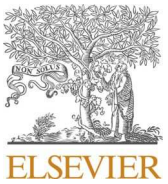
Internet of Things 24 (2023) 100927



Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.sciencedirect.com/journal/internet-of-things

A novel continuous authentication method using biometrics for IOT devices

Dipen R Bhuva, Sathish Kumar *

Department of Electrical Engineering and Computer Science, Washkewicz College of Engineering, Cleveland State University, Cleveland, OH, 44115, United States

ARTICLE INFO

Keywords:
Continuous authentication
Internet of Things
Electrocardiography (ECG)
Electromyography (EMG)
Machine learning
Biometrics

ABSTRACT

In this paper, we examine continuous authentication for IoT devices using real-time biometrics of a person's electrocardiogram (ECG) and electromyography (EMG). ECG is mainly used as a biometric identifier because it has specific features such as mathematical, morphological, and wavelet characteristics. EMG is a bio-signal defining a hand gesture of a person. Our authentication system would require no human interaction as it will have a continuous authentication schema. As soon as the user leaves a specific perimeter, the session will be killed by the system. In this paper, we propose a challenging and integrated methodology for developing, prototyping, and evaluating a continuous authentication scheme to ensure that currently insecure IoT networks are improved to have a high level of security with two layers of biometric security with continuous authentication to perform authentication in an automated manner. We used the dataset from PhysioNet for ECG, which contains samples of around 12 K for 298 people. We also used the EMG dataset available on the geostatic python library containing 150 K samples. In this experiment, we concluded that it is viable to use our continuous authentication for IoT devices with the lowest performance consumption and power consumption. The experimentation also demonstrates that the training model on two bio-signals helps obtain higher accuracy on continuous authentication within an average of 99.6%-99.99%. Our authentication schema can be implemented and integrated on any IoT device with having at least one wireless frequency that can receive and send a signal to the sender/authenticator.

1. Introduction

It is expected in the near future that there will be exponential growth in the number of Internet of Things (IoT) users. Our everyday lives are being revolutionized by ambient intelligence and massively linked IoT devices ranging from smartphones and wearables to robotics, autonomous cars, and thermostats. Authentication is essential to ensure a safe interface between these devices and consumers [1].

Most backscattering devices are used in the context of continuous authentication for IoT devices. Backscatter systems conduct passive communication by reflecting ambient signals, which can enable low power consumption, low cost, and ubiquitous connectivity for smart devices in serving diverse applications and use cases [2]. It also offers a viable low-power technique for linking Internet-of-Things (IoT) devices in order to achieve ubiquitous computing [2]. Currently, continuous authentications are more likely to

* Corresponding author.
E-mail address: s.kumar13@csuohio.edu (S. Kumar).

https://doi.org/10.1016/j.iot.2023.100927

Available online 1 September 2023

be RFID-based and for IoT devices. RFID-based authentication is similar to backscattering in which an RFID tag without a battery (or any domestic power source) receives energy through the transmission of an RFID reader and sends a reply with the same energy. An intruder or hacker can capture this authentication for the purpose of impersonating anyone; furthermore, this session could be used for his/her (intruder or hacker) benefit.

Electrocardiography (ECG) is the process of creating an electrocardiogram, which is a recording of the electrical activity of the heart. It is a heart electrogram, which is a graph of voltage against the time of the electrical activity of the heart recorded using electrodes that are inserted on the skin or by using an ECG sensor. For normal person with no heart diseases, the repetitive heart pattern or sequence of heartbeats can be represented in as a waveform, which has a cyclical repetition of five fiducial points represented by P, Q, R, S, and T. The first waveform is the P wave, which represents the depolarization of myocardial cells in the atria. The Q, R, and S waveforms are usually referred to as the QRS complex, which corresponds to atrial repolarization and ventricular depolarization [3].

Electromyography (EMG) is a method for measuring and recording electrical activity in skeletal muscles. EMG is conducted with an electromyograph to create a record called an electromyogram. When muscle cells are electrically or neurologically engaged, an electromyograph monitors the electrical potential created by these cells. The signals may be studied to detect anomalies and activation levels as well as to study the biomechanics of human or animal movement. A needle is used to measure EMG which is called as needle EMG is a type of electrodiagnostic medical procedure used by neurologists. A surface EMG is a non-medical method used by numerous experts, including physiotherapists, kinesiologists, and biomedical engineers, to measure muscle activity. In computer science, EMG is used as middleware in gesture recognition to allow physical activity to serve as an input to a computer in form of graph, as a kind of human-computer interaction.

To improve the security of digital information, a biometric authentication approach based on electrocardiographic (ECG) and electromyographic (EMG) pattern recognition is gaining popularity for a variety of applications. When compared to other biometric traits, such as fingerprints and faces, ECG signals offer various benefits, including increased security, easier collection, liveness detection, and health information. This identification technique is divided into two parts: classification and matching tasks. Support Vector Machines (SVMs), autoencoders, convolution neural networks, and SoftMax classifiers are examples of traditional classifiers that primarily focus on the categorization of labels. However, training a static classifier with matching tasks for large ECG-based authentication systems, where the test samples are often unknown persons, is clearly not appropriate. The similarity of the ECG or EMG signals of a unique user is one type of authorization challenge. Another option is to handle the matching problem as if it were a one-class classification task. For example, [4] utilizes a one-class SVM classifier for matching. However, developing a one-class SVM model for a large training set is difficult.

Our work contributes a novel continuous authentication schema that does not requires an additional interface and can run in the background with a minimal impact on performance from the IoT, indirectly helping IoT devices reduce power consumption. Our Continuous Authentication (CA) schema can be implemented with any IoT device which has at least one wireless frequency and the ability to receive signals from the sender. This signal will be used to authenticate a legitimate person primarily by their heartbeat. If the authentication accuracy falls below the threshold, our CA schema will automatically authenticate that person with a hand movement without that person's having the knowledge that they are being authenticated with EMG. This CA schema requires training data from the legitimate person for the ML model before they are authenticated by the schema. Our authentication schema protects against session hijacking as it is a continuous and as it is very hard to replicate a person's heartbeat. While ECG authentication has been explored before, our novelty lies in the integration of electromyography (EMG) as a biometric identifier, specifically capturing hand gestures. By combining our Fine tuning of ECG CNN model & alteration of CNN layer, we have achieved an average accuracy of 99% for 295 patient's ECG dataset. We have also conducted experiments with EMG dataset from the geostatic Python library, demonstrating the viability and effectiveness of our continuous authentication approach with high accuracy, low computation complexity and low power consumption. Further, increasing reliance on machine learning models in various domains necessitates a thorough evaluation of their robustness against adversarial attacks. Impersonation attacks, wherein an unauthorised user attempts to impersonate a legitimate user, pose a significant threat to the security of these models. Therefore, evaluating the model's ability to differentiate between genuine users and intruders becomes paramount.

This paper begins by explaining the approach used for CA in IoT with existing real-time ECG and EMG CA. Further, using example [5], we will pick the CNN model architecture while also making some alterations to it in accordance with our experiment. We will do the same following our experiment with different machine learning models and their results for both ECG and EMG authentication. Once the methodology is completed, this paper presents our results and model robustness against impersonation attack. Finally, this paper will be described lessons learned from the experiment, future work required, and conclusion.

2. Background

2.1. Continuous authentication

Almost all cyber-physical systems rely on user authentication. Traditionally, authentication was done quietly at the start of a session using something the user knows, such as a password or pattern; something the user has, such as a pin; something performed by the user, such as scanning a fingerprint or recording a voice; or a combination of these [6]. As a result, one-time authentication is vulnerable to session imposters, credential-stuffing, and password-spraying. Session imposters are attackers trying to take over sessions that have been open for longer than the users have been using them. Credential stuffing and password spraying are when attackers take advantage of similar log-in information by gathering credentials leaked from other services or making authorization attempts based on commonly used passwords. Existing one-time authentication techniques are inadequate as a result of the following.

i) IoT cannot provide an interface (e.g., the keyboard, fingerprinting sensor, camera) to perform authentications.
ii) One-time authentication is not safe for long-term sessions as it is highly vulnerable to session hijacking.
iii) It is highly annoying for the user if the device continues to request authentication.

To overcome the limitations of one-time authentication, continuous authentication is a reliable approach to make sure that a benign user is in communication with the edge device. Continuous authentication (CA) is an approach to authenticate users in real-time when the user is around an edge device. For example, a biometric fingerprint is a CA. While there are several wearable biometric authentication solutions, continuous authentication is a difficult challenge. A continuous authentication system would have to run in the background without interfering with the user's daily activities. For example, the user should not be requested to submit a fingerprint at regular intervals, and the system should not log real users out in the middle of a session [7]. Some examples of CA are represented in the following:

- Physical movement. Sensors can be used to track a user's distinct way of moving, for instance, how a person walks while holding a phone or certain hand positions and actions when carrying or using a device.

Table 1
Existing continuous authentication approach on IOT.

Author	Method	Approach	Metrics	Limitation
M. Shahzad et al., 2017 [11]	developed a Wi-Fi-based human authentication system, called WifiU, which recognizes users based on their gait.	WifiU entirely use Wi-Fi devices to capture gait patterns. WiFiU consists of two Wi-Fi devices: one for continuously sending signals, which can be a router, and one for continuously receiving signals, which can be a laptop.	recognition accuracies, perimeter covered, gait instances	Top most accuracy reached was 93% for one person among 3 candidate and the lowest accuracy was 79.3%.
Y. Liang, et al., 2020 [1]	the nature of CA in IoT applications, highlight the key behavioral signals, and summarize the extant solutions from an AI perspective.	Keystroke, Touchscreen Dynamics, Eye movement, walking gait, body gesture.	N/A	This framework requires high computation power with an additional cost of storage and temporary memory(RAM).
H. Alamleh et al., 2020 [12]	They can calculate their location using any of the previously mentioned technology (Wi-Fi, Bluetooth, cellular signals, GPS satellites, etc.).	Location generated by mobile devices can be utilized for the purpose of continuous authentication.	Number attempts, number of successful authentications attempts, termination of session, max time and average time.	This method can be easily impersonate by intruder as it is vulnerable to session hijacking due to its non-liveness.
A. Badhib et al., 2021 [13]	research proposes a fast and secure device-to-device continuous authentication protocol that relies on devices' features	Devices feature such as token, battery, and location are used for CA and mitigates DoS attacks using shadow IDs and emergency keys.	Communication cost, total bits, packet transfers. Number of continuous authentications	Non-liveness feature results in replication of such features resulting in false authentication.
S. Hathal et.al., 2017 [14]	Lightweight authentication scheme using Timed Efficient Stream Loss-Tolerant Authentication scheme	The design of a secure broadcast authentication.	Verified signals, expected packet size, false positive rate.	RFID authentication can be used by intruder to sniff RFID packets and find out secret key for future authentication.
D. Crouse, 2015 [15]	Work on a face-based continuous authentication system that is inconspicuous in operation	Facial orientation adjustment improves face recognition accuracy and the efficacy of the prototype continuous authentication system.	Accuracy, false-positive rate, session numbers and performance.	Face-based continuous authentication requires external environmental factors to get good accuracy.
H. Feng, 2017 [17]	VAuth, the first solution that allows continuous authentication for voice assistants.	VAuth is intended to be used in commonly used wearable devices such as eyeglasses, earphones/ buds, and necklaces, where it records the user's body-surface vibrations and compares them to the speech signal received by the voice assistant's microphone.	Accuracy, false-positive rate, true-positive rate, distance and speech(db)	Speech-based continuous authentication usually get disrupted due to noise coming from external environment resulting in low accuracy.
Y. Zhang, 2018 [16]	Eye movement to continually verify the present wearer of the VR headset to better safeguard genuine users of VR headsets (or head mounted displays in general) against attacks.	Researchers created a prototype device that allows them to apply visual stimuli to the wearer while also recording the wearer's eye movements. They leverage implicit visual cues to elicit eye movements from headset wearers while being unobtrusive to their typical activities. This allows them to continually authenticate the user without the wearer being aware of the authentication taking place in the background.	Accuracy, false-positive rate, true-positive rate, equal error rate.	The approach cannot be used for IOT authentication as it needs external device to wear on head and accuracy cannot be high using eye movement.

- Facial recognition. While facial recognition is commonly used for authentication (such as accessing a mobile phone), it may also be used to continually authenticate individuals.
- User behavior patterns such as interactive gestures, how a user writes or taps, finger pressure, how long a user presses a key on a keyboard, or how they swipe or use a mouse may be continually observed. Exceptions to the norm can then be noted or flagged.
- Voice authentication. For continuous authentication, patterns in voice (such as variations in pitch and frequency) can be monitored. Out-of-the-ordinary characteristics can be observed by continuously comparing input speech to a control dialog used as a reference.

2.2. Biometric authentication

Biometric, which incorporates the real user's distinct liveliness or body-related characteristic (e.g., facial recognition, fingerprint or palm scan, retina or iris scan, voice recognition). Traditional authentication can use different combinations of these key aspects, resulting in multi-factor authentication. Performing continuous authentication relies on continuous data processing by a risk engine which applies the appropriate degree of authentication throughout the session. Continuous authentication may also be one of the key aspects of traditional authentication, for example, a credit card gateway using the location of user while performing a transaction.

2.3. IoT devices

The Internet of Things (IoT) is a new communication paradigm that aspires to link many types of devices to the Internet in order to collect data generated by sensors; remotely control appliances and equipment; monitor surroundings, cars, and buildings; and so on [8]. The quantity and diversity of IoT devices has significantly increased in recent years, with over 30.9 billion IoT expected to be linked to the Internet by 2025 [9]. With expected growth, researching the integration of IoT devices, CA, and Backscatter technology is needed to achieve CA with IoT devices with low power consumption and higher throughput.

3. Related work and limitation

CA has been investigated extensively. Several of the earliest contributions was made in 1995, offering an examination of a user's typing patterns on an IBM PC keyboard. Years later, in 2000, the use of a webcam on a desktop computer was demonstrated to be able to perform continuous facial analysis on participants. Further, neural network models were used to analyze users' typing behavioral patterns on a desktop PC in 2006 [10].

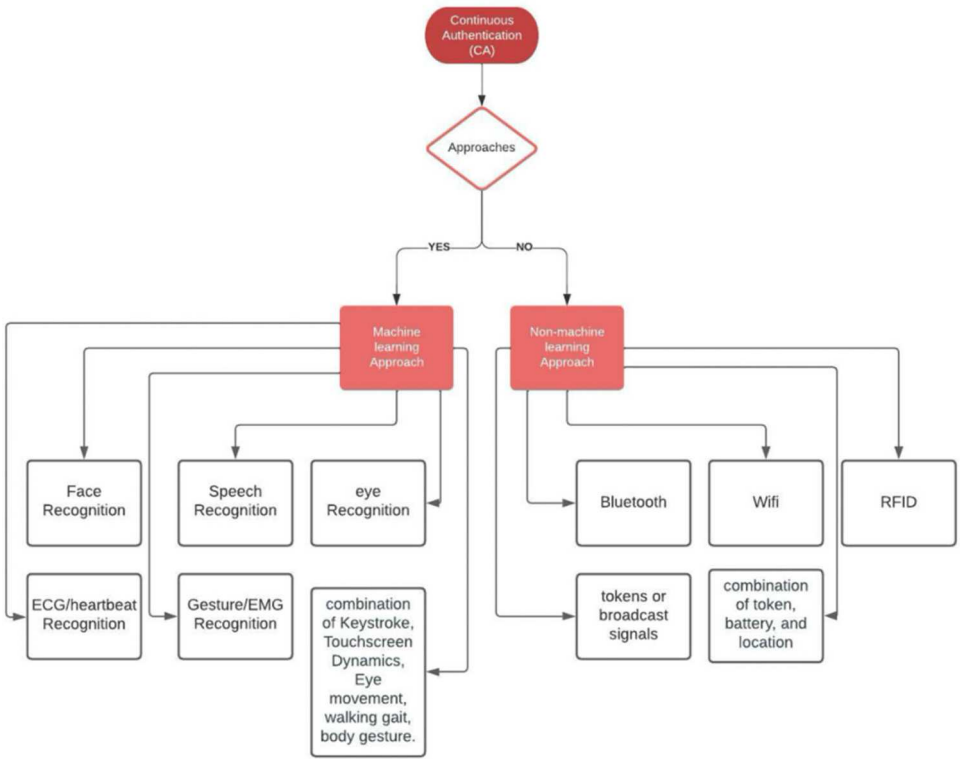


Fig. 1. Classification of continuous authentication.

3.1. CA for IoT devices

The existing CA approach in IoT from Table 1 is done with the help of Bluetooth, IoT, Behavioral gait, and many more. With Bluetooth, an IoT can recognize an authentic device within a range of specific area and can give access to the master node which is the device that is connected with master node [11]. For example: an apple watch connected with a device such as laptop automatically, doesn't require any authentication as long as it is connected with master node(laptop). For example, Bluetooth function poses a security risk. Assume an attacker, maybe acting as a friend, steals the user's watch and gains physical access to her computer. This may happen if the two are at a lunch meeting and the user goes away from the table to get something from the buffet but leaves her watch and computer behind. If the attacker is wearing the watch and the user unlocks her phone while away from the table but within Bluetooth range of the watch, the watch also unlocks. The attacker can then use the watch to open the user's Laptop without guessing her password [11] and is vulnerable to bluesnarfing. With RFID, a person can unlock door or can operate any machine as long as the RFID is closer to the operator node. With Behavioral gait, an operator node can decide with the help of artificial intelligence if a person is legit or intruder. With combination of different feature such as location, Bluetooth id, tokens, etc. can also be used for continuous authentication on IoT. But all of this has its own limitation which is presented in the Table 1.

Table 1 describes the realm of continuous authentication (CA) systems, several approaches have been explored. M. Shahzad et al., 2017 [11], developed WifiU, a Wi-Fi-based system that identifies users based on their gait. Despite achieving recognition accuracies of up to 93%. The system is vulnerable to impersonation and session hijacking. Y. Liang et al., 2020 [1], focused on IoT applications and summarized existing AI-based solutions for CA. However, their framework requires significant computation power and incurs additional costs of storage. H. Alamleh et al., 2020 [12], proposed a method based on mobile device location, but its susceptibility to session hijacking raises concerns. A. Badhib et al., 2021 [13], introduced a device-to-device protocol relying on device features, but the non-liveness characteristic can lead to false authentication. S. Hathal et al., 2017 [14], presented a lightweight authentication scheme, yet it is vulnerable to RFID packet sniffing. D. Crouse, 2015 [15], worked on face-based CA, but external environmental factors impact its accuracy. H. Feng, 2017 [17], developed VAuth for voice assistants, but external noise affects its speech-based authentication accuracy. Lastly, Y. Zhang, 2018 [16], explored eye movement authentication for VR headsets, but its limited applicability to IoT and reliance on external devices pose challenges.

