table 2. ECG Experiment Settings

Parameters	Values
AR Order	12
Transform Level	8
Window Size	1000
Feature Extracted	276

CNN and LSTM deep learning models are introduced for ECG and PPG fusion based authentication and to compare single user vs group based authentication. A sample CNN model is presented in Figure 10. The CNN net has eight connected layers. Each of the connected layers is sequenced as follows, one-dimensional convolution layer, followed by the normalisation layer, then the dropout layer, followed by another one-dimensional convolution layer, then the dropout layer, Rectified Linear Unit (ReLU) layer, the dropout layer, then followed by next additional layer. Finally, the network is connected with a fully

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

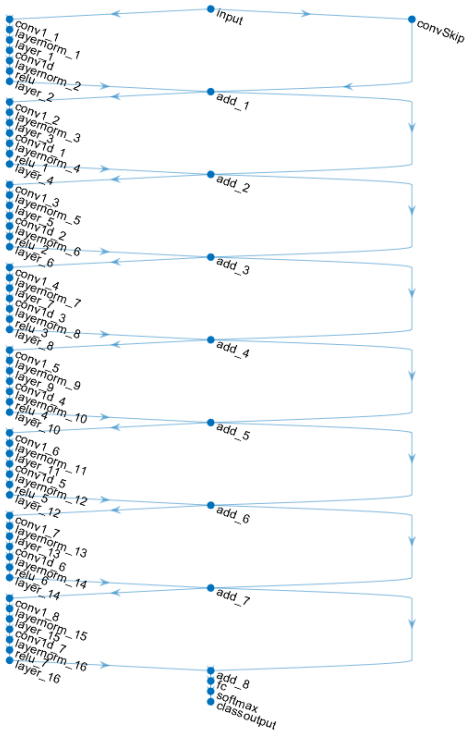

Figure 10. The CNN model for Data-Fusion-Centric Authentication

connected layer, softmax activation layer and classification output layer. The LSTM model for the experiments is presented in Figure 11.

The LSTM model consists of Sequence Input Layer, bi-LSTM layer, fully connected layer, softmax layer followed by classification output layer. Further details about the models and the source code can be found in [54].

5.3.1. ECG Signal Based Authentication

The first experiment for ECG signals has been conducted using the ECG signals of 53 users from BIMDC dataset [55].

The dataset was initially divided into two portions – "TrainA" and "TestA". One of the users, "UserA" from "TrainA" is marked as the authenticated user, and the rest of all the data from "TrainA" and "TestA" are considered intruders. The ECG signal data of "UserA" and other users is about 7 minutes long. These signals are processed to create multiple instances of an equal length of 9 seconds. The data of "UserA" was then further partitioned to 33% training and 67% testing data. The training samples of "UserA" are copied multiple times to increase the training instances that will allow overtraining of the authenticated user, and through this overtraining, it will enhance the security of the biometric model to identify the authenticated user.

Additionally, it will improve data balance and symmetry during the training session. The dataset of the remaining users from "TrainA" and the users of "TestA" are also processed to create 9 seconds length samples. Multiple machine learning classifier algorithms are used and compared to find the best performer within the training set and tested with the test samples. The outcome of the test results of 2533 samples is presented in Table 3.

To validate the scalability of the biometric model, subsequently, we run the second experiment for ECG signal adding the combination of three datasets which are: MIT-BIH Arrhythmia Database [57], MIT-BIH Normal Sinus Rhythm Database [56], and BIDMC Congestive Heart Failure Database [58]. We use the ECG records of 120 users. All these 120 users are regarded as intruders. The result of the test of 10213 samples is presented in Table 4.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

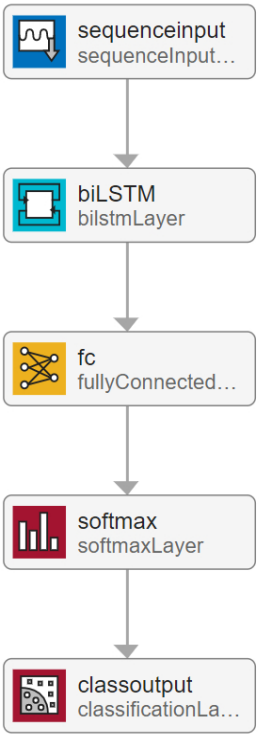

Figure 11. The LSTM Model for Data-Fusion-Centric Authentication

Table 3. ECG Result Details

ML Algorithm	Sensitivity	Precision	Accuracy	F1 Score	EER
KNN Fine	75.6%	47.7%	98.3%	85.6%	0.013
Ensemble Bagged Trees	95.1%	65.0%	99.1%	97.1%	0.03
Naive Bayes	95.1%	100%	99.9%	97.5%	0.03
SVM	100%	26.1%	95.4%	97.6%	0.02
GAM	97.6%	41.7%	97.8%	97.7%	0.02