Fig. 1, represents the current state of art on continuous authentication approaches to perform continuous authentication on IoT devices. Despite efforts, the first proposal for IoT-based CA did not arise until 2009 [18]. Now in 2021, CA was developed with the help of ECG to achieve excellent efficiency in terms of accuracy on finding uniqueness.

3.1.1. ML-based related work

An example of continuous authentication, which can be implemented with the help of facial recognition, speech processing, fingerprinting and further ML (Machine Learning) approach, can be implemented to identify the authenticate person. Nonetheless, continuous authentication is still subject to environmental factors. Facial recognition is limited by a lack of memory and processing capacity, as well as, an uncontrolled ambient environment. Inadequate lighting or background noise also prevents the device from completing efficient facial recognition. During phone calls the voice is analyzed for ongoing authentication. However, speech-based verification remains in the background, with substantial processing expenses, battery power consumption, and storage. Fingerprint scanning also involves the purchase of expensive sensors that the average user does not possess [19].

The existing CA were made with respect to performance, time, and complexity; however, none of them were made with the concern of power consumption, low complexity in authentication, and lower PC configuration in regards to experiments. In order to achieve CA

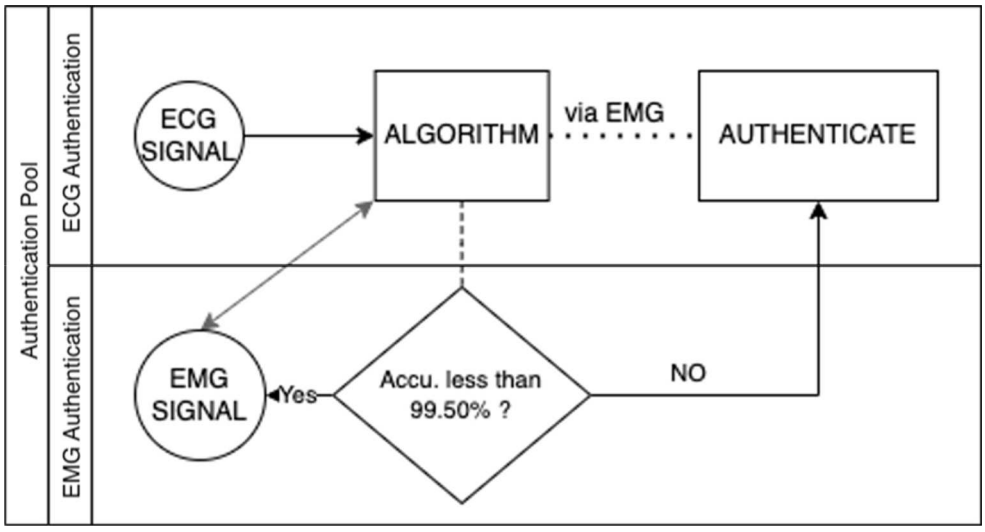


Fig. 2. Authentication workflow ECG and EMG signals.

Table 2
Authentication performed via ECG or EMG on IoT Devices using ML.

Authors	Method	Pre-condition	Database	ECG \EMG or Both	Metrics	Limitation
Barros, A., 2019 [21]	Investigated performance of Naive Bayes (NB), Support Vector Machine (SMV), Multilayer Perception (MLP), and Random Forest (RF) using ECG signal.	Processed about 60 min of ECG collected data for each driver (total of 14). 3 s as a time slot, they have about 1200 instances with 9 features each	Database used is Physio Net.	ECG	Accuracy, Sensitivity, Specificity.	Done with 14 drivers which means less subjects or a smaller number of samples.
Conor S., 2021 [6]	Novel algorithm which uses QRS detection, weighted averaging, Discrete Cosine Transform (DCT), and a Support Vector Machine (SVM)	The signals need to be recorded at highest possible sample rate that is 512 Hz.	Database was recorded using the MAXIMECG MONITOR with around 18 people and is not open source.	ECG	Balanced Accuracy Rate (BAR), Length of signal, False Positive Rate, Trained Rank Pruning (TRP) which alternates between low rank approximation and training.	Done with less subjects, so it will affect accuracy when taking more subjects.
Guoxin W., 2020 [22]	Because the weights in convolution layers are floatingpoint values, CNN-based algorithms offer outstanding accuracy but tremendous complexity. To address this issue, they substituted binary weights and estimated weights for the original weights.	There are 549 records in the database from 290 different subjects. One to five recordings are assigned to each subject. Each record contains 15 signals that are measured at highest sample rate frequency with different recorders(leads). Each signal is digitized at 1000 samples per second with a 16-bit resolution throughout a 16.384 mV range.	Database used is Physionet PTB ECG database	ECG	Authentication Accuracy, Time Complexity, CPU cycles of different weight variants.	CNN output determination is based on convolution computations necessitate several floating-point multiplications, which have an impact on performance.
Donida L., 2019 [5]	Deep-ECG uses a deep CNN to extract key characteristics from one or more leads and compares biometric templates by computing simple and quick distance functions, resulting in exceptional accuracy for identification, verification, and periodic re-authentication.	1500 samples per user (500 samples per lead), acquired with different distance each varying from dataset from all the databases with different time span.	They used many different databases including E-HOL-03–0202–003 [5] and PTB ECG database which is from Physionet	ECG	Accuracy, Performance, Computation time needed to train.	Needs high performance specification where the research was done in the following PC with 3.5 GHz Intel (R) Core (TM) i7–7800X CPU, RAM 32 GB, GPU NVIDIA TITAN X (Pascal) with 12 GB of memory. Computation time needed to train model was 9 h and 10 min.
P. Chandrakar, 2021 [23]	Scheme uses the captured ECG signal from a smart IoT device. The signal is then used to extract different ECG complexes.	The user characteristics such as the QRS complex, P peak, T peak, etc. A feature vector is derived after pre-processing of the signal.	Dataset [24]	ECG	TP (True Positive), TN (True Negative), FP (False Positive) and FN (False Negative)	Requires high computation cost for extra feature extracted from ECG signal. Large amount of feature also affects in lower accuracy when done with large amount of subjects.

(*continued on next page*)

Table 2 (*continued*)

Authors	Method	Pre-condition	Database	ECG \EMG or Both	Metrics	Limitation
Q. Li, Z. Luo, 2021 [25]	Multi-channel sEMG signals acquired from the user hand gesture are converted into sEMG images which are used as the input for deep anomaly detection model (WHICH HAS CNN in it) to classify the user as client or imposter.	Three methods to generate images from the sEMG data: sEMG map, instantaneous sEMG image and difference sEMG image (recorded EMG)	Recorded EMG data	EMG	Area under the ROC Curve (AUC), Accuracy	This CNN model requires high computation cost which indirectly affects power consumption.
Yamaba, H., 2020 [26]	Using Support Vector Machine (SVM) it produces significant accuracy with less computation power and the method proposed uses series of gestures used for authentication.	Recording EMG with highest Mhz to decrease noise signal using Myo armband and labelled it.	Myo: Gesture control armband [26]	EMG	FRR, FAR, Accidental success rate.	Recorded signal with highest possible megahertz which is the only reason of good accuracy in SVM Model.
Y. Wang, 2022[43]	They employed four classifiers—random forest (RF), k nearest-neighbors (k NN), multilayer perceptron (MLP), and radial basis function-based SVM (RBF-SVM)—and fivefold cross-validation and grid search [27] to optimize their parameters.	To analyze ECG, they use 54 healthy people (no heart disease) aged 19–35. They got 30 min of ECG data with 200 instances of QRS complexes meaning 54×200=10,800 samples.	Dataset used was recorded.	ECG	Accuracy, Attack success rate, FPR, confusion matrix	Model accuracy was calculated with 54 participants which can result in high FPR in accuracy with huge number of users.
D. Progonov, 2022 [28]	Their study examines heartbeat signal authentication on modern smartwatches. Discrete and Continuous Wavelet Transforms were used to extend heartbeat signal features for reliable user authentication in various usage contexts.	They used ECG & Photoplethysmogram (PPG) sensor to record ECG in different actins like resting, sitting, walking, standing.	Dataset was manually recorded.	ECG	Error levels, False rejection rate and False acceptance rate, Accuracy for R fiducial point in different actions.	Their model attained the highest False acceptance rate was 23% and False rejection rate was 2% which means that this authentication has lower rate of unauthorizing user and blocking authorized user.

Table 3
Continuous authentication done via ECG or EMG on Non-IoT devices using ML.

Author	Method	Pre-condition	Database	ECG/EMG or Both	Metrics
Belgacem N., 2015 [30]	Optimum-Patch Forest (OPF) classifier with autocorrelation (AC) and Fast Fourier Transform (FFT) for human authentication	PTB-database for ECG and RECORDED EMG Used 5 Physionet's databases	Physionet's database	Both (Extracted ECG from EMG)	False Rejection Rate and False Acceptance Rate (Accuracy&Error rate)
S. A. Raurale, 2021 [31]	LDA projection based Multi-layer Perceptron (MLP) and the Radial Basis Function (RBF) neural network classifier	The dataset by Raurale et al. [37] which includes EMG recordings from ten subjects of 27 $\pm$ 4 years is considered.	Signals were recorded	EMG	False Rejection Rate and False Acceptance Rate Accuracy, Equal Error Rate
A. M. H. Wong, 2020 [32]	TensorFlow Keras has been used to process the data to authenticate the hand gestures. The neural network is a Keras Sequantial model which consists of three hidden layers with 30, 20, and 10 nodes respectively, and the epoch size used is 15.	7 participants to record their hand gesture(3 males and 4 females,age19–29, 50 rythms)	Signals were recorded	EMG	Confusion Matrix(True Label, Predicted Label), False Rejection Rate and False Acceptance Rate
Hammad, M., 2019 [33]	12-layer CNN to authenticate the ECG signals	Introduced a new database, which is suitable for training and validating authentication systems.	MWM-HIT database	ECG	average accuracy, sensitivity and positive predictivity
Pławiak, P., 2020 [34]	used ResNet to extract the local features from raw ECGs and summarized the local-feature series by other network components such as attention mechanism	ECG signals obtained from two ECG databases (Physikalisch-Technische Bundesanstalt [PTB] and Check Your Bio-signals Here initiative [CYBHi]) for authentication.	Physionet's database	ECG	accuracy, precision, recall, F1-score, and equal error rate, which are related to false positive, false negative, true positive, and true negative rates to evaluate the performance.
L. Lu, 2020 [35]	Alternative EMG-based personal identification approach which uses CWT and CNN is proposed. collected data is transformed into two-dimensional graphics by CWT. Finally, the CNN algorithm is adopted to classify the experimented subjects.	MYO armband from Thalmic Labs [26] is used to acquire EMG signal. It is a complete wireless motion and EMG sensing platform	Recorded Signals with Myo armband	EMG	Identification Accuracy, True Positive Rate and False Positive Rate under different thresholds of the model

in IoT, IIOT, and MIOT devices, we should consider power consumption as it is the most important consideration while maintaining performance, time, and complexity in any device. Table 2 represents the best ML approach for ECG authentication which aligns with the current motive of continuous authentication of IoT devices with ECG authentication.

3.1.1.1. ECG/EMG-based related work. There are two types of machine learning approaches used for IoT ECG authentication .

(1) Algorithms Based on handcrafted Features [20]: Handcrafted feature extraction is divided into two types: fiducial and non-fiducial. Algorithms based on fiducial characteristics extract from a single ECG beat, or segment the distinctive local attributes of ECG beats such as temporal or amplitude onset, peak (minimum or maximum), and offset. Fiducial properties include the P, Q, R, S, and T peak waves, the time difference between the peaks of the Q and T waves, and the QT interval. In the literature, several subsets of these fiducial traits have been employed. Non-fiducial feature extraction does not rely on characteristic points to generate the feature set. Instead, some systems rely on evaluating an ECG comprehensively, or generally using time or frequency analysis to extract different statistical data. This approach tries to extract discriminative information from the ECG waveform without the need for fiducial point localization.
(2) Algorithms Based on Non-handcrafted Fiducial Features [20]: The majority of handmade feature extraction algorithms include a pre-processing procedure to prepare the ECG (e.g., a statistical analysis such as fiducial or non-fiducial features extraction). Researchers have begun to investigate non-handcrafted features, and usage of deep learning approaches to gain greater performance and resilience since the debut of deep learning. Handmade techniques rely on independent procedures and preparation, such as feature transformations and/or noise reduction, in addition to its optimization work, which results in poor performance. As a result, deep learning contributes to improved performance by circumventing the aforementioned constraints.

Table 2, represents the ECG-based continuous authentication or EMG-based continuous authentication schemes for IoT devices.

Table 2 describes the realm of continuous authentication with ECG or EMG using ML for IoT devices. Barros et al., 2019 [21], explored the performance of various machine learning algorithms using ECG signals and achieved promising results. However, their study was limited by the small number of subjects, involving only 14 users. Conor S., 2021 [6], proposed a novel algorithm for ECG analysis, but the limited number of individuals in their database and its non-open-source nature hindered broader applicability. Guoxin W., 2020 [22], addressed the complexity of CNN-based algorithms for ECG analysis, but their study highlighted the potential impact on performance when using floating-point multiplications. Donida L., 2019 [5], introduced a deep CNN-based method for ECG analysis, demonstrating exceptional accuracy, but the high-performance requirements and computation time were noted as limitations. P. Chandrakar, 2021 [23], proposed an ECG-based scheme for authentication using smart IoT devices but highlighted the high computation cost and the potential impact of a large number of features on accuracy. Q. Li and Z. Luo, 2021 [25], employed sEMG images for anomaly detection, yet the high computation cost associated with the CNN model was mentioned as a limitation. Yamaba, H., 2020 [26], proposed an authentication method using the Myo armband but limited to the reliance on the recorded signal at the highest possible sampling rate. Y. Wang, 2022 [27], explored ECG authentication with four classifiers, but the limited number of participants may affect the results when considering a larger number of users. Finally, D. Progonov, 2022 [28], investigated heartbeat signal authentication using smartwatches, reporting promising results; however, the study was limited by the manually recorded dataset. Their model was limited to highest False acceptance rate which is 23% and False rejection rate was 2% which means that this authentication has lower rate of blocking unauthorizing user.

Overall, these studies provide valuable insights into ECG-based authentication methods but also highlight the limitations associated with sample size, computation cost, dataset availability, and potential performance impacts.

3.1.2. Non-ML based work

Approach used in CA for IoT is RFID or key fob authentication used in smart cars such as Tesla. Wouters observed that the Model S key fob encrypts the code delivered to the vehicle's radio receivers with a 40-bit encryption [29]. This is quite simple in terms of encryption and isa limitation imposed by the fob's computing capability. Wouters et al., discovered the car's continual radio ID

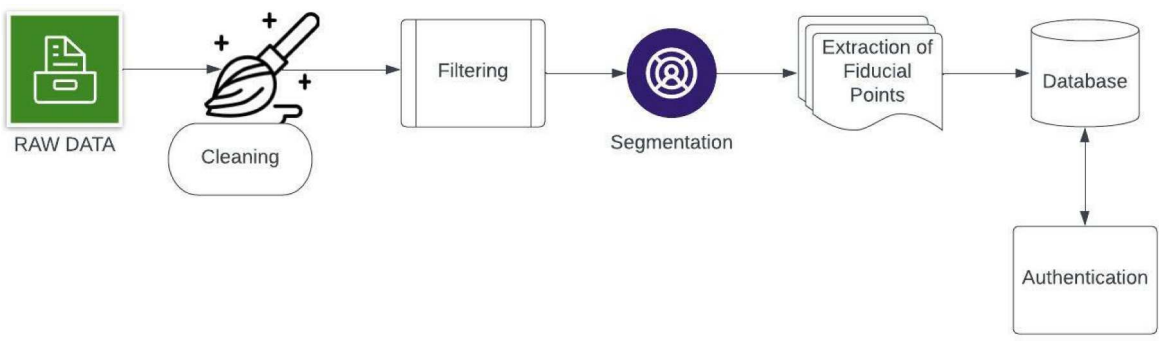


Fig. 3. ECG-based continuous authentication process.

broadcast and feed it to the target's key fob. Following the fob's reaction and intercept two return-broadcasts Wouters et al. was able to break into the automobile in under two seconds after acquiring two code samples and running them through a 6-terabyte table of pre-computed keys [29]. Here the approach can be defined as Bluetooth-based authentication, Wifi-based authentication, RFID-based authentication or any token-based authentication as described from Table 1.

Existing CA efforts have been made efficiently without non-biometric features while CA with Biometric devices needs high power consumption and high-performance usage. Different CA approaches have limitations due to it's non-liveness (Bluetooth, WiFi, RFID) detection for authentication, and if CA is made with the features of liveness characteristics (ECG, EMG, Facial, Eye, fingerprint). The CA has ow accuracy in detecting an authentic person with having dependent accuracy on external environmental factors.

These inconveniences, therefore, hindered the extensive use of IoT devices in response to high-security demands. Continuous authentication with the help of behavioral biometrics, integral physiological biometrics, behavioral metrics, and knowledge-based credentials is password or pin experimented [1]. Some of them work with ECG authentication, but none were made with the consideration of low power consumption and less complexity in an algorithm. In addition, none of the existing CA for IoT works combined an extra layer of security features using EMG.

3.2. ECG/EMG-based CA for non-IoT devices

Our research focus was based on CA for IoT devices using ECG and EMG due to its liveliness authentication detection, which is the reason we surveyed existing CA approaches used with ECG or EMG on any devices. Table 3, represents the approaches for continuous authentication using ECG or EMG Biometric features for any device where several studies have explored different approaches for authentication using biometric signals for non-IoT devices. Belgacem N., 2015 [30], focuses on human authentication using the OPF classifier with AC and FFT techniques applied to ECG and EMG signals. The PTB-database, containing samples from Physionet's databases, is used for evaluation, and metrics like FRR and FAR are employed to assess system performance. S. A. Raurale, 2021 [31], proposes a method that combines LDA projection with MLP and RBF neural network classifiers for authentication based on EMG recordings. The evaluation in this study considers metrics such as FRR, FAR, accuracy, and EER. A. M. H. Wong, 2020 [32], employs TensorFlow Keras to process hand gesture data for authentication, utilizing a Keras Sequential model and evaluating the system using metrics like Confusion Matrix, FRR, and FAR. Hammad, M., 2019 [33], introduces a 12-layer CNN architecture for ECG signal authentication, utilizing the MWM-HIT database and evaluating system performance based on average accuracy, sensitivity, and positive predictivity. Pławiak, P., 2020 [34], uses ResNet architecture to extract local features from ECG signals sourced from PTB and CYBHi databases, employing metrics such as accuracy, precision, recall, F1-score, and EER. L. Lu, 2020 [35], presents an alternative approach for personal identification using EMG signals transformed into two-dimensional graphics using CWT, classified with a CNN algorithm, and evaluated based on Identification Accuracy, True Positive Rate, and False Positive Rate under different model thresholds. The limitation of the ECG-based or EMG-based continuous authentication approaches for Non-IoT devices are that it requires high computation resources to provide good accuracy.

4. Research objective

This paper examines a continuous authentication for IoT devices that uses real-time biometrics of a person's ECG and EMG, which can be used with a maximum refresh rate for continuous authentication which further can be used in many IoT applications. This authentication is important due to its liveliness detection from the person which is hard for any intruder or hacker to impersonate. Even if a person tries to replicate the heartbeat features to unlock the authentication scheme, they will need to pass the second layer of the authentication system, which is the EMG pattern recognition, making it harder for a hacker or intruder to bypass the authentication system. Further taking into the consideration of IoT requirements, there are some characteristics such as Low Complexity of Algorithm, Low Power Consumption and highest accuracy that need to be considered in the solution design.

5. Methodology

Mainly, security technologies used in Biometric are one-time authentication, which requires user interaction to identify a single person. Using our Continuous Authentication, a user will be identified with the help of a behavioral biometric, which requires no human interaction. This system could authenticate a person 3 times per minute on ECG and up to 10 times per minute with EMG pattern recognition which is adequate for continuous authentication if it is far from the reader. Our system will analyze ECG and EMG, which will help a machine identify a user. Further, the sensor can also be implanted on a person's skin as it is small in size and the

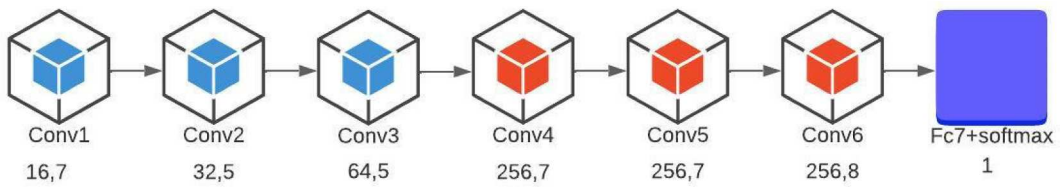


Fig. 4. CNN model used in ECG experimentation.

approach can be integrated. With the help of biometric measurements, it would be easy to identify any individual, which would give us more accuracy on liveliness detection or efficiency than the current application, which authorizes an individual through continuous authentication. On top of biometric, this system will use multiple approaches to secure from intruders impersonating a benign user, making it a novel method for continuous Authentication with ECG and EMG. To prepare a safe and secure authorization system for IoT devices, we will be following the traditionally regulated CIA Triad: confidentiality, integrity, and availability. If one of these CIA triad principles is not fulfilled, it is possible to say the security is breached [36].

5.1. ECG-based continuous authentication

Our proposed system begins with ECG signal recognition to confirm that the accepted score is from an alive user, which not only naturally detects liveliness, but is also better at rejecting impostors due to QRS complexes. The sampling rate of ECG signals varies based on the testing device. To experiment on signals collected from numerous sensors, the signals of diverse input sampling rates must first be converted into an average sample rate signal.

Furthermore, the strength of heartbeats among ECG measurement participants will vary depending on whether or not they exercise, take medicine, and so on. As a result, there must be a procedure for normalizing the amplitude of the ECG signal. Preprocessing is carried out by computing an individual's average ECG waveform and using the group average of all ECG waveforms to compute the average space of average ECG waveform samples and align ECG waveforms [37]. These average ECG waveform (QRS complexes) samples will be used in machine learning. As shown in Fig.3, if the accuracy of the machine learning model drops below 99.50% while authenticating, the system would automatically rely on EMG authentication until the machine learning model gains the accuracy to 99.50% upon the authentication scheme, which will again switch to ECG authentication.

5.2. EMG-based continuous authentication

Electrical bio signals are preferred as biometric features due to their concealed nature and ability to identify liveliness. Biological signals have gained popularity as a method for human-computer interaction in recent years [31]. Biological signals such as brain waves, pulse waves, and electromyograms (EMG) have been studied extensively. Electromyograms (EMG) measures muscle response or electrical activity in response to nerve stimulation of the muscle. As shown in Table 2 and 3, EMG has been used in a variety of studies to date. EMG authentication requires pattern recognition, where EMG pattern can be recorded at the beginning of initiation of the system similar to fingerprint or face unlock and further can be used to unlock the system with that recorded EMG pattern. This requires no additional sensor as there are several types of publicly available sensors which can record ECG and EMG as required. However, this may require an additional switch in hardware in the current state of the art in ECG & EMG sensor hardware.

Listing 1 algorithm is a high-level representation of a continuous authentication system using ECG (heartbeat) and EMG (motion) signals. The goal of the algorithm is to determine whether to accept or reject the user based on the input signals.

Following is the description of the algorithm step by step:

1 *Input*: ECG and EMG signals are provided as the input to the algorithm.
2 For each ECG, the following steps are performed:
  a *Input Correction*: If necessary, the input signals are corrected or processed to ensure data quality.
  b *ECG Signal Processing*: Filtering: The ECG signal is filtered to remove noise and artifacts.
  c *Preprocessing*: Preprocessing techniques are applied to enhance the signal quality.
  d *Point Extraction:* Relevant fiducial points are extracted from the preprocessed data.
  e *Accuracy Improvement Loop*: The algorithm enters a loop where the preprocessed data is used as input to a CNN (Convolutional Neural Network) model. The output accuracy of the model is updated, and the loop continues until the accuracy reaches a certain limit.
3 *Acceptance or Rejection*: If the accuracy of the CNN model is equal to or higher than the specified limit, the algorithm returns "accept" as the output, indicating that the user is authenticated. If the accuracy is below the limit, a pattern matching algorithm, denoted as matching pattern (DT Model), is applied to determine a pattern match and obtain an EMG score.
  a The EMG score is compared to a predefined limit for EMG signals.
  b If the EMG score is lower than the EMG limit, the algorithm returns "reject" as the output, indicating that the user is not authenticated.
  c If the EMG score exceeds or meets the EMG limit, the algorithm returns "accept" and proceeds to the ECG step again.
  d Exit: If the initial input fails the correction step, the algorithm exits.

Fig. 2 explains an authorization process that will help us to create a continuous authentication project. Here we propose a specific selection of features used in previous research, which can only be based on the fiduciary amplitude and time of the signal obtained without any complex processing, and then examine some of the most used machine learning algorithms, i.e., the SVM (Support Vector Machine), and RF (Random Forest), convolution neural network (CNN).

Support Vector Machines (SVM) are often used as best choice classifiers in biological signal analysis applications. SVM is a pattern recognition algorithm that separates a collection of training features with a maximum margin from the hyperplane. Non-linear kernel changes may be used when linear separation is not achievable. Different kernels with quadratic, polynomial, and radial basis functions are available. The selection of an appropriate kernel function is dependent on the particular dataset and its feature [21].

Listing 1
ECG and EMG based continuous authentication.

```
ALGORITHM:
INPUT: ECG&EMG SIGNAL
OUTPUT: ACCEPT OR REJECT
foreach ECG and EMG Signal do
    INPUT ← ECG AND EMG
    If INPUT do CORRECTION
        ECG:
        foreach INPUT do
            apply → filteration;
            apply →preprocessing;
            apply →point extraction;
            fiducial points → pre-processed_data;
        while accuracy=0 do:
            pre-processed_data → Y_i"j"d" (CNN Model);
            accuracy ← updated_accuracy;
        if accuracy >= limit then
            return accept;
        else
            pattern → matching.pattern(DT Model);
            emg_score ← matching.pattern(DT Model);
            authenticate.emg_score → EMG;
              if emg_score <  LIMIT(EMG)
                  return reject;
              else
                  return accept & goto → ECG();
    else
        exit()
end
```

Our work will also experiment with decision trees and CNN. Given the variety of characteristics retrieved from ECG signals, the efficiency of frequently used features in ECG biometric authentication techniques is comprehensively investigated in our work. The characteristics such as QRS-complex detection are specifically considered. These characteristics are put into decision tree classification

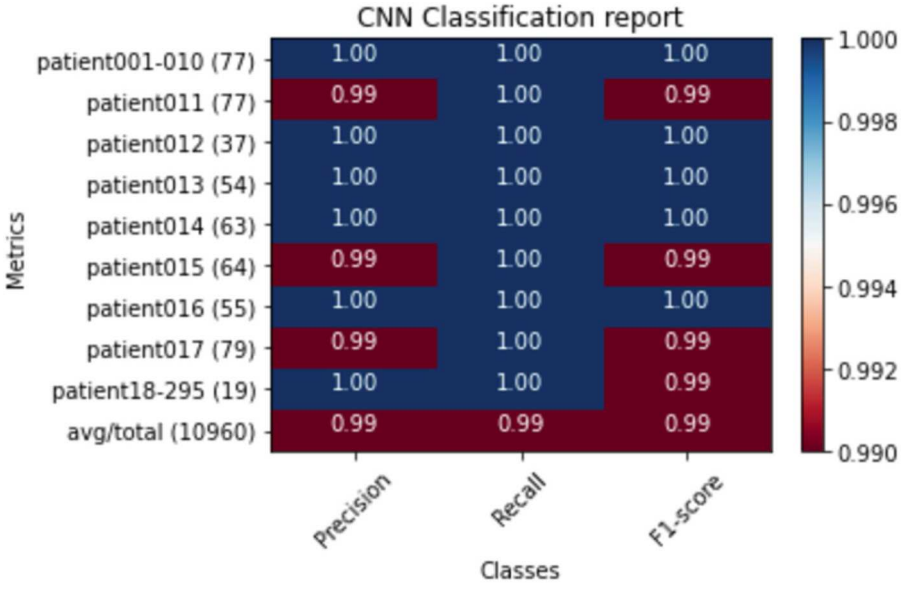


Fig. 5. CNN classification heatmap for ECG experimentation.

algorithms. Convolutional layers process the input signal x by convolving it with a bank of K filters f, using biases b. As a result, they obtain an output signal y.

$$\mathbf{Herex} \in \mathbf{R}^{\mathbf{H}\times\mathbf{W}\times\mathbf{D}}, \mathbf{fx} \in \mathbf{R}^{\mathbf{H}\times\mathbf{W}\times\mathbf{D}}, \mathbf{y} \in \mathbf{R}^{\mathbf{H}\times\mathbf{W}\times\mathbf{D}} \tag{1}$$

From Eq. (1) H, W and D are the height, width, and depth dimensions, respectively. In the basic configuration of the convolutional layer, for each coordinate (i, j, d), the output is computed as follows:

$$\mathbf{Y}'_{\mathbf{i}'\mathbf{j}'\mathbf{d}''} = \mathbf{b}_{\mathbf{d}''} + \sum_{i=1}^{H''}\sum_{j=1}^{W''}\sum_{d=1}^{D} f_{ijd} \times x_{i'+i-1, j''+j-1, \mathbf{d}''', \mathbf{d}''} \tag{2}$$

Padding of the input signal x or subsampling stride of the output are required in some layers. We focus on top-bottom-left-right paddings ($P_h^-, P_h^+, P_w^-, P_w^+$) and strides in particular (S_h, S_w).

$$\mathbf{Y}'_{\mathbf{i}'\mathbf{j}'\mathbf{d}''} = \mathbf{b}_{\mathbf{d}''} + \sum_{i=1}^{H''}\sum_{j=1}^{W''}\sum_{d=1}^{D} f_{ijd} \times x_{S_h(i'-1)+i-P_h^-, S_w(j-1)+j-P_w^-} \tag{3}$$

Since IoT devices have minimal computing power, complex architectures need to be avoided [21]. Furthermore, the performance of these algorithms needs to be analyzed to the user constantly. This will help us create a low complexity system [22] that will help integrate the above approach with our existing IoT authentication module. Further we can use EMG pattern recognition when ECG precision or accuracy of identifying the person drops below 99.50% and use EMG pattern recognition for authentication as shown in Fig. 2.

Fig. 3 represents the simple ECG/EMG authentication approach used in our method. Once the sensor device is implanted in any person's body, it will transmit an ECG and EMG signal with the help of a sensor. Further, the receiver will use the above-mentioned approach presented in flowchart to extract features from ECG/EMG data, helping an IoT device to identify an individual. This approach will be continuous, and as soon as the system detects any intruder or if the authorized person's leaves, the access will be denied immediately. The above integration of ECG and EMG will help to create a novel approach for continuous Authentication, a system with the highest efficiency, and no human interaction.

6. Experimentation and results for evaluating different ECG and EMG using ML models

The experiment will be carried out with an intruder user and a legit user. Both of the signal points will be collected in csv file, which are available in ECG dataset from PhysioNet [38] and EMG dataset from geostat. The ECG data is processed as shown in following Fig. 5. Processing EMG data is comparatively easier, since the process is reduced in half comparing to converting ECG raw data to csv.

Fig. 3 represents the initial steps for experimenting our continuous authentication approach. The success of the approach will be measured in terms of time, accuracy, sensitivity, specificity and error.

Firstly, we will conduct two different experiments:

6.1. Differentiating different ECG signals between multiple samples experimentation

In order to conduct this experiment. We will be diving the experiment in multiple phases which are:

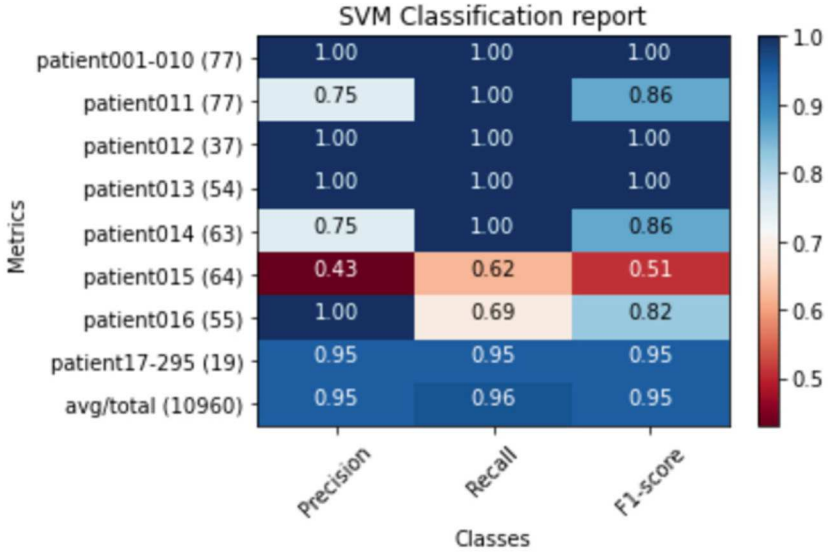


Fig. 6. SVM Classification heatmap report for ECG experimentation.

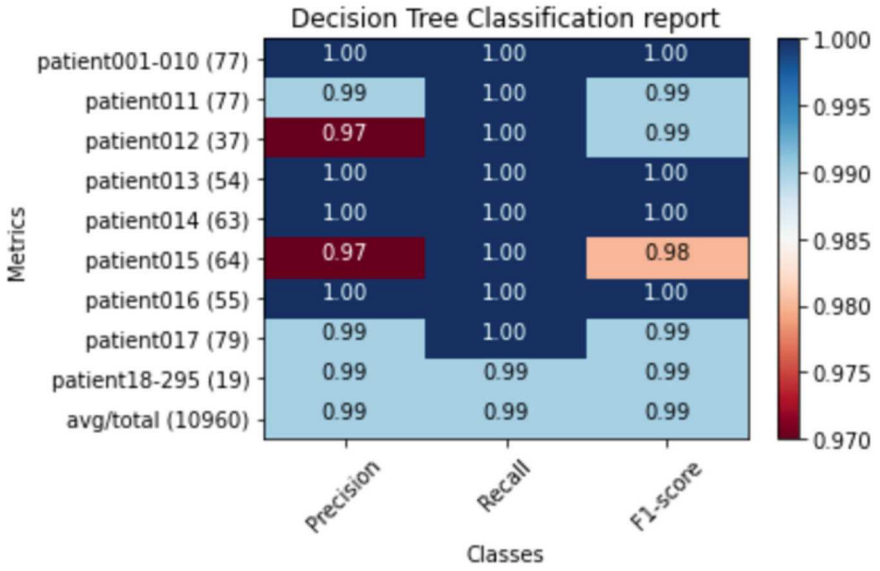


Fig. 7. Decision Tree Classification heatmap report for ECG experimentation.

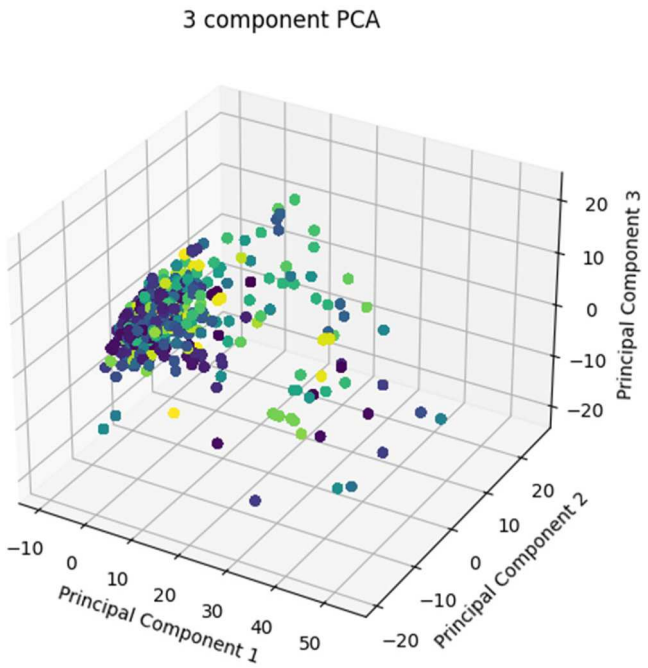


Fig. 8. K-mean Classification of Physio Net.