Table 4. ECG Result Details - Scalable Attack Scenarios

ML Algorithm	Sensitivity	Precision	Accuracy	F1 Score	EER
KNN Fine	75.6%	38.3%	99.4%	85.9%	0.12
Ensemble Bagged Trees	100%	9.6%	96.2%	98.1%	0.19
Naive Bayes	95.1%	100%	99.9%	97.5%	0.02
SVM	100%	2.63%	85.2%	91.9%	0.08
GAM	97.6%	5.3%	93.1%	95.2%	0.05

After performing the single-user authentication for ECG only signals, we experimented with the ECG only group authentication. For this experiment, a group of three is created, considering that they belong to the same personal healthcare network. ECG signals from these three users are regarded as authenticated users, and the others are considered

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

intruders. We use the same strategies to process ECG signals, labelling, feature extractions, training and testing as single-user experiments.

Multiple ML algorithms are used to find the best performing model. Out of these algorithms, the SVM receives the given number of features in the learning phase and performs a grid search optimisation algorithm to find the optimal normalisation resolution factor α. Then the machine derives the normalisation resolution factor with the remaining features by comparing them with those being used in the learning phase. The code for our SVM template is as follows:

```
template = templateSVM(...
    'KernelFunction','polynomial',...
    'KernelScale','auto',...
    'BoxConstraint',1,...
    'Standardize',true);
model = fitcecoc(...
     trainFeatures,...
     train_n_test_label,...
     'Learners',template,...
     'Coding','onevsone', ...
     'ClassNames',{'AUTH','NAUTH'});
```

The source codes of all the experiments and related files are available in Github [54].

The model using Naive Bayes did not perform well in the multiuser authentication model. Out of the algorithms used to train the model, GAM performed comparatively better with a precision of 52.6% and EER 0.04. The results are presented in Table 5.

Table 5. ECG Result Details - Multiuser Authentication

ML Algorithm	Sensitivity	Precision	Accuracy	F1 Score	EER
KNN Fine (3 Usr)	85.5%	31.6%	90.9%	88.2%	0.09
Ensemble Bagged Trees (3 Usr)	91.1%	42.9%	95.3%	93.3%	0.05
Naive Bayes (3 Usr)	82.3%	43.2%	94.3%	88.1%	0.06
SVM (3 Usr)	100.0%	7.7%	45.8%	60.3%	0.54
GAM (3 Usr)	91.1%	52.6%	95.9%	93.5%	0.04

5.3.2. PPG Signal Based Authentication

We set up the PPG signal based authentication experiment using a similar data preprocessing technique as ECG experiments. We combined two PPG datasets which are BIMDC [55], and PPG real-world datasets [60]. The combined sample user number is 66. We follow similar procedures to create 9 seconds length sample points for the training and testing portion of the data. Multiple training algorithms are used and compared to find the best performing algorithm to create a model. Then the models are tested with the test samples. Similar parameters as Table 2 are used to extract features from the signals.

The results of the single user authentication using PPG are presented in Table 6.

To validate the group based multiuser authentication, a group of three is created. PPG from these three users are regarded as authenticated users, and the others are considered as intruders. AR coefficients, Shannon's entropy and wavelet variance features are extracted. The transform level, the window size of the signal and other settings are already mentioned in Table 2. The results from the test samples are presented in Table 7.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

Table 6. PPG Result Details - Single User Authentication

ML Algorithm	Sensitivity	Precision	Accuracy	F1 Score	EER
KNN Fine	75.6%	4.9%	79.8%	77.7%	0.20
Ensemble Bagged Trees	97.6%	12.8%	91.0%	94.1%	0.09
Naive Bayes	100%	6.8%	85.5%	92.1%	0.15
SVM	56.1%	9.7%	92.3%	69.9%	0.08
GAM	97.6%	11.3%	89.6%	93.4%	0.10