6.1.1. Data pre-processing

We retrieved ECG signal characteristics from the original dataset from PTB database [38]. It takes ECG records in the PhysioNet PTB Diagnostic ECG Database and generates a dataset for further use. The code loads each record, resamples the signal, detects QRS peaks, corrects the peaks, and calculates the average QRS complex. It then removes outliers based on a count threshold. The count threshold refers to the minimum number of valid QRS complexes required for a record to be included in the dataset. If the count of valid QRS complexes is below this threshold, the record is considered an outlier and is discarded. In the provided code, the count threshold is set to 8. Therefore, any record with fewer than 8 valid QRS complexes will be excluded from the dataset. Afterward, it calculates the correlation coefficients between each QRS complex and the average QRS complex, selects the maximum correlation coefficients, and generates combinations of indices. For each combination, it creates a temporary data frame with the corresponding signal segments and appends it to the final dataset. The processed dataset is saved as a CSV file. This ECG signal has multiple fiducial points, that can be

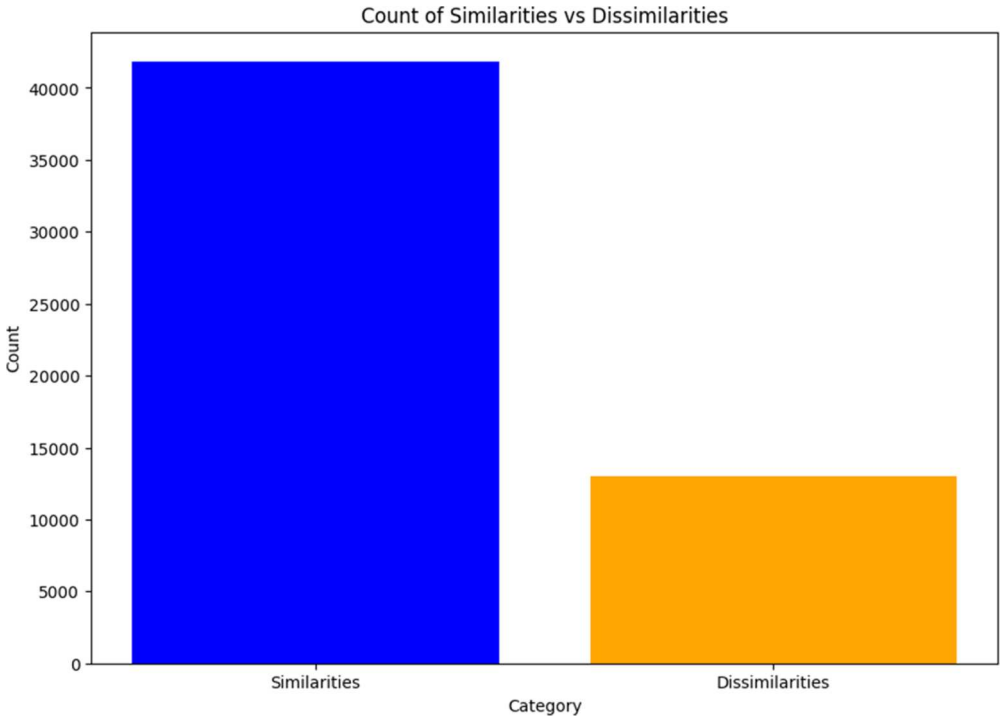


Fig. 9. Count of Similarity vs Dissimilarity.

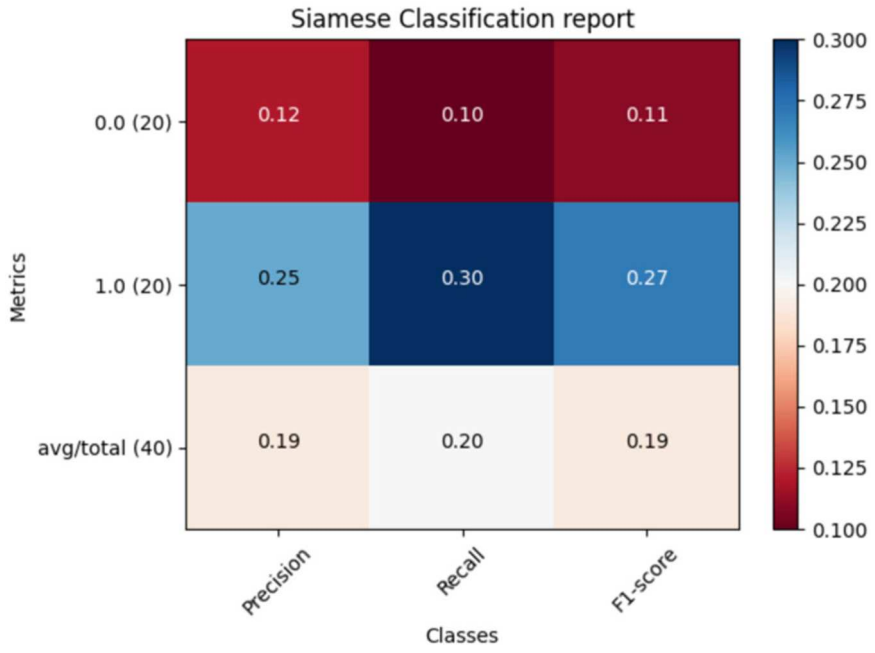


Fig. 10. Siamese binary classification report.

utilized to divide a lengthy signal into shorter segments. Then, for each 'R' point, we detected it and chose a time frame of 1 s. As a result, we obtained a large number of 'QRS' duration or QRS complexes, each having 200 samples [22]. Following that, we chose 15–25 complexes at random. When we have finished preprocessing all of the individuals' records, we will utilize those complexes as input data for the convolution neural network.

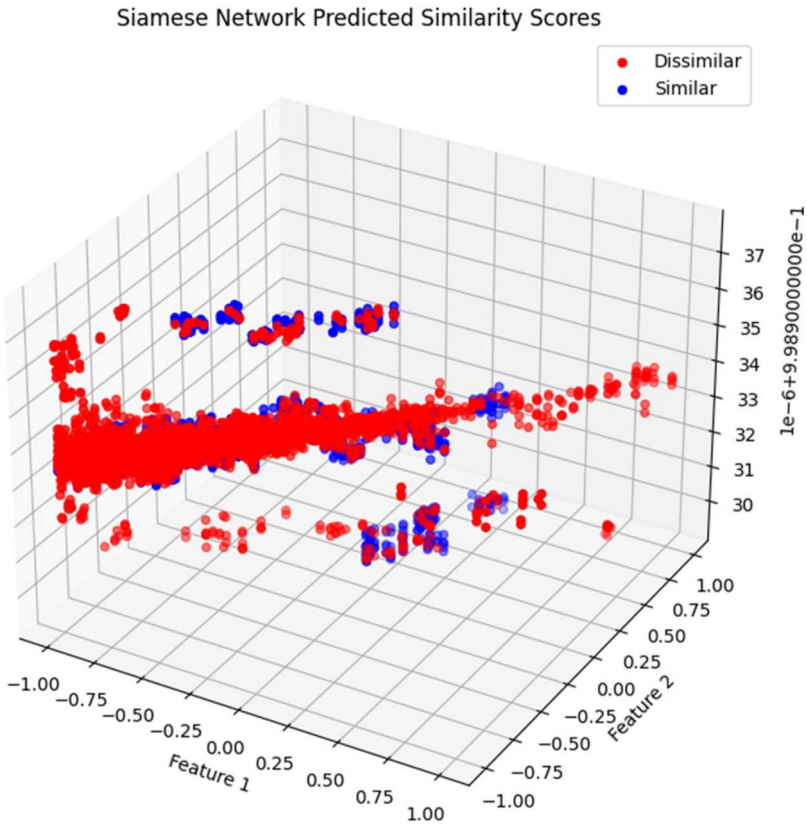


Fig. 11. 3D plot features of Siamese Network.

6.1.2. *Modeling*

To develop our model, we employed a CNN framework inspired from [5]. With around 20 epochs, we trained the CNN model using gradient descent. The batch size was set at 16. To produce high-dimensional characteristics of ECG signals, deleting the fully-connected layers of the training CNN structure and maintaining the convolution layers that include ECG signal information [22]. The model architecture consists of several convolutional layers with ReLU activation and max pooling, followed by dropout regularization and fully connected layers as shown in Fig. 4. The model is compiled with cross-entropy loss and the Adam optimizer. The training process is carried out for a specified number of epochs, with the best model weights saved based on validation accuracy. The performance of the trained model is evaluated using classification metrics such as precision, recall, and F1-score. The training and validation loss

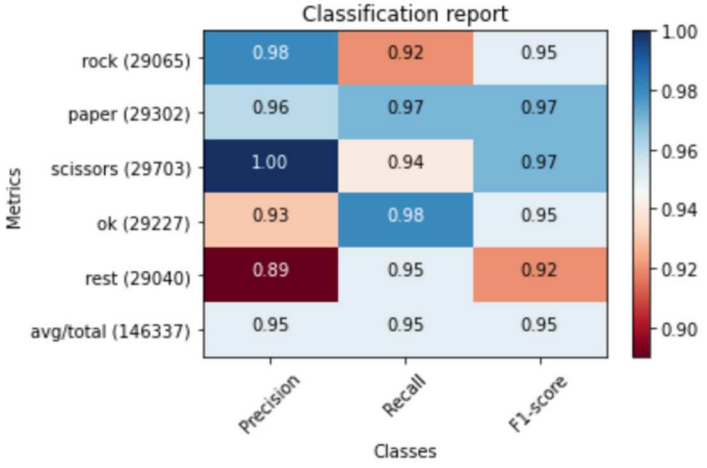


Fig. 12. Decision tree Classification heatmap report for EMG experimentation.

curves are plotted using Matplotlib. Finally, the trained model is saved for future use.

Fig. 4 represents CNN Model, which represents the building of CNN model layer for ECG. Fig. 5 represents classification heatmap report for CNN model used for ECG authentication to identify unique patients among 295 patients(295 users).

In addition to CNN, we performed SVM model to distinguish all 295 patients(295 users). We used default kernel which is radial basis function kernel "RBF". Further we set gamma to auto, so it can be scaled on auto and did the punishment or penalty of 2 for the parameters. The following Fig. 6 shows the SVM had an average of 95% of right prediction for all 20% of the test data. Fig. 6 represents the classification heatmap report for SVM model.

Similarly, we performed the similar approach using decision tree model to distinguish all patients from. Fig. 7 represents the classification heatmap report for the decision tree model.

Fig. 8 represents the classification results obtained by k-mean clustering algorithm. The color of each point in the scatter plot is determined by the corresponding numeric label assigned to the data sample. The conversion to numeric labels enables the visualization of different categories or classes in the scatter plot. Principal Component 1 (x-axis), Principal Component 2 (y-axis), and Principal Component 3 (z-axis) represent orthogonal directions in the multidimensional feature space. The points in one area indicates that for K-mean clustering, it is not able to separate all individual with ECG Fiducial points.

Fig. 9 represents count of similarities found by k-mean clustering, which is approximately 40,000, indicates that there are around 40,000 instances where the closest user identified by the algorithm based on fiducial points of ECG matches the actual user in the test data. This suggests that the fiducial points of ECG have successfully captured similar patterns or characteristics among these users, leading to a decent number of correct identifications. On the other hand, the count of dissimilarities, approximately 13,000, represents instances where the closest user identified by the algorithm does not match the actual user in the test data. This indicates that there are differences in the fiducial points of ECG among these users, resulting in high number of incorrect identifications.

Fig. 10, shows the heatmap classification report for identification of 2 users (0,1) with using Siamese network. The similarity score presents that the Siamese model is able to not able to detect similarity between two users as it has lower precision, recall and F1-score.

Fig. 11, represents Siamese model cannot identify all user but was able to find to some unique users. By watching 3D plot diagram, it has a high number of red points indicating, dissimilarity between the same user's fiducial point making it high number of false rejection rate.

6.1.3. ECG authentication process

For authentication, accuracy experiments were used and we pass user, intruder, and test data where the test number is represented below. We passed all of the three data to a trained model to obtain accuracy where accuracy is shown as below:

$$\text{Accuracy} = \frac{user_{score} + intruder_{score}}{test_{number}} \tag{4}$$

Where test number is:

$$\text{test\_number} = \text{user\_number} + \text{intruder\_number} \tag{5}$$

Here user_number represents the number legit user and intruder_number represents the number of intruders. The ECG features of both users which is intruder and authorized user are passed to CNN model to get the correlation of accuracy of authorized and unauthorised users. To assess the model's robustness, we employ an impersonation attack approach. The methodology involves selecting an intruder who impersonates a legitimate user during the data-preprocessing phase. We calculate the intruder accuracy, which represents the model's performance when the intruder attempts to deceive the system. Additionally, we measure the test user

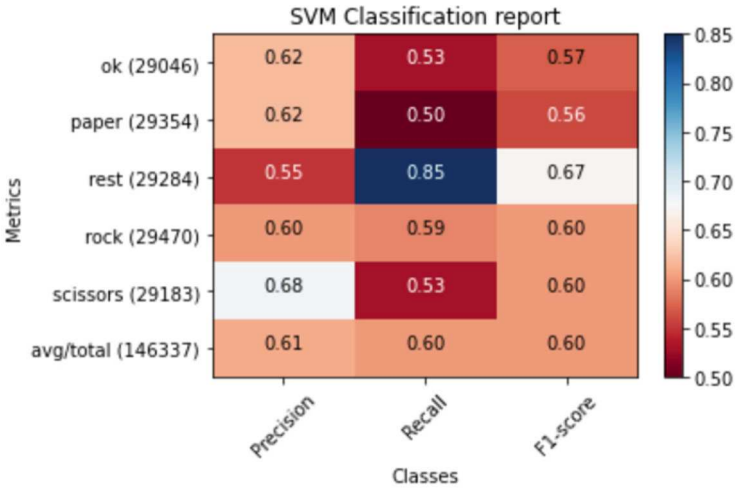


Fig. 13. SVM model Classification heatmap report for EMG experimentation.

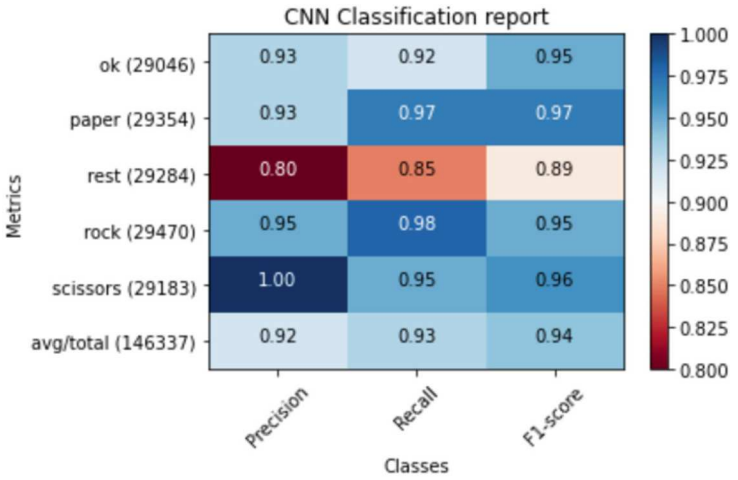


Fig. 14. CNN model Classification heatmap report for EMG experimentation.

accuracy to evaluate the model's capability to correctly identify and authenticate genuine users.

6.2. *Differentiating different EMG signals between multiple samples experimentation*

In order to conduct this experiment, we will be diving the experiment into multiple phases:

6.2.1. *Data pre-processing*

For this experiment, we got the dataset from geomstats.datasets.utils and extracted the data to a CSV file, for further operation [2]. The backend of getting data was done with the help of NumPy. Further moving on we pre-processed data with hand gesture data such as Rest, Scissors, Ok, Rock and Paper. The above hand gesture is recorded with 7 channels and labeled with its hand gesture and with its time. Data cleaning was done to remove any noise or artifacts present in the data. This involves techniques such as baseline correction, filtering (e.g., bandpass, notch), and removing outliers. Further segmentation is used to split the continuous data into individual gestures based on the provided timestamps. This ensures that each gesture is treated as a separate sample for analysis. Further, feature extraction is done to extract relevant features from the segmented data to capture the characteristics of each gesture. Commonly used features for EMG data include frequency-domain features (e.g., spectral entropy, power spectrum), and time-frequency features (e.g., wavelet transform). After extracting features, standard normalization is used to normalize the feature values to a consistent scale. This step helps mitigate the influence of different magnitude ranges across channels and ensures that all features contribute equally during classification. If the number of features is high or if there is redundancy in the feature set, applying dimensionality reduction techniques which is feature selection algorithm is used to reduce the feature space while preserving important information. Further, we will use this data to feed different models and test their prediction, so the model with the highest accuracy can be used with the authentication process.

6.2.2. *Modeling*

To develop our model, we used decision tree algorithm which is fast and easy to use and we got the f1-score which is above 90%, which means that the decision tree has the perfect precision and recall. Fig. 12 shows the classified heatmap report for decision tree-based model. As we can see the lowest accuracy, we have got is in rest gesture that is while doing no gesture. To make it more precise we can remove the rest label as it is not needed in the authentication proposal because a person has to do some gestures in order to get into the authentication system. But we kept the rest data so that the model has to perform for all possible gestures. Further, we can also conclude that the more pressure we put on hand will result in more precision, which means scissors, which will be similar in all different ML models.

We then repeated the experiment with SVM model, by passing data to SVM algorithm and used the default kernel which is Radial Basis Function (RBF) and set gamma to auto, where we set the penalty to 2. Fig. 13 shows the classification heat map report for the SVM model. While seeing the heat map, we can see that RBF cannot be used to perform prediction on gestures as it seems its accuracy is too low.

We further repeated the experiment using CNN model with 100 epochs. We used Sequential model for the experiment. Before performing CNN experiment, we converted the label into numerical digits so that further it can be converted to float32 and then further to NumPy array, so that it can be processed in CNN model. Fig. 14 represents the classification heatmap report for CNN model with respect to EMG-gesture classification.

6.2.3. *EMG authentication process*

To perform the *EMG* authentication experimentation, we defined a pre-defined pattern (gesture example: rock, ok, paper, scissors).

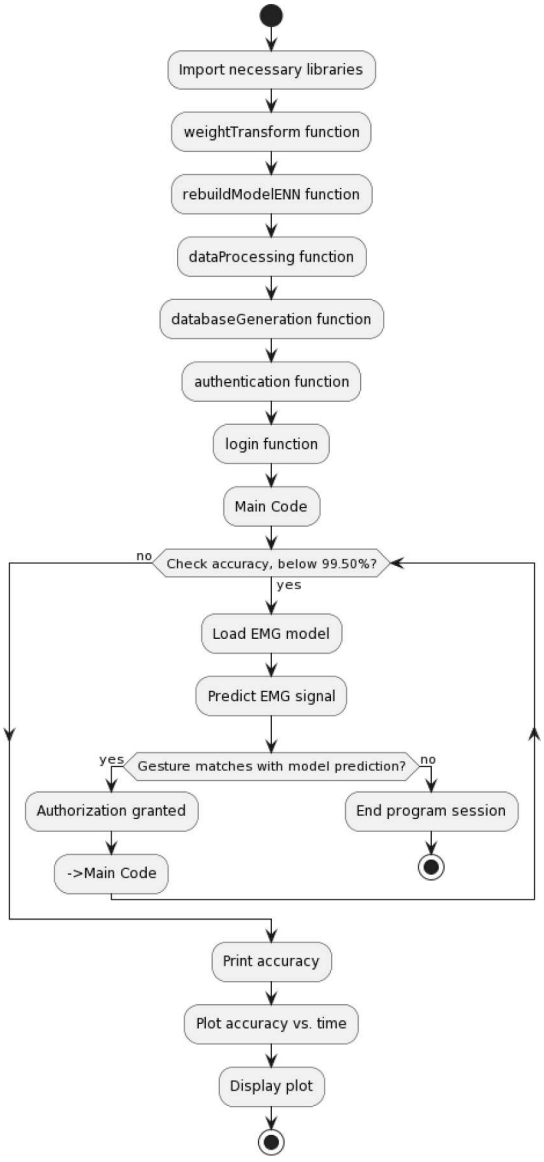


Fig. 15. Flowchart for ECG and EMG Authentication.

This label will be used to identify the combination of ML prediction and unlock pattern, giving us the output as authorized or unauthorised. Further, this can be integrated into ECG continuous authentication files and using EMG authentication when needed by the authentication system and such authentication decision can again be carried out with ECG after a specific time interval.

6.3. 2-layer authentication process

As shown in Fig. 15, the authentication starts by importing necessary libraries such as numpy, pandas, progress.bar, matplotlib, time, and keras. The function weightTransform is defined, which applies different transformations to the weights of a model's convolutional layers based on the specified mode and parameter n which can be defined by end-user while running authentication process. The function rebuildModelENN loads a pre-trained Keras model from the path and applies weight transformations to its convolutional layers using the weightTransform function. It also retrieves the output tensors of each layer in the model. The function dataProcessing reads a dataset from the provided path (CSV format) and performs data preprocessing steps like randomly selecting users, creating a test user dataset, creating a test intruder and converting it to set of templates. The function databaseGeneration takes the model and template as input and predicts output of the valid user using the model. The function authentication performs the authentication process by comparing the output of the model with the templates. It calculates the correlation coefficient between each login part and database part and checks if it exceeds the specified threshold. If a match is found, it returns True; otherwise, it returns False. The

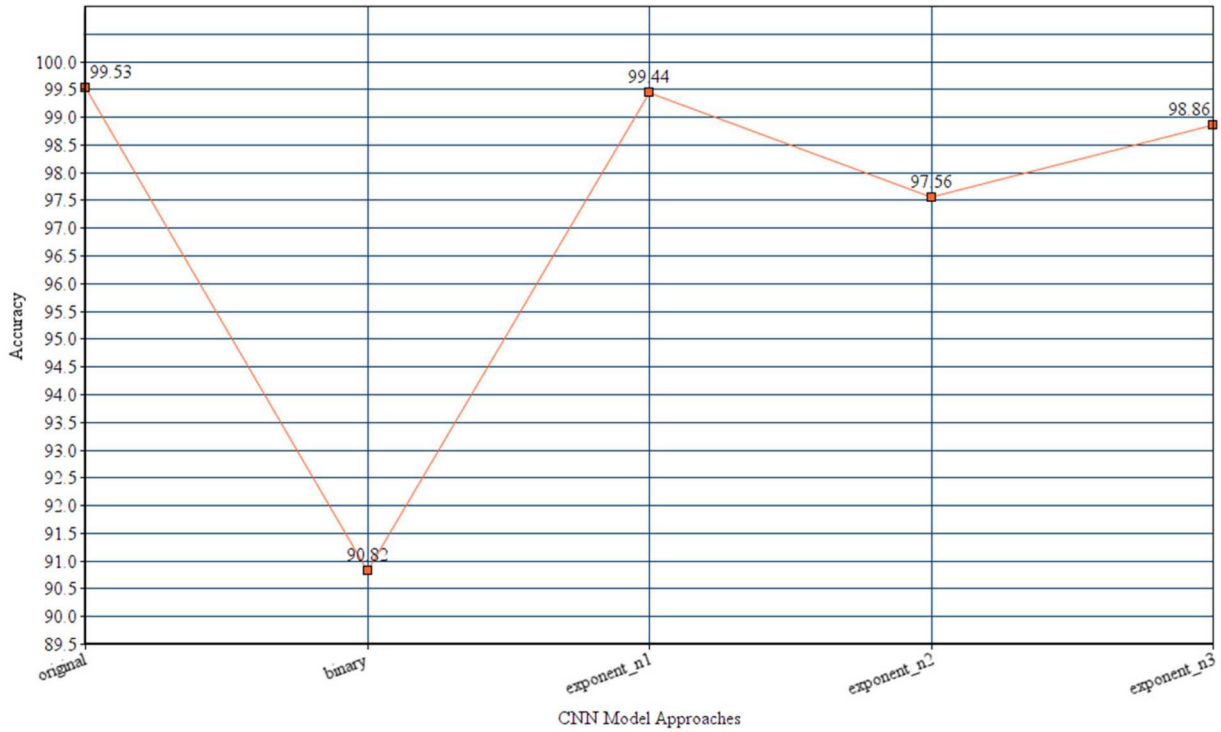


Fig. 16. Performance of authentication using different approaches in CNN model with 15 parameters.

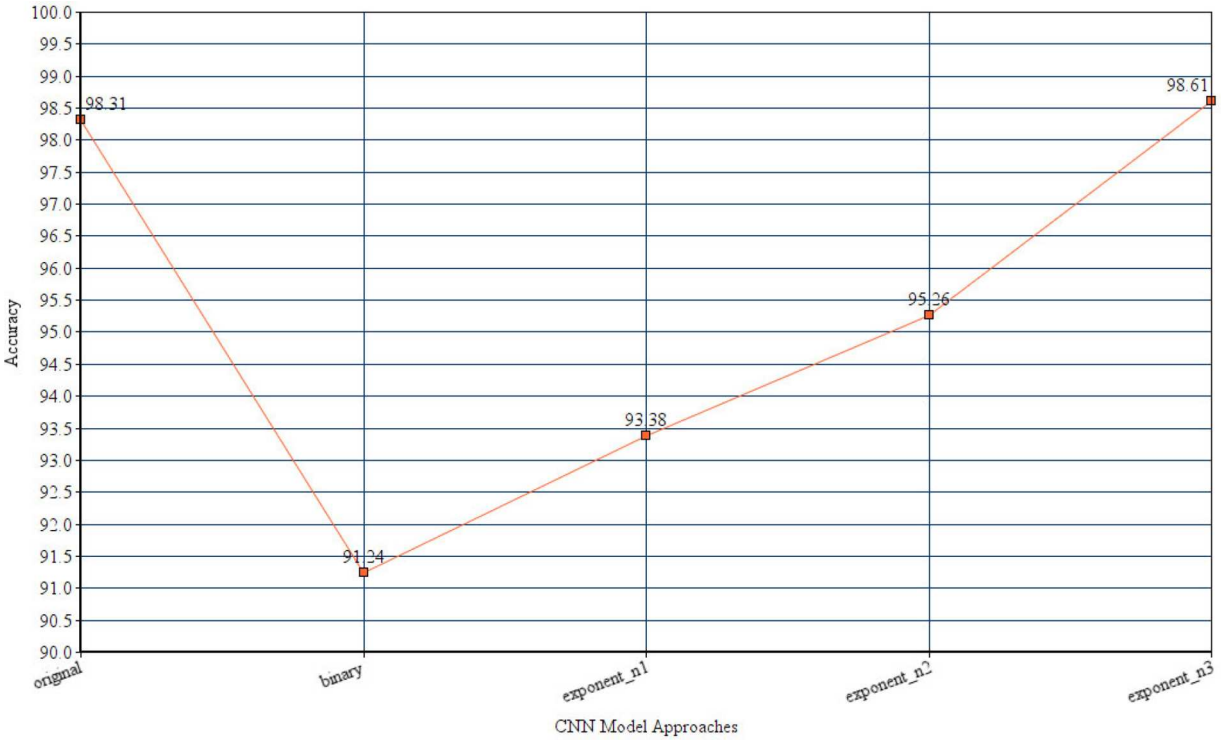


Fig. 17. Performance of authentication using different approaches in CNN model with 25 parameters.

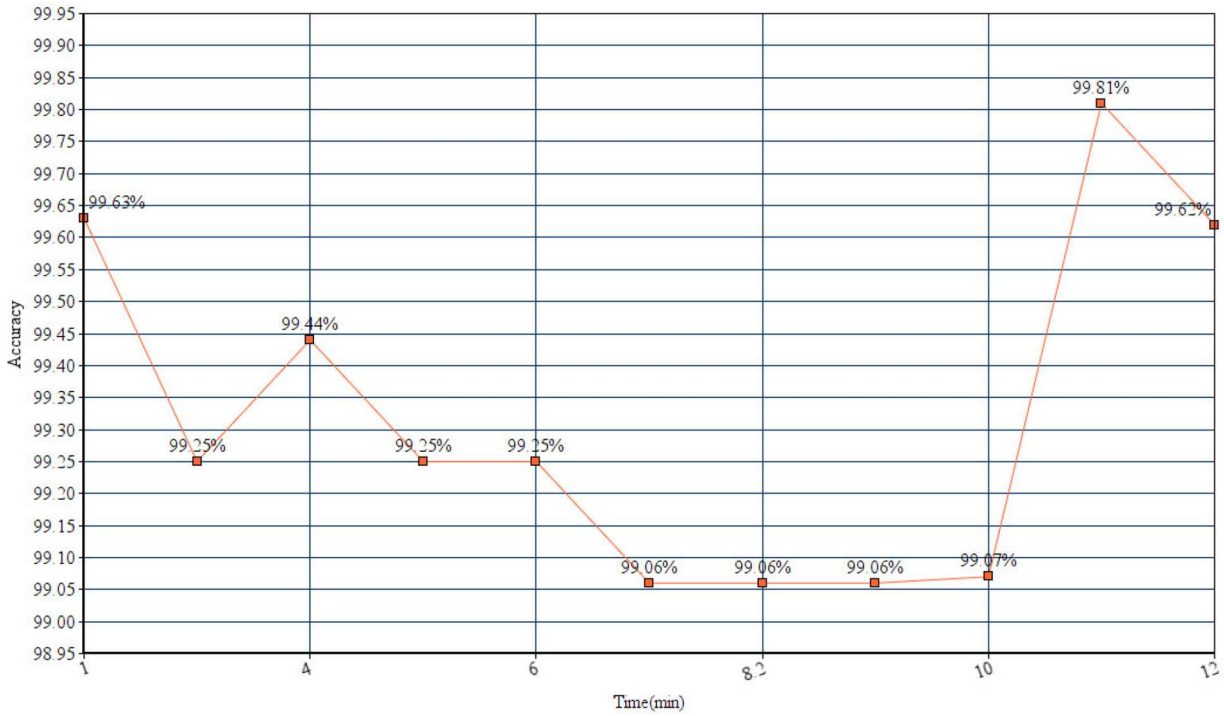


Fig. 18. Discarding convolutional layer 1 with 15 QRS complexes in Data Preprocessing.

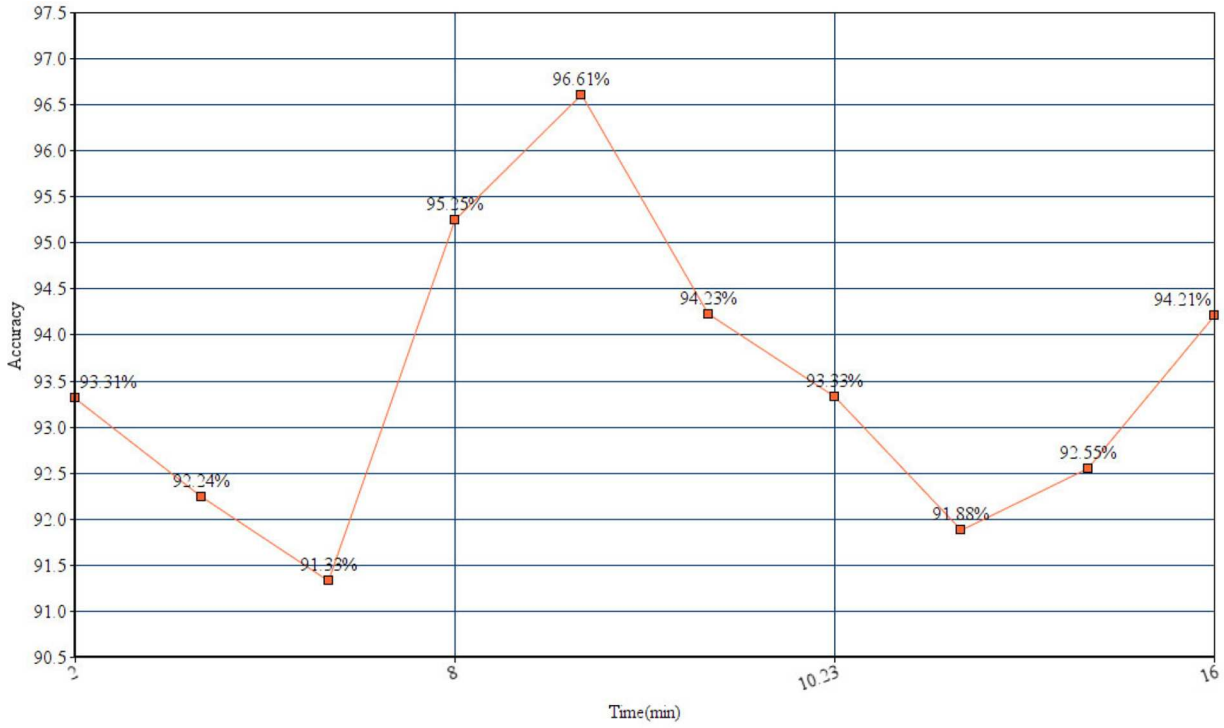


Fig. 19. Binary Approach of CNN model with convolutional layer 1 with 25 parameters.

function login performs the login process for both test users and test intruders. It iterates through the test users and intruders, applies the authentication process, and calculates the accuracy of user and intruder verification based on the number of successful matches. The main function of the code executes the login function to perform the login process and obtain the accuracy. If the accuracy is below

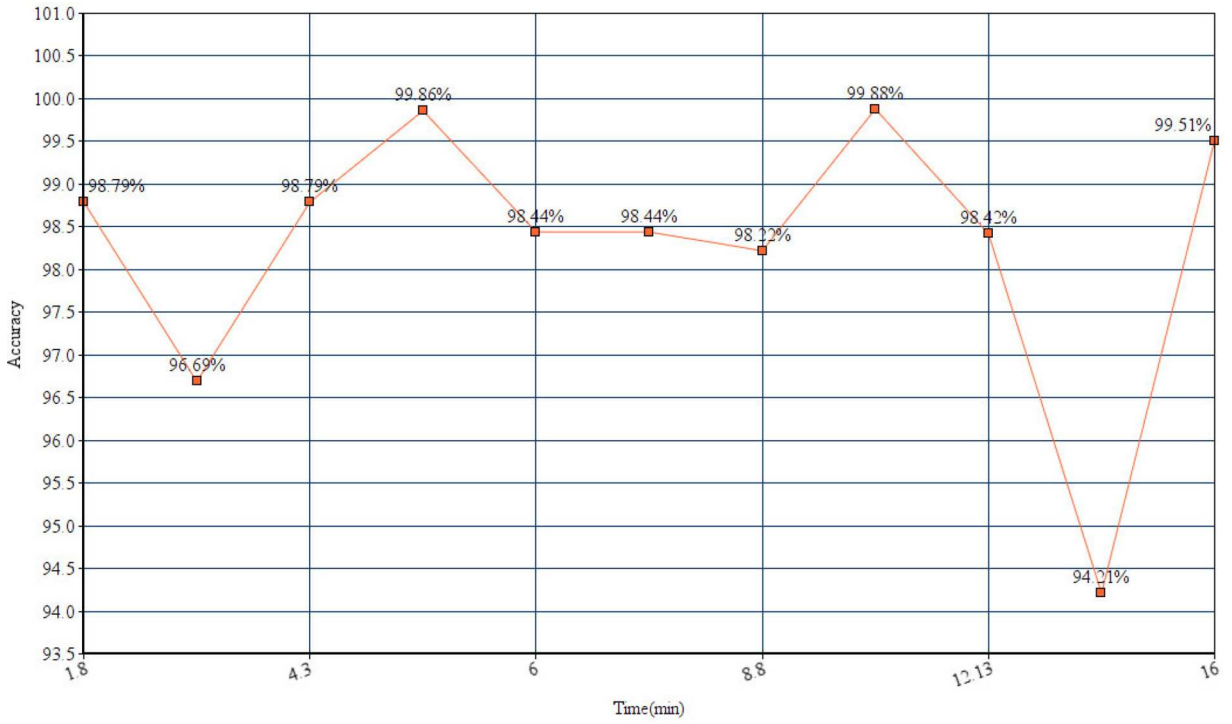


Fig. 20. Normal Approach of CNN model with convolutional layer 1 with 25 parameters.