Table 7. PPG Result Details - Multiuser Authentication

ML Algorithm	Sensitivity	Precision	Accuracy	F1 Score	EER
KNN Fine (3 Usr)	70.2%	13.8%	79.0%	74.5%	0.21
Ensemble Bagged Trees (3 Usr)	52.4%	32.7%	93.0%	67.5%	0.07
Naive Bayes (3 Usr)	56.5%	6.9%	63.9%	60.1%	0.36
SVM (3 Usr)	48.4%	17.6%	87.5%	62.8%	0.13
GAM (3 Usr)	77.4%	28.2%	90.1%	83.6%	0.10

5.3.3. ECG-PPG Fusion Signal Based Authentication

Consequently, experiments are conducted with ECG and PPG fused signals from the BIMDC dataset [55]. This dataset has over 6 minutes of these two signals of each 53 users. Several fusion techniques were used to validate which fusion signal will provide better result as described in the data fusion section. At first, we simply add the amplitude of the ECG and PPG signals and apply classifier machine learning algorithms as follows. Firstly, from the fused signal we extract Shanon's Entropy (SE), Wavelet variances (WV) and AR coefficients. Then we train and test the model to recognise a single authenticated user. The signal data of each user are processed and prepared to create smaller sample data points where each data point contained around 9 seconds length of signal (worth 11 heartbeats). Training and testing portions of the data are separated in 70/30 proportion.

Multiple training algorithms are used to train the model. To select the best performing model, many tests are conducted on the trained model using the testing sample portion of the dataset. The extracted features based on Table 2 parameters are used to train multiple classifiers. However, the above-mentioned classifiers with time and time-frequency joint features have not achieved a promising result. The model was trained to apply the ten-fold cross-validation method. Additionally, EER and F1 score was considered in selecting the best model. The best performing classification model trained using GAM achieved a precision of 44.4% and EER of 0.02.

We have tried different fusion methods and extracted some new features to improve the result further. We also create smaller sampling points by reducing the frequency. The preprocessed data is proportion to 70/30 for the training and testing. We conduct the fusion using Square Root (SQRT), RMS, GM, AM and HM. A detailed discussion of these metrics has been provided in the data fusion section. All these metrics except HM produce good results for the fusion signal. For further fusion signal based experiments, we use RMS fusion as standard as it provided slightly better F1 scores than other fusion approaches that were applied. We have extracted IF and SE features as described in [61]. These features are used in deep learning models: CNN and LSTM. LSTM model is specialized in finding

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0223.v1

Table 8. ECG-PPG Fusion Result Details - Single User Authentication

ML Algorithm	Sensitivity	Precision	Accuracy	F1 Score	EER
KNN Fine	70%	76.7%	98.4%	82.1%	0.15
Ensemble Bagged Trees	19.5%	61.5%	98.5%	32.6%	0.40
Naive Bayes	97.6%	29.9%	96.2%	96.9%	0.03
SVM	0.0%	0.0%	98.4%	0%	0.50
GAM	97.6%	44.4%	98.0%	97.8%	0.02
CNN (2 HB 1 Usr)	97.2%	92.1%	99.8%	98.5%	0.21
LSTM (2 HB 1 Usr)	94.4%	97.1%	99.8%	97.1%	0.16
CNN (8 HB 1 Usr)	85.7%	73.2%	99.2%	92.1%	0.85
LSTM (8 HB 1 Usr)	97.1%	94.4%	99.8%	98.5%	0.16
CNN (16 HB 1 Usr)	88.2%	40.5%	97.4%	92.7%	2.56
LSTM (16 HB 1 Usr)	70.6%	60.0%	98.6%	82.5%	1.39

patterns in a time series sequence. In the experiment of single-user authentication, LSTM has demonstrated precision and F1 score rate as 97.1% and EER 0.16. CNN has provided a precision rate of 92.1%, F1 score of 98.5% and EER of 0.21. Table 8 shows the comparison of the experiment results.

After conducting the single user experiments, we run the group based authentication experiments. The data processing and feature extraction method remains the same as in previous experiments. The results of the multiuser ECG-PPG Fusion experiments are presented in Table 9. Multiple LSTM training configurations are used as mentioned in 9. It is observed that when user group member size is increased, the accuracy decreases. However, when the window sample size is increased from two heartbeats to 8 heartbeats, the accuracy and EER change rate are changed to a negligible amount. It indicates that the model trained with LSTM and a minimum of two HBs can provide an excellent authentication scheme.