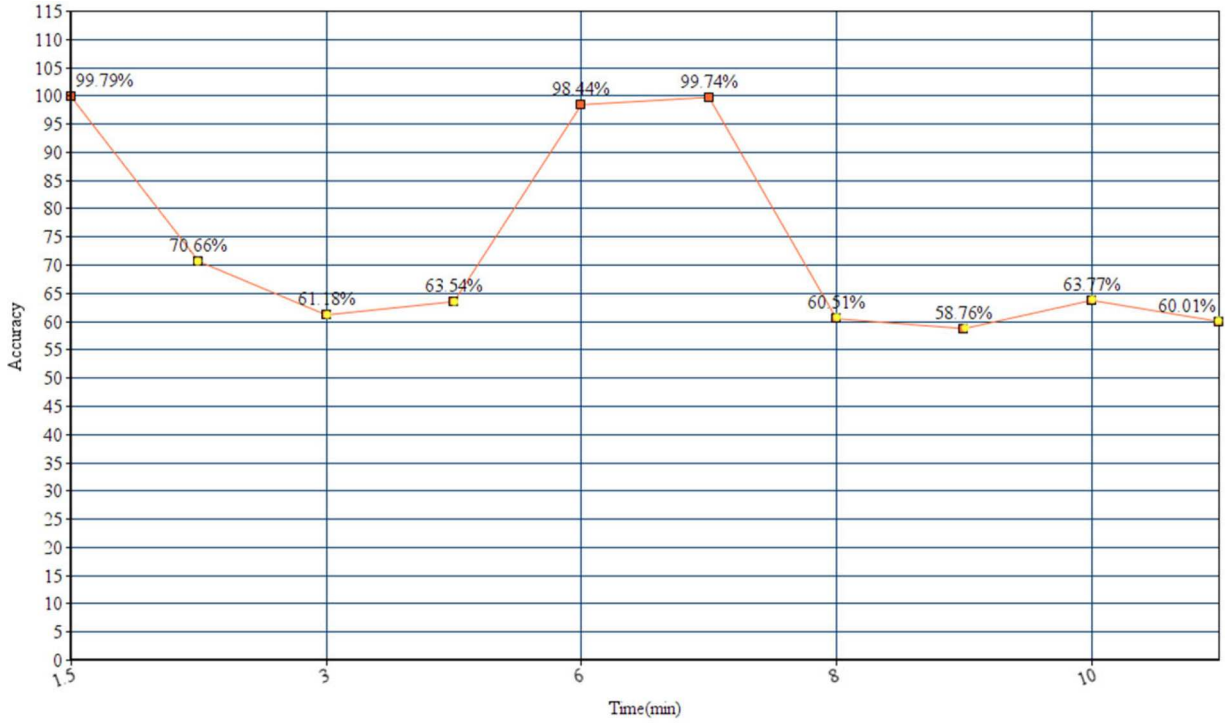


Fig. 21. CA performance for SVM model using ECG and EMG data executed on OSC environment.

99.50%, it performs an additional process of EMG signal prediction using a pre-trained model (decision-emg.joblib). It then compares the predicted sequence with an unlock pattern to determine authorization. If gesture matches with model predication it gives access and reiterates through ECG authentication again, if not the program session is ended.

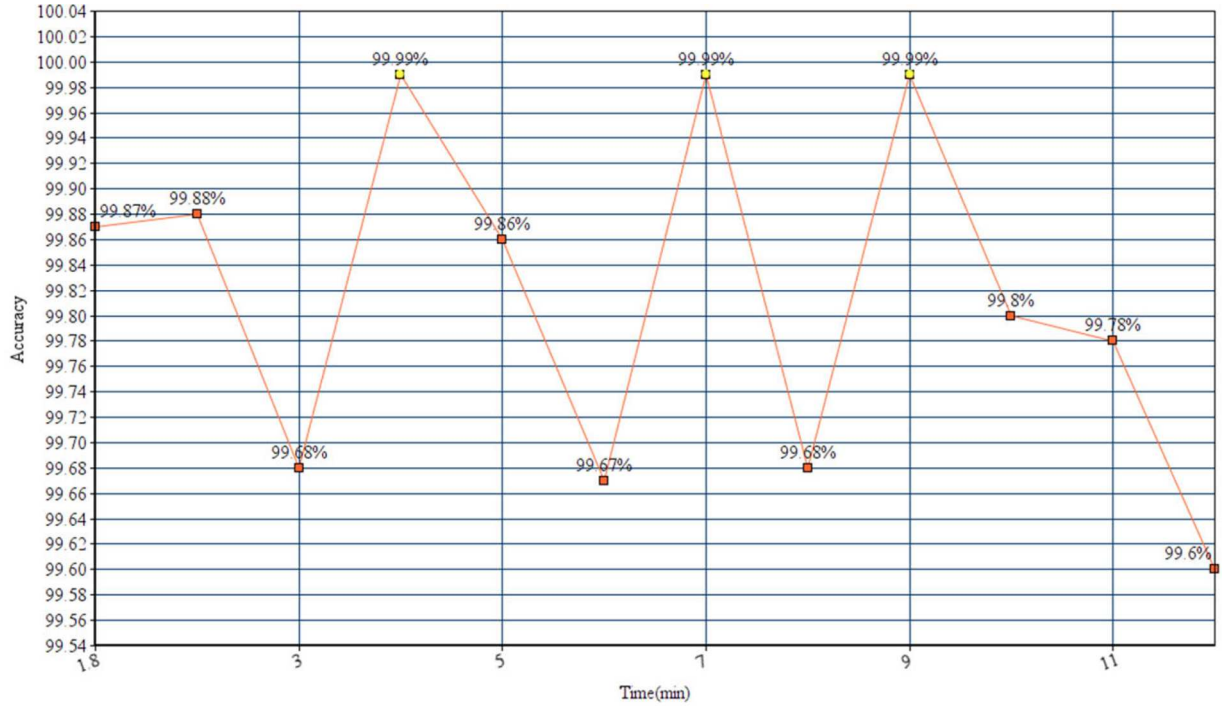


Fig. 22. CA performance for Decision Tree model using ECG and EMG data executed on OSC environment.

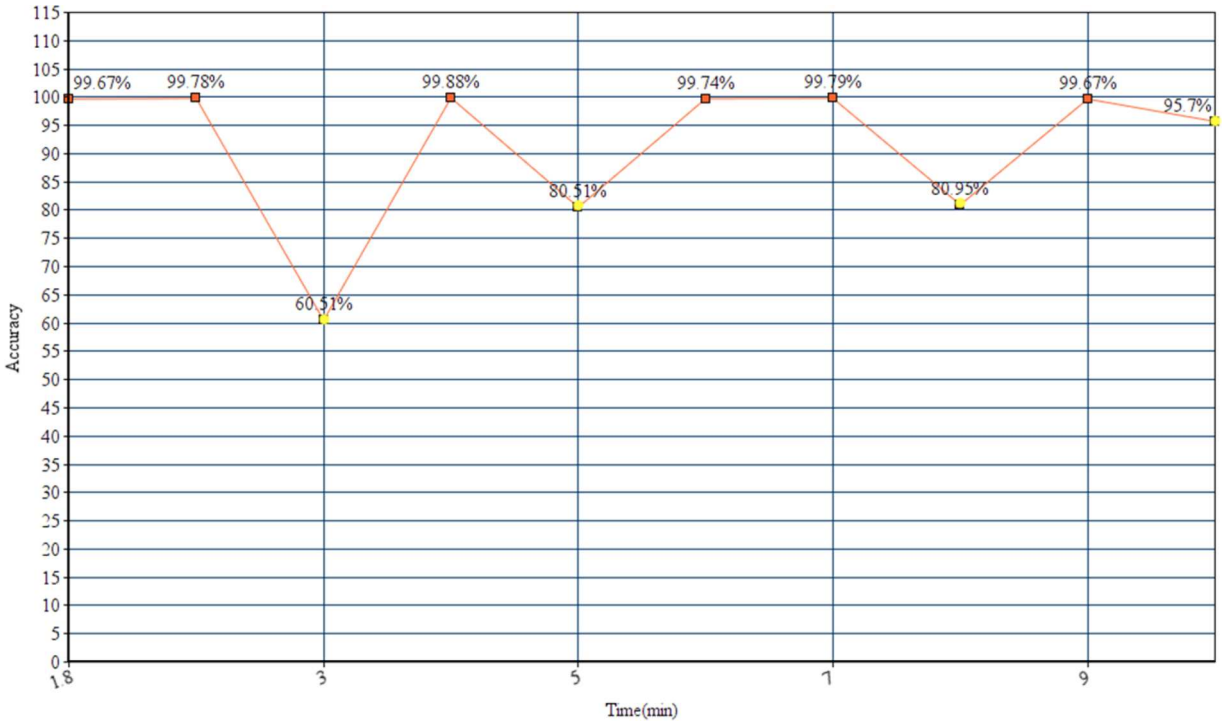


Fig. 23. CA performance for CNN model using ECG and EMG data executed on OSC environment.

7. CA experimentation and results/solution evaluation for ECG and EMG based-approach

The following figures in the results section are based on continuous authentication with different approaches and different machine learning models with best performance are selected for comparison purposes.

7.1. CA experimental results for ECG-based authentication with different CNN models

Fig. 16-20 shows the performance of authentication using ECG with different configuration in CNN model and executed in Ohio supercomputers with 1 node to get ECG accuracy. Fig. 16 represents adding only 15 parameters of QRS complex data in Data Preprocessing stage. Fig. 17 represents authentication using ECG with different approaches in the CNN model. The traditional approach of 25 QRS parameters needs more time and parameters when compared to our limit on QRS complex [5].

The following result in Fig. 17 is for the current state of art machine learning model [5] with CNN layer 1 which is conducted on Ohio supercomputers (OSC) and 1 node was used to get ECG's machine learning model and its accuracy. Fig. 17 represents current state of art approach of adding 25 parameters of QRS complex data in Data Preprocessing with CN-layer 1 included in CNN model executed on Ohio supercomputer environment using 1 node.

Fig. 18-20 represents comparisons of different methods of CNN model for ECG authentication with respect to the behavior of the model and time being a constraint in a continuous authentication approach. Fig. 18 represents the results of our approach with adding 15 parameters of QRS complex in machine learning model with discarding convolutional layer 1. The behavior of model represents to be fastest among all approaches in CNN model.

Fig. 19 represents the binary approach done with CNN model for continuous authentication with ECG. The binary weight approach replaces original floating-point integers with binary numbers (1 and −1). Here 25 parameters of QRS are randomly selected.

Fig. 20 represents the CNN network is supplied all of the ECG data with features for training and testing. They go via a stack of several convolutions and max-pooling layers, two completely linked layers, and a soft-max layer which is the normal approach used while experimenting with ECG authentication. Here 25 parameters of QRS are randomly selected.

7.2. CA experimental results for combined ECG and EMG-based ML models

We have performed ECG & EMG authentication where EMG is used as a second layer of authentication. The yellow dots in graph represents the switching to second layer of authentication only if the ECG authentication is below threshold. The threshold set by us is 99.50% accuracy. We set up the threshold to the highest level because we wanted to know how frequently the continuous authentication gets changed to EMG and then back to ECG. With the accuracy threshold of 99.50%, we can leverage the results of the most secure and authentic approach for continuous authentication on IoT devices.

7.2.1. SVM model for ECG and EMG authentication

Fig. 21 shows the performance of continuous authentication using ECG and EMG with SVM model used at both ECG & EMG authentication layers. While performing the following experiment as we can see that the system relies more on EMG authentication rather than ECG as primary because SVM model for ECG authentication has lower accuracy than 99.50% many times while performing

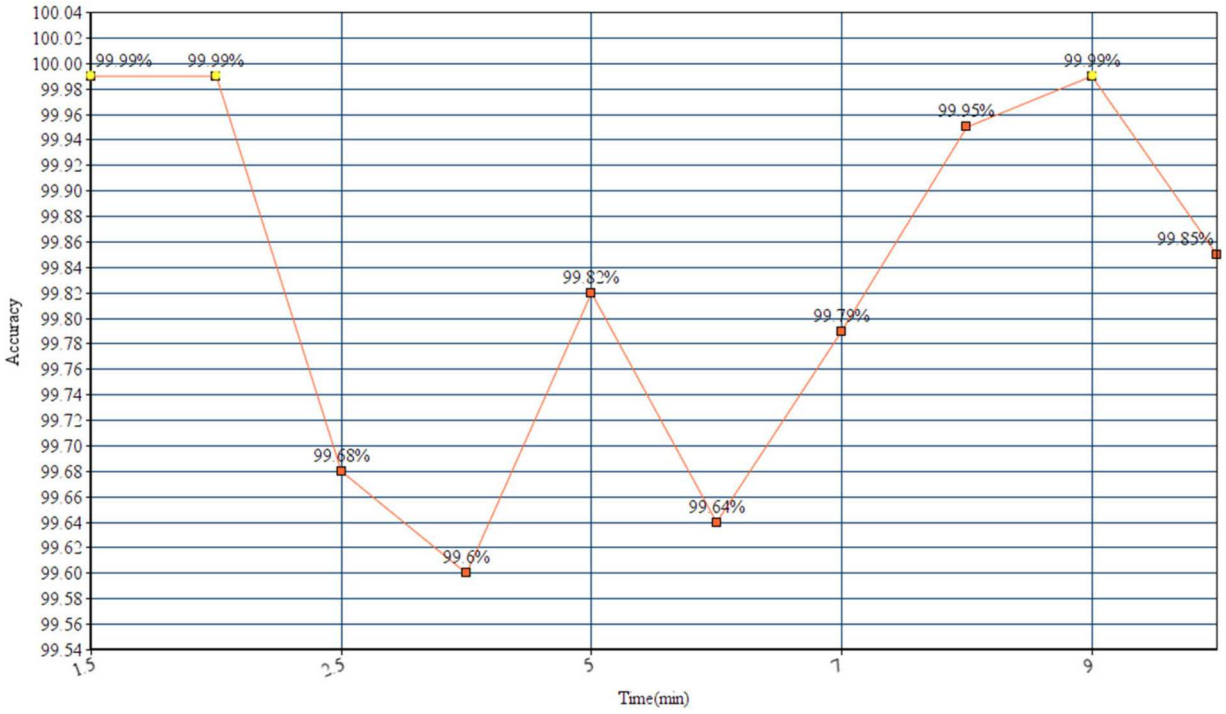


Fig. 24. CA performance for CNN model using ECG and DT using EMG data executed on OSC environment.

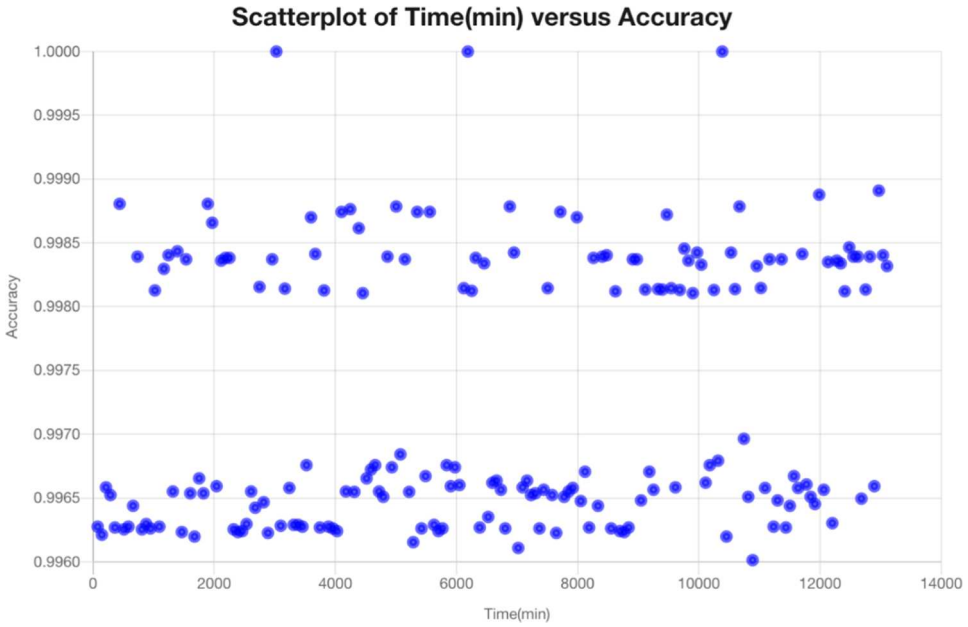


Fig. 25. CA performance with the best approach and authentication number set to 11,000 executed on OSC environment.

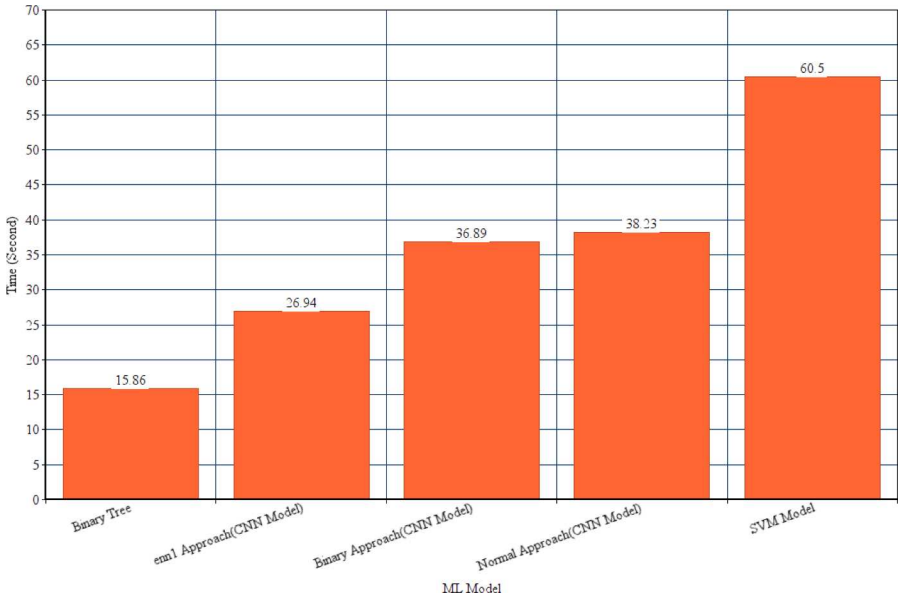


Fig. 26. CA Latency with the different approaches executed on OSC environment.

continuous authentication. This is the worst performance we observed with ECG and EMG authentication.

7.2.2. Decision tree for ECG and EMG authentication

Fig. 22 shows the performance of continuous authentication using ECG and EMG data with Decision Tree model at both ECG & EMG authentication layers. While performing this experiment as we can see Decision Tree has on average less accuracy on ECG and has less switching to second layer of authentication which is EMG authentication resulting in lower average accuracy. Yellow color in the graph represents switch from ECG to EMG due to accuracy threshold set to 99.50%.