Table 9. ECG-PPG Fusion Result Details - Multiuser Authentication

ML Algorithm	Sensitivity	Precision	Accuracy	F1 Score	EER
KNN Fine (3 Usr)	90.3%	37.0%	92.6%	91.5%	0.07
Ensemble Bagged Trees (3 Usr)	93.5%	50.7%	95.6%	94.6%	0.04
Naive Bayes (3 Usr)	90.3%	19.7%	82.8%	86.2%	0.17
SVM (3 Usr)	97.6%	27.4%	88.1%	92.4%	0.12
GAM (3 Usr)	98.4%	35.3%	91.7%	94.8%	0.08
CNN (16 HB 3 Usr)	88.7%	73.4%	97.5%	93.1%	2.45
LSTM (16 HB 3 Usr)	30.2%	21.3%	89.8%	45.6%	10.23
CNN (16 HB 5 Usr)	76.4%	91.9%	97.1%	86.4%	2.88
LSTM (16 HB 5 Usr)	83.1%	73.3%	95.5%	89.5%	4.88

6. Discussion

The objective of the experiments was to find the best continuous authentication model on (1) single signal vs fusion signal based authentication, and (2) single user vs group of user-based authentication, using conventional classifiers and contemporary deep learning algorithms. In Table 10 the summarised results presented from the experiments. From Table

 doi:10.20944/preprints202206.0223.v1

10 it is observed that in single authentication mode, among the classifiers, the Naive Bayes model has provided the best result for ECG-only authentication reaching 100% precision and 99.92% accuracy and zero false-positive cases out of 2533 test samples. The naive Bayes based model demonstrated resiliency against a large number of intrusion attacks during the scalability test. When 10213 samples were tested in the second experiment, this model experienced zero false-positive cases and reached an EER of 0.024. During the PPG only authentication experiments, none of the classifiers reached up to a good benchmark, although LSTM provided a comparatively better result [61]. In the case of ECG and PPG signals based on RMS type fusion, the deep learning LSTM model illustrated good precision and low EER compared to CNN based model, even though we chose to change signal sample length from 2 heartbeats to 16 heartbeats. It will ensure a multimodal and reliable authentication scheme.

Table 10. Summary of the Biometric Experiments

Type of Experiments	Top Algorithm	Precision	Accuracy	EER
Single User ECG	Naive Bayes	100%	99.9%	0.02
Single User PPG	SVM	9.7%	92.3%	0.08
Single User ECG and PPG Fusion	LSTM	97.1%	99.8%	0.16
Multi User ECG	GAM	52.6%	95.9%	0.04
Multi User PPG	Ensemble Bagged Trees	32.7%	93%	0.07
Multi User ECG and PPG Fusion	CNN	73.4%	97.5%	2.45

When multiple user groups of 3 and 5 are created to verify the group authentication model, overall authentication performance is reduced compared to ECG only model when using the classifiers. LSTM deep learning net provided satisfactory accuracy and precision. However, many valid login attempts are declined. Therefore, further research is required to improve the sensitivity and accuracy of group authentication. Based on the benchmark performance defined earlier, our proposed models can achieve high accuracy, especially in single and multiuser authentication, using Naive Bayes, LSTM and CNN, as illustrated in Table 10.

From our literature review, only a few notable works have reported ECG and PPG together as biometric traits for multimodal authentication systems. We present the comparison in Table 11.

Table 11. Comparison with Multimodal ECG and PPG Studies

Study	Feature Extraction	Authentication Type	Classifier	Result
[32]	MATLAB functions	Single User	Cross-Correlation	Accuracy: PPG: 99.98%, ECG: 88.79%, EER: Not reported
[31]	CNN and Naive Bayes	Single User	CNN	Accuracy: 98.9%, EER: Not reported
[28]	Not reported	Single User	Classifiers	Accuracy: Not Reported, EER: 0.20
This work	WPT, AR, IF and SE	Single and Multi User	LSTM, CNN, NB, GAM	Accuracy: Single User: 99.8%, EER: 0.16, MultiUser: 97.5%

7. Limitations

Our work has some limitations. Firstly, in the case of combined ECG and PPG signals, both single-user and multi-user authentication have room for further improvement. The error rate can be improved with further investigations. Secondly, we have analysed our model for impersonation and spoofing attacks, injection and tampering attacks and registration phase attacks. However, we did not explore DDoS, side-channel attacks, sleep deprivation, eavesdropping or man in the middle attacks for our model. We will model and test these attacks for our proposed method in our future work. Thirdly, the performance of the group authentication model in the case of fusion signal deteriorated compared to the ECG-only model. LSTM provided satisfactory accuracy and precision. However, many valid login attempts were rejected. Therefore, further research is required to improve the sensitivity and accuracy of group authentication.

8. Conclusion

This paper has proposed a multimodal biometric-based continuous authentication model for personalised healthcare services. We show the feasibility of multimodal single and group-based authentication mechanisms in such a network environment. We use both time domain and joint time-frequency domain feature extraction methods to extract useful features from ECG, PPG and fused ECG-PPG signals. Then we test the performance of each type of signal with different classifications as well as deep learning algorithms with fused data to enhance the performance of the model. ECG signal-based data works better than PPG and fused signals in most cases. However, adding PPG as a fused signal to ECG gives an extra layer of security for the users to minimise ECG spoofing attacks. Our future works involve further improving the fused signal and group-based authentication models.

Author Contributions: Conceptualization, F.A. and F.F.; methodology, F.A., F.F and B.S; validation, F.A., F.F. and B.S.; Simulation F.A.and F.F; writing—F.A and F.F.; writing—review and editing, F.A., F.F, B.S, Z.J and L.W; All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tuerxunwaili.; Nor, R.M.; Rahman, A.W.B.A.; Sidek, K.A.; Ibrahim, A.A. Electrocardiogram Identification: Use a Simple Set of Features in QRS Complex to Identify Individuals. In Proceedings of the Recent Advances in Information and Communication Technology 2016; Meesad, P.; Boonkrong, S.; Unger, H., Eds.; Springer International Publishing: Cham, 2016; pp. 139–148.
2. Hossain, M.S.; Muhammad, G.; Rahman, S.M.M.; Abdul, W.; Alelaiwi, A.; Alamri, A. Toward end-to-end biometrics-based security for IoT infrastructure. *IEEE Wireless Communications* **2016**, *23*, 44–51. https://doi.org/10.1109/MWC.2016.7721741.