7.2.3. CNN model for ECG and EMG authentication

Fig. 23 shows the performance of continuous authentication using CNN model for ECG and EMG data at both ECG & EMG authentication layers. While performing CNN model for ECG and EMG authentication, it clearly represents low accuracy on second

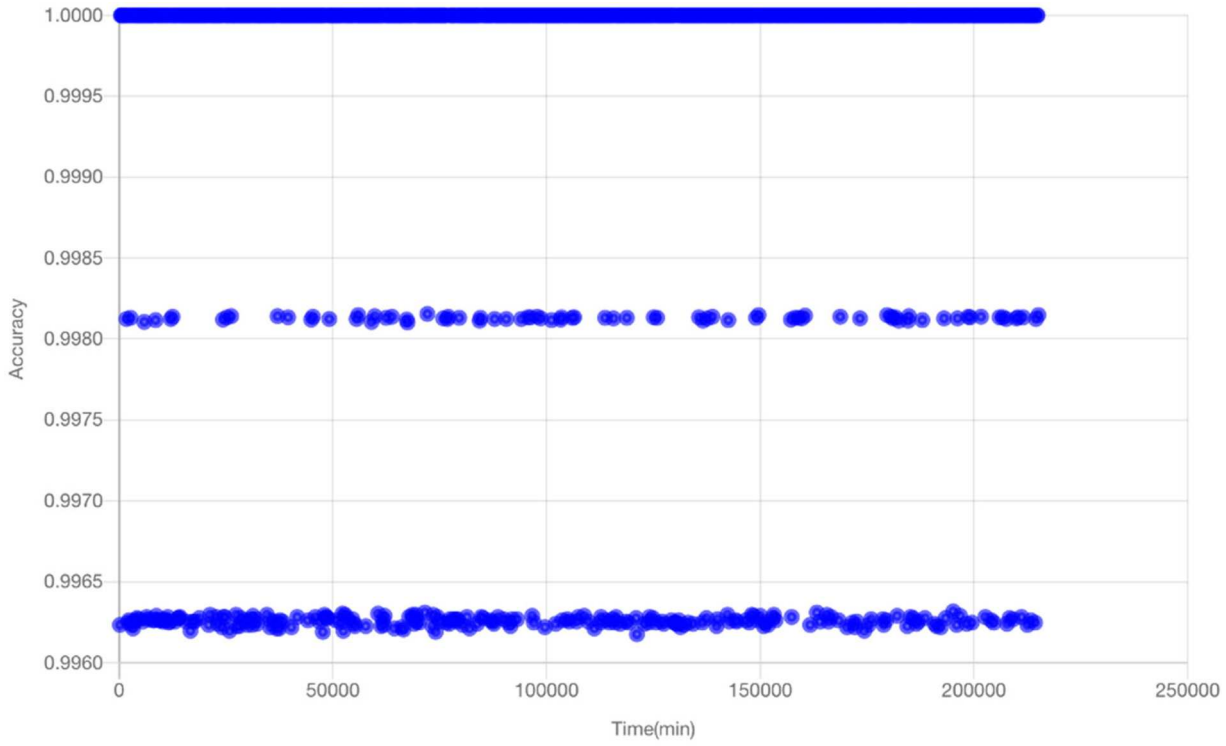


Fig. 27. Performance of CA with respect to accuracy vs time for 3 days of CA of raspberry pi.

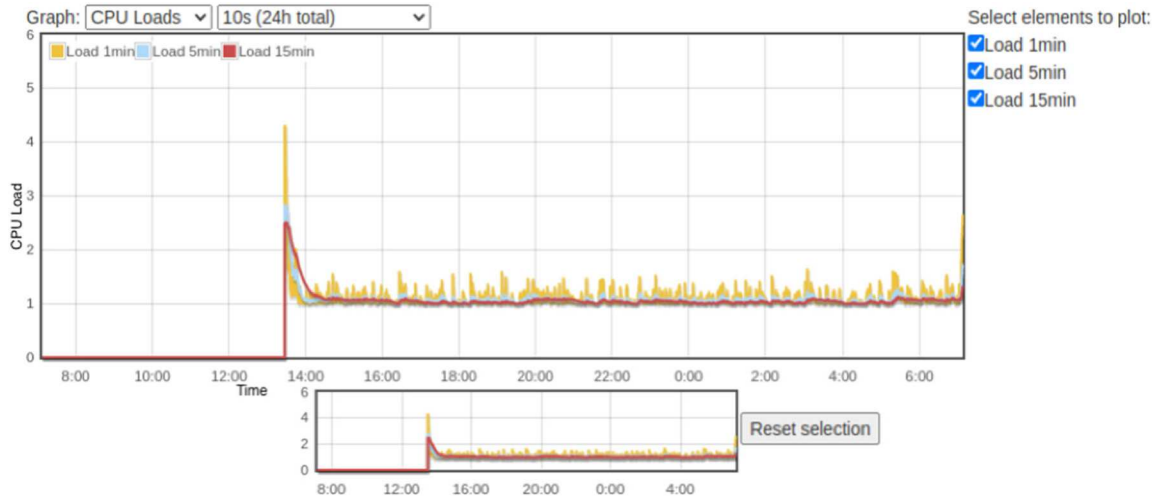


Fig. 28. CPU load for performing CA in raspberry pi.

layer of security which is EMG that is yellow spots in graphs, which is not acceptable. The following continuous authentication behavior is the worst scenario at the EMG level and it needs a lot of performance power to conduct the experiment. Another problem with the CNN model found during experimentation was it needs more time to initiate as the authentication file uses both models as CNN which requires more time in the initiation phase.

7.2.4. CNN model for ECG and decision tree for EMG authentication (Best authentication approach)

Since CNN model performed best at ECG layer and DT performance best at EMG layer. We did not choose the CNN model for EMG as it would require a major amount of performance power for TWO CNN model running on a system, one for ECG and the other for EMG. We performed the experiment with CNN model for ECG and Decision Tree model for EMG and got a quit promising result. The graph

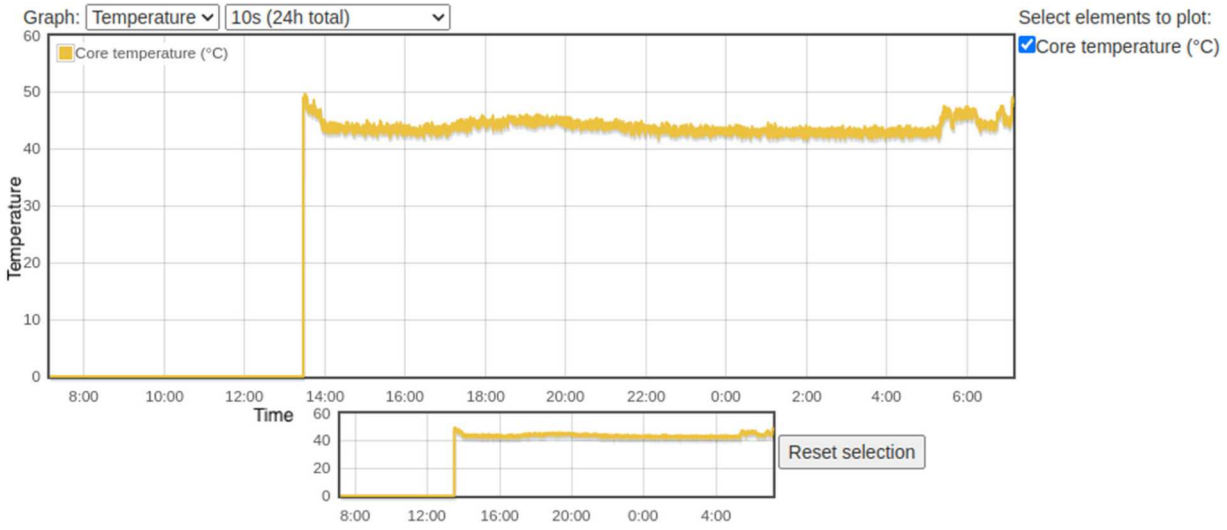


Fig. 29. Temperature of core processor for performing CA in raspberry pi.

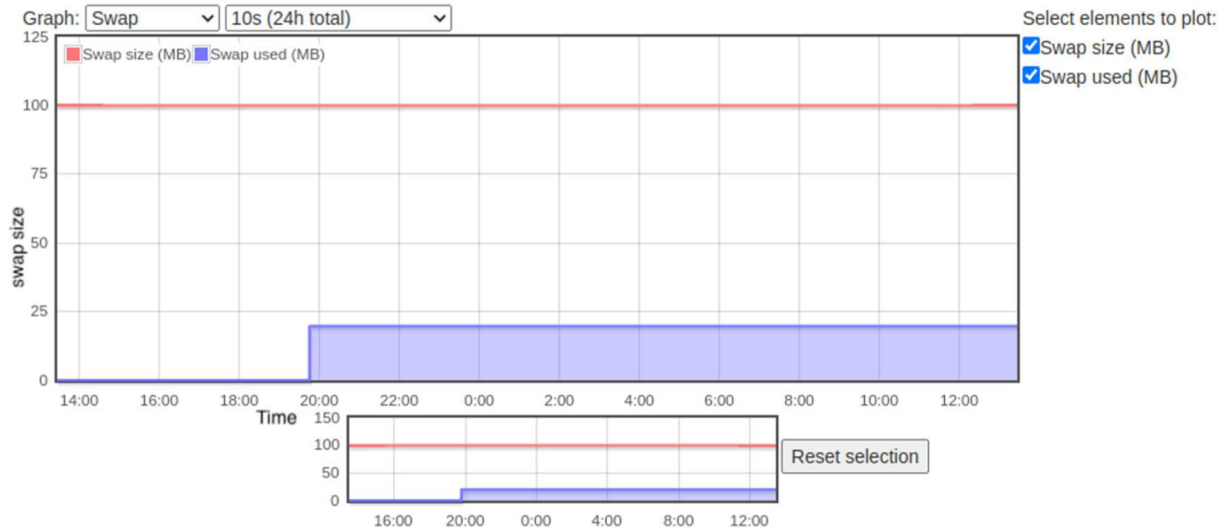


Fig. 30. Swap size for performing CA in raspberry pi.

shown in Fig. 24 is the accuracy of ECG at layer 1 and EMG at layer 2 authentication. The yellow point in the following graph represents the EMG authentication switch from ECG authentication. The following continuous authentication behavior is the best case taken from the experiment because it has the highest average accuracy while performing CA and the lowest performance requirement.

Fig. 25 shows a continuous authentication pattern with the number of authentications set at 11,000. The following graph has been plotted with the number of 300 points of accuracy data with its respective time. With the help of Fig. 25 we can also see the continuous authentication pattern between time frames which stays between 99.60%−99.70%, 99.80%−99.90% and 100% all the time when being executed.

7.3. CA experimentation-latency metrics

Fig. 26 represents the latency between identifying individuals with respect to different ML models. As we can see from the Fig. 26 decision tree outperforms all different ML models in terms of Latency which is the only reason the second layer of EMG authentication was selected with the decision tree because dual CNN model will result in tremendous latency on IoT devices. We can also identify that the CNN exponent_n1 approach with 15 parameters has the least latency out of all other models with consideration of the best accuracy result from the above figures.

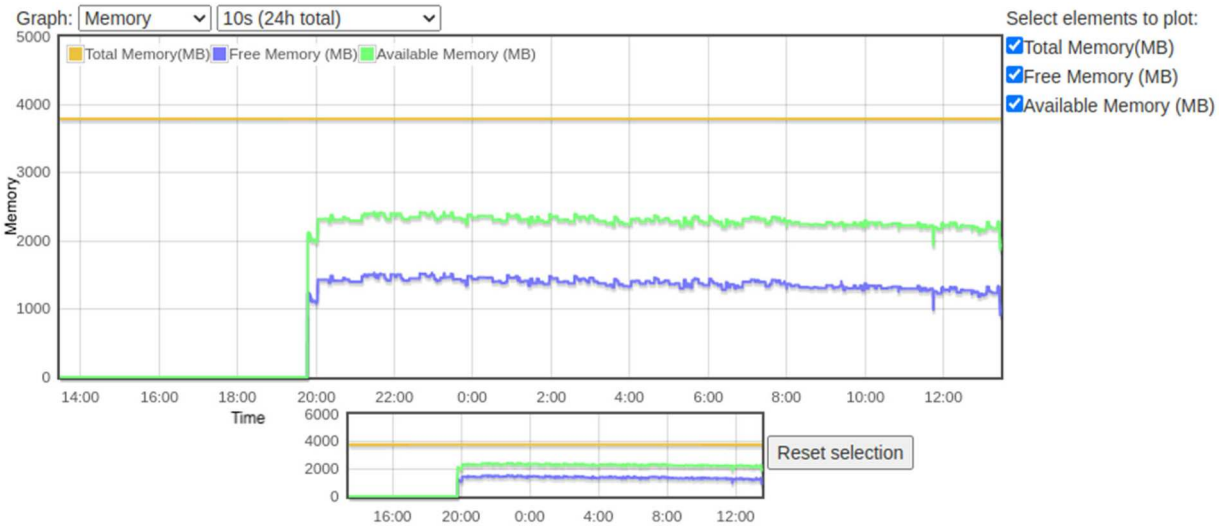


Fig. 31. Total memory used for performing CA in raspberry pi.

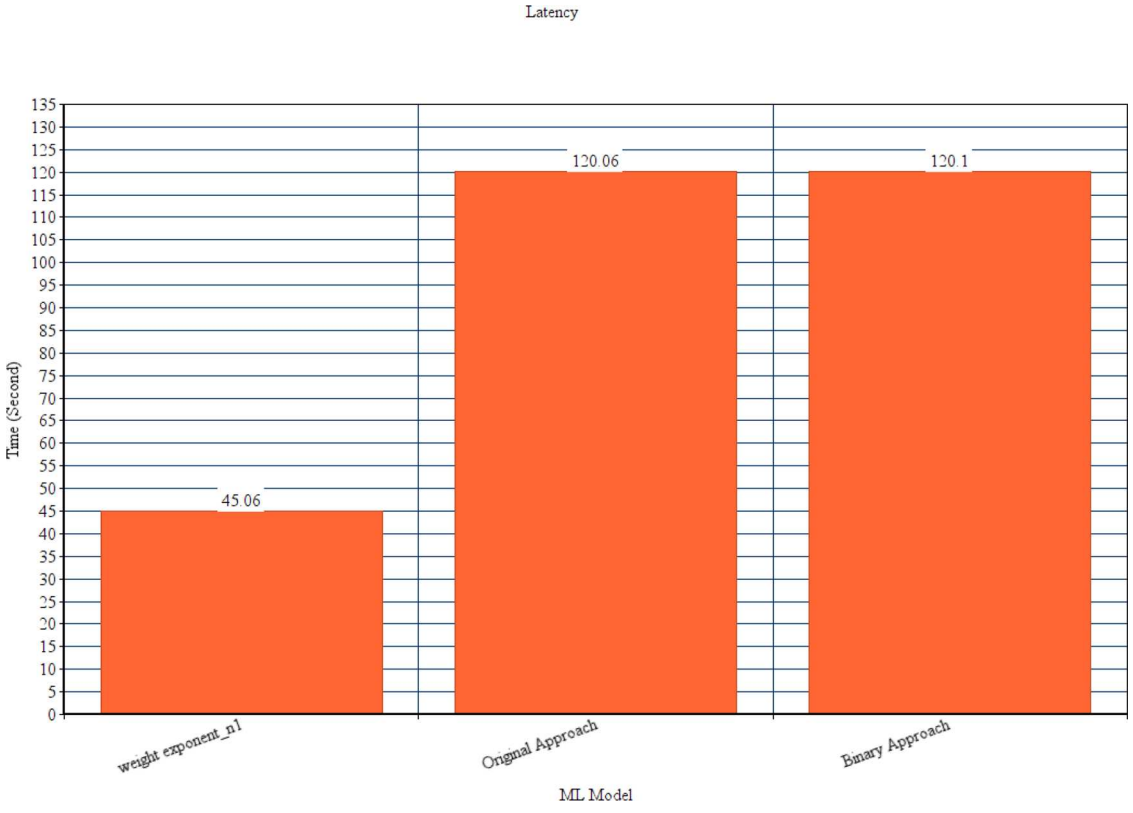


Fig. 32. CA Latency with different ML CNN models with ECG&EMG in raspberry pi.

7.4. CA experimentation evaluated on raspberry Pi

The following Fig. 27-31 represents the accuracy, performance, swap size, temperature, memory vs time on raspberry pi with respect to continuous authentication. Here the number of authentications is set at 11,000. We set the RAM limit to 1GB and restricted the system to utilize 1 CPU core to simulate resource-constrained IoT environments. The Raspberry Pi 4, with its Broadcom BCM2711 SoC featuring a Quad-core Cortex-A72 ARMv8 processor running at 1.8 GHz and 4GB LPDDR4–3200 SDRAM, provides a relevant platform for our experimentation. The combination of wireless connectivity (2.4 GHz and 5.0 GHz IEEE 802.11ac wireless, Bluetooth

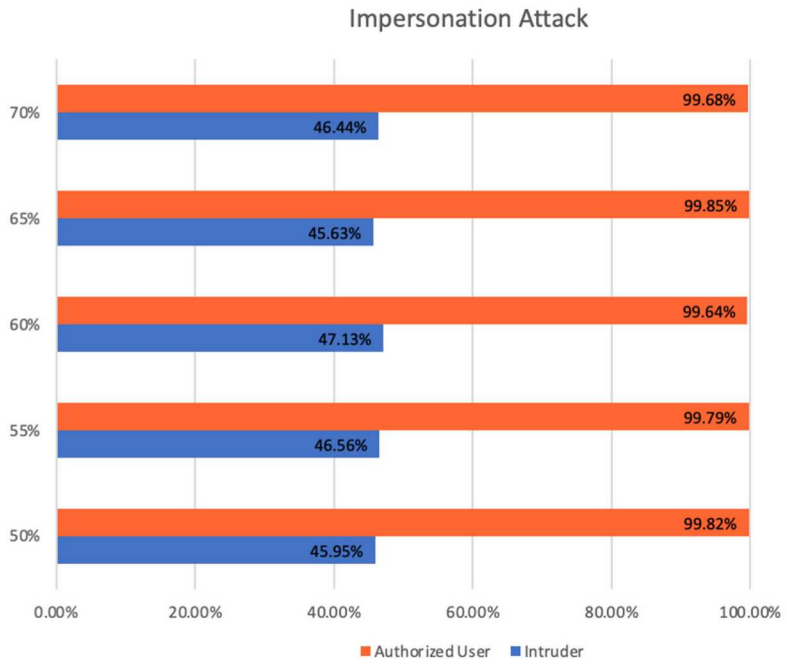


Fig. 33. Model Robustness against impersonation attack.

5.0, BLE), Gigabit Ethernet, USB ports, HDMI ports, GPIO header, and various multimedia capabilities ensures the Raspberry Pi 4 is a suitable choice for IoT applications.