3. Eberz, S.; Paoletti, N.; Roeschlin, M.; Kwiatkowska, M.; Martinovic, I.; Patané, A. Broken Hearted: How to attack ECG Biometrics. Internet Society, 2017.
4. Farid, F.; Elkhodr, M.; Sabrina, F.; Ahamed, F.; Gide, E. A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services. *Sensors* **2021**, *21*. https://doi.org/10.3390/s21020552.
5. Al-Naji, F.H.; Zagrouba, R. A survey on continuous authentication methods in Internet of Things environment. *Computer Communications* **2020**, *163*, 109–133. https://doi.org/https://doi.org/10.1016/j.comcom.2020.09.006.
6. Gonzalez-Manzano, L.; Fuentes, J.M.D.; Ribagorda, A. Leveraging user-related Internet of Things for continuous authentication: A survey. *ACM Computing Surveys (CSUR)* **2019**, *52*, 1–38.
7. Peris-Lopez, P.; González-Manzano, L.; Camara, C.; de Fuentes, J.M. Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things. *Future Generation Computer Systems* **2018**, *81*, 67–77. https://doi.org/https://doi.org/10.1016/j.future.2017.11.037.
8. Tu, S.; Waqas, M.; Rehman, S.U.; Mir, T.; Abbas, G.; Abbas, Z.H.; Halim, Z.; Ahmad, I. Reinforcement learning assisted impersonation attack detection in device-to-device communications. *IEEE Transactions on Vehicular Technology* **2021**, *70*, 1474–1479.
9. Kaji, S.; Kinugawa, M.; Fujimoto, D.; Hayashi, Y.i. Data injection attack against electronic devices with locally weakened immunity using a hardware Trojan. *IEEE Transactions on Electromagnetic Compatibility* **2018**, *61*, 1115–1121.
10. Gnad, D.R.; Krautter, J.; Tahoori, M.B. Leaky noise: New side-channel attack vectors in mixed-signal IoT devices. *IACR Transactions on Cryptographic Hardware and Embedded Systems* **2019**, pp. 305–339.
11. Ssettumba, T.; Abd El-Malek, A.H.; Elsabrouty, M.; Abo-Zahhad, M. Physical layer security enhancement for Internet of Things in the presence of co-channel interference and multiple eavesdroppers. *IEEE Internet of Things Journal* **2019**, *6*, 6441–6452.
12. Udoh, E.; Getov, V. Performance analysis of denial-of-sleep attack-prone MAC protocols in wireless sensor networks. In Proceedings of the 2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim). IEEE, 2018, pp. 151–156.
13. Sancho, J.; Alesanco, Á.; García, J. Biometric authentication using the PPG: A long-term feasibility study. *Sensors* **2018**, *18*, 1525.
14. Huang, Y.; Yang, G.; Wang, K.; Yin, Y. Multi-view discriminant analysis with sample diversity for ECG biometric recognition. *Pattern Recognition Letters* **2021**, *145*, 110–117. https://doi.org/https://doi.org/10.1016/j.patrec.2021.01.027.
15. Wu, S.; Chen, P.; Swindlehurst, A.L.; Hung, P. Cancelable Biometric Recognition With ECGs: Subspace-Based Approaches. *IEEE Transactions on Information Forensics and Security* **2019**, *14*, 1323–1336. https://doi.org/10.1109/TIFS.2018.2876838.
16. Louis, W.; Komeili, M.; Hatzinakos, D. Continuous authentication using one-dimensional multi-resolution local binary patterns (1DMRLBP) in ECG biometrics. *IEEE Transactions on Information Forensics and Security* **2016**, *11*, 2818–2832.
17. Huang, Y.; Yang, G.; Wang, K.; Liu, H.; Yin, Y. Learning Joint and Specific Patterns: A Unified Sparse Representation for Off-the-Person ECG Biometric Recognition. *IEEE Transactions on Information Forensics and Security* **2020**, *16*, 147–160.
18. Lim, C.L.P.; Woo, W.L.; Dlay, S.S.; Gao, B. Heartrate-Dependent Heartwave Biometric Identification With Thresholding-Based GMM–HMM Methodology. *IEEE Transactions on Industrial Informatics* **2019**, *15*, 45–53. https://doi.org/10.1109/TII.2018.2874462.
19. Hejazi, M.; Al-Haddad, S.; Singh, Y.P.; Hashim, S.J.; Abdul Aziz, A.F. ECG biometric authentication based on non-fiducial approach using kernel methods. *Digital Signal Processing* **2016**, *52*, 72–86. https://doi.org/https://doi.org/10.1016/j.dsp.2016.02.008.
20. Srivastva, R.; Singh, Y.N. ECG analysis for human recognition using non-fiducial methods. *IET Biometrics* **2019**, *8*, 295–305.
21. Bassiouni, M.M.; El-Dahshan, E.S.A.; Khalefa, W.; Salem, A.M. Intelligent hybrid approaches for human ECG signals identification. *Signal, Image and Video Processing* **2018**, *12*, 941–949.
22. Ergin, S.; Uysal, A.K.; Gunal, E.S.; Gunal, S.; Gulmezoglu, M.B. ECG based biometric authentication using ensemble of features. In Proceedings of the 2014 9th Iberian Conference on Information Systems and Technologies (CISTI). IEEE, 2014, pp. 1–6.
23. Pelc, M.; Khoma, Y.; Khoma, V. ECG signal as robust and reliable biometric marker: Datasets and algorithms comparison. *Sensors* **2019**, *19*, 2350.
24. Wu, G.; Wang, J.; Zhang, Y.; Jiang, S. A continuous identity authentication scheme based on physiological and behavioral characteristics. *Sensors* **2018**, *18*, 179.
25. Wang, F.; Han, J. Multimodal biometric authentication based on score level fusion using Support Vector Machine. *Opto-electronics review* **2009**, *17*, 59–64.
26. Kumar, G.S.; Devi, C.J. A Multimodal SVM Approach for Fused Biometric Recognition. *Int. J. Comput. Sci. Inform. Technol* **2014**, *5*, 3327–3330.
27. Kwon, Y.B.; Kim, J. Multi-modal authentication using score fusion of ECG and fingerprints. *Journal of information and communication convergence engineering* **2020**, *18*, 132–146.
28. Yadav, U.; Abbas, S.N.; Hatzinakos, D. Evaluation of PPG Biometrics for Authentication in Different States. In Proceedings of the 2018 International Conference on Biometrics (ICB), 2018, pp. 277–282. https://doi.org/10.1109/ICB2018.2018.00049.
29. El-Rahiem, B.A.; El-Samie, F.E.A.; Amin, M. Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein. *Multimedia Systems* **2021**, pp. 1–13.
30. Hammad, M.; Liu, Y.; Wang, K. Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint. *IEEE Access* **2019**, *7*, 26527–26542. https://doi.org/10.1109/ACCESS.2018.2886573.
31. Mousavi, F.S. Fusion of ECG and PPG Signals in Apply to Spoof Detection and Biometric Authentication. PhD thesis, University of Toronto (Canada), 2020.

32. Bastos, L.; Tavares, T.; Rosário, D.; Cerqueira, E.; Santos, A.; Nogueira, M. Double Authentication Model based on PPG and ECG Signals. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 601–606. https://doi.org/10.1109/IWCMC48107.2020.9148521.
33. Yang, J.; Huang, Y.; Zhang, R.; Huang, F.; Meng, Q.; Feng, S. Study on PPG Biometric Recognition Based on Multifeature Extraction and Naive Bayes Classifier. *Sci. Program.* **2021**, *2021*, 5597624:1–5597624:12.
34. Lee, S.W.; Woo, D.K.; Son, Y.K.; Mah, P.S. Wearable Bio-Signal (PPG)-Based Personal Authentication Method Using Random Forest and Period Setting Considering the Feature of PPG Signals. *J. Comput.* **2019**, *14*, 283–294.
35. Zhao, T.; Wang, Y.; Liu, J.; Chen, Y.; Cheng, J.; Yu, J. TrueHeart: Continuous Authentication on Wrist-worn Wearables Using PPG -based Biometrics. In Proceedings of the IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, 2020, pp. 30–39. https://doi.org/10.1109/INFOCOM41043.2020.9155526.
36. Luque, J.; Cortès, G.; Segura, C.; Maravilla, A.; Esteban, J.; Fabregat, J. END-to-END PHOTOPLETHYSMOGRAPHY (PPG) Based Biometric Authentication by Using Convolutional Neural Networks. In Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO), 2018, pp. 538–542. https://doi.org/10.23919/EUSIPCO.2018.8553585.
37. Blasco, J.; Peris-Lopez, P. On the Feasibility of Low-Cost Wearable Sensors for Multi-Modal Biometric Verification. *Sensors* **2018**, *18*. https://doi.org/10.3390/s18092782.
38. Mukherjee, S.; Tamayo, P.; Slonim, D.; Verri, A.; Golub, T.; Mesirov, J.; Poggio, T. Support vector machine classification of microarray data. Technical report, AI Memo 1677, Massachusetts Institute of Technology, 1999.
39. Jiang, L.; Zhang, L.; Li, C.; Wu, J. A Correlation-Based Feature Weighting Filter for Naive Bayes. *IEEE Transactions on Knowledge and Data Engineering* **2019**, *31*, 201–213. https://doi.org/10.1109/TKDE.2018.2836440.
40. Richman, J.S. Chapter Thirteen - Multivariate Neighborhood Sample Entropy: A Method for Data Reduction and Prediction of Complex Data. In *Computer Methods, Part C*; Johnson, M.L.; Brand, L., Eds.; Academic Press, 2011; Vol. 487, *Methods in Enzymology*, pp. 397–408. https://doi.org/https://doi.org/10.1016/B978-0-12-381270-4.00013-5.
41. Dietterich, T.G. An experimental comparison of three methods for constructing ensembles of decision trees: Bagging, boosting, and randomization. *Machine learning* **2000**, *40*, 139–157.
42. Hassan, A.R.; Siuly, S.; Zhang, Y. Epileptic seizure detection in EEG signals using tunable-Q factor wavelet transform and bootstrap aggregating. *Computer Methods and Programs in Biomedicine* **2016**, *137*, 247–259. https://doi.org/https://doi.org/10.1016/j.cmpb.2016.09.008.
43. Plesinger, F.; Nejedly, P.; Viscor, I.; Halamek, J.; Jurak, P. Parallel use of a convolutional neural network and bagged tree ensemble for the classification of Holter ECG. *Physiological Measurement* **2018**, *39*, 094002. https://doi.org/10.1088/1361-6579/aad9ee.
44. LLC, M. Classification GAM.
45. Albawi, S.; Mohammed, T.A.; Al-Zawi, S. Understanding of a convolutional neural network. In Proceedings of the 2017 International Conference on Engineering and Technology (ICET). IEEE, 2017, pp. 1–6.