Fig. 27 represents the pattern of continuous authentication with respect to accuracy vs time for 3 days of continuous authentication on raspberry pi with ECG and EMG sensor data. Here the number of authentications is 11,000 and the dots in Fig. 27 represent one authentication at a distinct time interval. With the help of Fig. 27 we can also see the continuous authentication pattern between time frames which stays between 99.60%−99.65%, 99.80%−99.85% and 100%, similarly to Fig. 27. We can see the similar behavior between experiment performed in OSC(Fig. 26) and experiment performed in raspberry pi (Fig. 27). So that it is proved that e our experiment performed in raspberry pi sustained the highest average accuracy of continuous authentication with our method.

Fig. 28 represents the CPU load, which is extracted from RPI-Monitor repository. The CPU load remains between 1 CPU load for entire continuous authentication and 1–2 with other system's requirement running, the spike is because of opening and closing of browser to get the result during continuous authentication.

As shown in Fig. 29, the temperature graph examines the temperature of core processor during the performance of continuous authentication with respect to time. The core temperature is directly proportional to CPU load as increase in performance leads to increase of temperature which is the reason of small spike between 40 and 50.

The graph in Fig. 30 represents the swap size of IoT device, where used swap and free swap size are defined with respect to time and the following graph is extracted during continuous authentication on IoT.

The graph in Fig. 31 represents the memory used while performing continuous authentication with respect to time. The reason for the usage of memory while performing experiments is due to storing raw accuracy data of machine learning models in an array with respect to time, which was used to plot all the graphs of different ML model on all of the above section of performance of CA.

Fig. 32 shows the result of different CNN model approaches used to perform authentication with having EMG authentication as a second layer of authentication. SVM model was not considered in IoT due to its large latency in OSC environment which is presented in Fig. 32. As we can see from the Fig. 32, we conclude that exponent_en1 should be used for ECG authentication and DT model used for EMG authentication in our CA schema rather than using traditional CNN models approach used in previous state of art.

8. Robustness against impersonation attack

The results obtained from our experiments provide valuable insights into the model's robustness against impersonation attacks. By manipulating 50% to 70% of the fiducial points of the authorized user, we effectively simulate an impersonation scenario and trained model accordingly. We analyze the model's accuracy, comparing the outcomes for the test intruder and the genuine test user. This analysis helps us gage the system's susceptibility to impersonation attacks and assess its ability to accurately differentiate between genuine and unauthorised users.

To evaluate the system's robustness against impersonation attacks, we conducted experiments and analyzed the results. Fig. 33 presents the findings, illustrating the accuracy of the model in distinguishing between authorized users and impersonating users (intruders). In Fig. 33, the y-axis represents the percentage of data used to impersonate an authorized user. The accuracy values are

depicted using two bars: a blue bar representing the accuracy of the intruder and an orange bar representing the accuracy of the authorized user.

The graph clearly demonstrates that the model exhibits a notable capability to differentiate between the authorized user and the impersonating user (intruder). This distinction is evidenced by the intruder's lower accuracy, as indicated by the blue bar. Conversely, the authorized user achieves a comparatively higher accuracy, represented by the orange bar. The discrepancy in accuracy between the intruder and the authorized user implies that the system successfully identifies and distinguishes between genuine users and impersonators. The lower accuracy of the intruder indicates the model's ability to detect and reject unauthorised access attempts because of EMG authentication as a second layer of authentication.

These results highlight the robustness of our continuous authentication system against impersonation attacks. The system's capability to differentiate between authorized users and impersonators is a promising indication of its resistance to unauthorised access and manipulation.

9. Anonymization and data protection in CA biometrics

In our proposed continuous authentication (CA) scheme utilizing ECG and EMG, data protection and privacy are paramount considerations. As our method involves sensitive health data, it is essential to ensure that the implementation complies with privacy protection standards outlined by the General Data Protection Regulation (GDPR) in the European Union (EU) [28].

In the context of GDPR, anonymization is defined as a process of turning data into a form which does not identify individuals and where identification is not likely to take place. To comply with this principle, our CA scheme includes several layers of anonymization:

1 De-identification: All personally identifiable information (PII), such as names and addresses, are removed from the data before processing. This includes direct identifiers as well as indirect identifiers that could potentially be linked back to the individual.
2 Data Masking: Raw ECG and EMG data are transformed in such a way that their original characteristics are not discernible but their format is preserved for computational analysis.
3 Noise Addition: We add a small amount of statistical noise to the data which prevents the original data from being reconstructed.

The anonymization process ensures that individual data cannot be traced back to the original subject, thereby providing a high level of privacy protection. However, it is also important to note that this process does not significantly alter the accuracy of our CA scheme.

In terms of the GDPR-EU documentation [28], the key aspects addressed by our method include lawful basis for processing (Article 6), rights of the data subject (Articles 15–22), and the data protection principles outlined in Article 5.

1 Lawful basis for processing: Data are processed on the basis of explicit consent from the user, and this consent can be withdrawn at any time.
2 Rights of the data subject: Individuals have the right to access their data, correct inaccuracies, request the erasure of their data, and object to or limit its processing. These rights are ensured by the design of our system.
3 Data protection principles: We have designed our CA scheme to meet the GDPR principles of data minimization, accuracy, storage limitation, and integrity and confidentiality.

In conclusion, while our proposed CA biometrics scheme provides a novel approach to authentication, we have taken considerable measures to ensure that it respects privacy and upholds the principles of GDPR. We believe that a balance between technological innovation and data privacy is not just feasible, but essential in today's digital world.

10. Lessons learned and future actions

The main purpose of our work is to study an effective approach of combining ECG-based authentication along with EMG-based authentication with respect to CA for IoT devices. The experiment conducted to evaluate a continuous authentication method using ECG and EMG data for IoT devices provided valuable lessons. Firstly, the significance of proper preprocessing of data was evident. By applying various preprocessing techniques such as resampling, peak detection, outlier removal, and correlation analysis for ECG data, and baseline correction, filtering, segmentation, feature extraction, and normalization for EMG data, the experiment demonstrated the importance of preparing the data accurately. These preprocessing steps played a crucial role in ensuring the reliability and accuracy of the authentication system.

Secondly, the choice of machine learning models had a significant impact on the system's performance. The experiment compared different models such as CNN, SVM, and Decision Tree for ECG and EMG authentication. It was observed that the selection of models influenced factors like accuracy, latency, and resource utilization. The best-performing approach was found to be a combination of CNN for ECG authentication and Decision Tree for EMG authentication, striking a balance between accuracy and computational efficiency. Considering the computational resources and latency constraints is crucial when designing authentication systems for IoT devices. Additionally, the experiment highlighted the advantages of a multi-layer authentication approach. By incorporating a secondary authentication layer (EMG) alongside the primary layer (ECG), the system achieved enhanced security. This two-layer approach provided an additional level of verification and increased the overall accuracy and reliability of the continuous authentication system.

While our preliminary experiments are successful, further research can be conducted to improve the latency of authentication. As an extension of the proposed approach, signal can be sent with the help of existing wireless signals by reflecting wireless signal with LTE-Backscatter device [2] which will be received by a receiver. The backscatter device requires no power source to transmit ECG and EMG signals. Once the Backscatter device is implanted in any person's hand, it will transmit an ECG and EMG signal with the help of a sensor and send it simultaneously with the help of existing wireless signals by reflecting wireless signal to a receiver that requires no power source to transmit. Future research and development efforts could focus on enhancing the bandwidth, data transfer rate, and signal fidelity of backscatter LTE devices to accommodate the complex analog nature of ECG and EMG signals. This would involve optimizing the modulation and reflection techniques used in backscatter technology to ensure accurate and reliable transmission of these biomedical signals. Further, the receiver will use our mentioned approach presented in Fig. 2. This approach will be continuous, and as soon as the system detects any intruder or authorized person leaves, the access will be denied immediately. Our research and integration of backscatter devices will help create a further novel approach for continuous authorization, creating the innovative smallest backscattering authorization system for continuous authentication system with the highest efficiency, no power source, and non-interaction with humans. This system will make it easier for people to integrate with the existing IoT applications effectively.

We will also be extending our focus to encompass the privacy aspect associated with this novel continuous authentication method. Recognizing that both electrocardiogram (ECG) and electromyography (EMG) data are sensitive medical information, any potential leakage could lead to serious privacy issues. Consequently, we will be adopting anonymization techniques, the effectiveness of which will be quantified in terms of the identifiable features removed and the level of distortion applied to the raw biometric data. This is expected to ensure that any compromised data cannot be linked back to an individual. Furthermore, we will be looking into the guidelines and regulations proposed by the General Data Protection Regulation (GDPR) in the European Union, which provides a well-defined framework for the protection of personal data. By aligning our method with these stipulations, we aim to not only enhance the security of our authentication scheme but also to ensure its compliance with international data protection standards, therefore guaranteeing the privacy and security of user data.

11. Conclusion

In this work, we designed and evaluated that a continuous authentication scheme using ECG and EMG data for IoT devices. This security solution targets a wide range of IoT devices, and all IoT, MIoT and IIoT devices are equipped with at least one wireless frequency. Based on our experiment CNN performed best for ECG data and Decision Tree performed best for EMG data with holding average accuracy of overall system 99.90%. This research paper also highlights the significance of evaluating model robustness against impersonation attacks through fiducial point manipulation. Our experiments on a representative dataset demonstrate the model's robustness against vulnerability to impersonation attack. Our proposed solution requires a small hardware circuit, which will calculate biometric data and transmit it on the current wireless signal from the body and to IoT device. Our technology can perform continuous authentication without interaction from human interest or without interference with the already crowded wireless spectrum, compared to conventional authentication methods. Our proposed framework can serve diverse IoT applications.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgements

This study was supported by funding through the US National Science Foundation Award number 2028397.

References

[1] Y. Liang, S. Samtani, B. Guo, Z. Yu, Behavioral biometrics for continuous authentication in the Internet-of-Things era: an artificial intelligence perspective, IEEE Internet of Things J. 7 (9) (Sept. 2020) 9128–9143, https://doi.org/10.1109/JIOT.2020.3004077.

[2] Z. Chi, X. Liu, W. Wang, Y. Yao, T. Zhu, Leveraging ambient LTE traffic for ubiquitous passive communication, in: Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication, Jul. 2020, https://doi.org/10.1145/3387514.3405861.

[3] J.R. Pinto, J.S. Cardoso, Explaining ECG biometrics: is it all in the QRS?, in: 2020 International Conference of the Biometrics Special Interest Group (BIOSIG), 2020, pp. 1–5.

[4] Y. Chu, H. Shen, K. Huang, ECG authentication method based on parallel multi-scale one-dimensional residual network with center and margin loss, IEEE Access 7 (2019) 51598–51607, https://doi.org/10.1109/ACCESS.2019.2912519.

[5] R. Donida Labati, E. Muñoz, V. Piuri, R. Sassi, F. Scotti, Deep-ECG: convolutional neural networks for ECG biometric recognition, Pattern Recognit. Lett. 126 (2019) 78–85, https://doi.org/10.1016/j.patrec.2018.03.028.

[6] C. Smyth, G. Wang, R. Panicker, A. Nag, B. Cardiff, D. John, Continuous user authentication using IoT wearable sensors, in: 2021 IEEE International Symposium on Circuits and Systems (ISCAS), 2021, pp. 1–5, https://doi.org/10.1109/ISCAS51556.2021.9401741.

[7] S. Aziz, M.U. Khan, Z.Ahmad Choudhry, A. Aymin, A. Usman, ECG-based biometric authentication using empirical mode decomposition and support vector machines, in: 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Oct. 2019, https://doi.org/10.1109/iemcon.2019.8936174.
[8] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, A. Zanella, IoT: internet of Threats? A survey of practical security vulnerabilities in real IoT devices, IEEE Internet of Things J. (2019) 1, https://doi.org/10.1109/jiot.2019.2935189.
[9] Vailshery, L.S., "Global Number of Connected IoT Devices 2015-2025," Statista. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.
[10] F.H. Al-Naji, R. Zagrouba, A survey on continuous authentication methods in Internet of Things environment, Comput. Commun. 163 (Nov. 2020) 109–133, https://doi.org/10.1016/j.comcom.2020.09.006.
[11] M. Shahzad, M.P. Singh, Continuous authentication and authorization for the Internet of Things, IEEE Internet Comput 21 (2) (Mar.-Apr. 2017) 86–90, https://doi.org/10.1109/MIC.2017.33.
[12] H. Alamleh, A.A.S. AlQahtani, Architecture for continuous authentication in location-based services, in: 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), 2020, pp. 1–4, https://doi.org/10.1109/3ICT51146.2020.9311972.
[13] A. Badhib, S. Alshehri, A. Cherif, A robust device-to-device continuous authentication protocol for the Internet of Things, IEEE Access 9 (2021) 124768–124792, https://doi.org/10.1109/ACCESS.2021.3110707.
[14] S. Bao, W. Hathal, H. Cruickshank, Z. Sun, P. Asuquo, A. Lei, A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and bloom filters, ICT Express 4 (4) (Dec. 2018) 221–227, https://doi.org/10.1016/j.icte.2017.12.001.
[15] D. Crouse, H. Han, D. Chandra, B. Barbello, A.K. Jain, Continuous authentication of mobile user: fusion of face image and inertial Measurement Unit data, in: 2015 International Conference on Biometrics (ICB), May 2015, https://doi.org/10.1109/icb.2015.7139043.
[16] Y. Zhang, W. Hu, W. Xu, C.T. Chou, J. Hu, Continuous authentication using eye movement response of implicit visual stimuli, in: Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1, Jan. 2018, pp. 1–22, https://doi.org/10.1145/3161410.
[17] H. Feng, K. Fawaz, K.G. Shin, Continuous authentication for voice assistants, in: Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking - MobiCom '17, 2017, https://doi.org/10.1145/3117811.3117823.
[18] L. Gonzalez-Manzano, J.M.D. Fuentes, A. Ribagorda, Leveraging user-related Internet of Things for continuous authentication, ACM Comput. Surv. 52 (3) (Jul. 2019) 1–38, https://doi.org/10.1145/3314023.
[19] S. Mekruksavanich, A. Jitpattanakul, Deep learning approaches for continuous authentication based on activity patterns using mobile sensing, Sensors (Basel) 21 (22) (2021) 7519, https://doi.org/10.3390/s21227519.
[20] Ruggero Donida Labati, Enrique Munoz, Vincenzo Piuri, Roberto Sassi, Fabio Scotti, Deep-ECG: convolutional neural networks for ECG biometric recognition, Pattern Recognit. Lett. 126 (2019) 78–85.
[21] A. Barros, D. Rosario, P. Resque, E. Cerqueira, Heart of IoT: ECG as biometric sign for authentication and identification, in: 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Jun. 2019, https://doi.org/10.1109/iwcmc.2019.8766495.
[22] G. Wang, D. John, A. Nag, Low complexity ECG biometric authentication for IoT edge devices, in: 2020 IEEE International Conference on Integrated Circuits, Technologies and Applications (ICTA), 2020, pp. 145–146, https://doi.org/10.1109/ICTA50426.2020.9332012.
[23] P. Chandrakar, A. Kumar, R. Ali, R.D. Patidar, A Secure ECG based Smart Authentication Scheme for IoT Devices, 2021 Emerging Trends in Ind. 4.0 (ETI 4.0) (2021) 1–7, https://doi.org/10.1109/ETI4.051663.2021.9619283.
[24] T. Lugovaya, "The ECG-ID database [Data set]", 2011, [online] Available: https://doi.org/10.13026/C2J01F.
[25] Q. Li, Z. Luo, J. Zheng, Deep learning-based user authentication with surface emg images of hand gestures, in: 2021 43rd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), 2021, pp. 2038–2041, https://doi.org/10.1109/EMBC46164.2021.9630312.
[26] H. Yamaba, et al., On a user authentication method to realise an authentication system using s-EMG, Int. J. Grid and Utility Comput. 11 (5) (2020) 725, https://doi.org/10.1504/ijguc.2020.110060.
[27] D. Progonov, O. Sokol, Heartbeat-based authentication on smartwatches in various usage contexts, Lecture Notes in Comput. Sci. (2021) 33–49, https://doi.org/10.1007/978-3-030-93747-8_3.
[28] N. NA, Official legal text, General Data Protection Regulation (GDPR) (Jul. 10, 2023). https://gdpr-info.eu/(accessed.
[29] R. Jones, Researchers Show Off Method For Hacking Tesla's Keyless Entry, So Turn On Two-Factor Authentication, October 22, Gizmodo, 2018. Retrieved January 25, 2022, from, https://gizmodo.com/researchers-show-off-method-for-hacking-tesla-s-keyless-1828951056.
[30] N. Belgacem, R. Fournier, A. Nait-Ali, F. Bereksi-Reguig, A novel biometric authentication approach using ECG and EMG signals, J. Med. Eng. Technol. 39 (4) (Apr. 2015) 226–238, https://doi.org/10.3109/03091902.2015.1021429.
[31] S.A. Raurale, J. McAllister, J.M.D. Rincon, EMG biometric systems based on different wrist-hand movements, IEEE Access 9 (2021) 12256–12266, https://doi.org/10.1109/access.2021.3050704.
[32] A.M.H. Wong, M. Furukawa, H. Ando, T. Maeda, Dynamic hand gesture authentication using electromyography (EMG), in: 2020 IEEE/SICE International Symposium on System Integration (SII), 2020, pp. 300–304, https://doi.org/10.1109/SII46433.2020.9026294.
[33] M. Hammad, S. Zhang, K. Wang, A novel two-dimensional ECG feature extraction and classification algorithm based on convolution neural network for human authentication, Future Generation Comput. Syst. 101 (Dec. 2019) 180–196, https://doi.org/10.1016/j.future.2019.06.008.
[34] M. Hammad, P. Pławiak, K. Wang, U.R. Acharya, ResNet-attention model for human authentication using ECG signals, Expert Syst. 38 (6) (Mar. 2020), https://doi.org/10.1111/exsy.12547.
[35] L. Lu, J. Mao, W. Wang, G. Ding, Z. Zhang, A study of personal recognition method based on EMG signal, IEEE Trans. Biomed. Circuits Syst. 14 (4) (Aug. 2020) 681–691, https://doi.org/10.1109/TBCAS.2020.3005148.
[36] W. Chai, What is confidentiality, integrity, and availability (CIA triad)? - Definition from WhatIs.com, WhatIs.com (2019). https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.
[37] H.J. Kim, J.S. Lim, Study on a biometric authentication model based on ECG using a fuzzy neural network, IOP Conference Series: Mater. Sci. Eng. 317 (Mar. 2018), 012030, https://doi.org/10.1088/1757-899x/317/1/012030.
[38] A.L. Goldberger, et al., PhysioBank, PhysioToolkit, and PhysioNet, Circulation 101 (23) (Jun. 2000), https://doi.org/10.1161/01.cir.101.23.e215.