46. Hochreiter, S.; Schmidhuber, J. Long short-term memory. *Neural computation* **1997**, *9*, 1735–1780.
47. Ting, W.; Guo-Zheng, Y.; Bang-Hua, Y.; Hong, S. EEG feature extraction based on wavelet packet decomposition for brain computer interface. *Measurement* **2008**, *41*, 618–625.
48. Li, C.; Zheng, C.; Tai, C. Detection of ECG characteristic points using wavelet transforms. *IEEE Transactions on Biomedical Engineering* **1995**, *42*, 21–28. https://doi.org/10.1109/10.362922.
49. Zhao, Q.; Zhang, L. ECG Feature Extraction and Classification Using Wavelet Transform and Support Vector Machines. In Proceedings of the 2005 International Conference on Neural Networks and Brain, 2005, Vol. 2, pp. 1089–1092. https://doi.org/10.1109/ICNNB.2005.1614807.
50. Li, T.; Zhou, M. ECG Classification Using Wavelet Packet Entropy and Random Forests. *Entropy* **2016**, *18*. https://doi.org/10.3390/e18080285.
51. Boashash, B. Estimating and interpreting the instantaneous frequency of a signal. II. Algorithms and applications. *Proceedings of the IEEE* **1992**, *80*, 540–568.
52. Pan, Y.; Chen, J.; Li, X. Spectral entropy: a complementary index for rolling element bearing performance degradation assessment. *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science* **2009**, *223*, 1223–1231.
53. LLC, M. Signal Classification Using Wavelet-Based Features and Support Vector Machines, 2021.
54. Farid, F.; Ahamed, F. Biometric Intrusion Detection using the Internet of Things and Machine Learning, 2021. https://github.com/fsumon/BiometricIDS.
55. Pimentel, M.A.F.; Johnson, A.E.W.; Charlton, P.H.; Birrenkott, D.; Watkinson, P.J.; Tarassenko, L.; Clifton, D.A. Toward a Robust Estimation of Respiratory Rate From Pulse Oximeters. *IEEE Transactions on Biomedical Engineering* **2017**, *64*, 1914–1923. https://doi.org/10.1109/TBME.2016.2613124.
56. Goldberger, A.L.; Amaral, L.A.; Glass, L.; Hausdorff, J.M.; Ivanov, P.C.; Mark, R.G.; Mietus, J.E.; Moody, G.B.; Peng, C.K.; Stanley, H.E. PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. *circulation* **2000**, *101*, e215–e220.
57. Moody, G.B.; Mark, R.G. The impact of the MIT-BIH Arrhythmia Database. *IEEE Engineering in Medicine and Biology Magazine* **2001**, *20*, 45–50. https://doi.org/10.1109/51.932724.

 doi:10.20944/preprints202206.0223.v1

58. Baim, D.S.; Colucci, W.S.; Monrad, E.S.; Smith, H.S.; Wright, R.F.; Lanoue, A.; Gauthier, D.F.; Ransil, B.J.; Grossman, W.; Braunwald, E. Survival of patients with severe congestive heart failure treated with oral milrinone. *Journal of the American College of Cardiology* **1986**, *7*, 661–670.
59. Goldberger, A.; Amaral, L.; Glass, L.; Hausdorff, J.; Ivanov, P.C.; Mark, R.; Mietus, J.; Moody, G.; Peng, C.; Stanley, H. Components of a new research resource for complex physiologic signals. *PhysioBank, PhysioToolkit, and Physionet* **2000**.
60. Siam, A.; Abd El-Samie, F.; Abu Elazm, A.; El-Bahnasawy, N.; Elbanby, G. Real-world PPG dataset. *Mendeley Data* **2019**.
61. Farid, F.; Ahamed, F. Biometric Authentication for Dementia Patients with Recurrent Neural Network. In Proceedings of the 2019 International Conference on Electrical Engineering Research Practice (ICEERP), 2019, pp. 1–6. https://doi.org/10.1109/ICEERP49088.2019.8956981.