Computer Communications 240 (2025) 108201

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Standardizing the evaluation framework for ECG-based authentication in IoT devices

Bonan Zhang [a,*], Lin Li [c], Chao Chen [a], Ickjai Lee [b], Kyungmi Lee [b], Kok-Leong Ong [a]

[a] RMIT University, 124 La Trobe St, Melbourne, 3000, VIC, Australia
[b] James Cook University, 1 James Cook Dr, Townsville, 4814, QLD, Australia
[c] Southern Cross University, Gold Coast Airport, Gold Coast, 4225, QLD, Australia

ARTICLE INFO

Keywords:
IoT
Biometric
ECG authentication
AI

ABSTRACT

Devices on the Internet of Things (IoT) often have constrained resources and operate in diverse environments, making them vulnerable to unauthorized access and cyber threats. Electrocardiogram (ECG) signals have emerged as a promising biometric for authenticating users in such settings. However, current ECG-based authentication studies lack a standardized evaluation framework tailored to resource-limited IoT contexts and long-term usage, making it difficult to assess their practical reliability. In this paper, we introduce a new evaluation framework for ECG-based authentication on IoT devices and construct a standardized dataset to facilitate rigorous testing. We categorize performance metrics into four key dimensions: scalability, adaptability, efficiency, and cancelability. Using this framework, we evaluate four representative ECG authentication algorithms for IoT devices. The results show that these algorithms struggle to maintain consistent performance under cross-session authentication scenarios. These findings highlight the critical importance of addressing the temporal variability of ECG signals and the current gap in robust ECG-based authentication for IoT devices. We believe the proposed framework will guide future research toward more resilient and secure ECG authentication systems for the IoT.

1. Introduction

The Internet of Things (IoT) refers to a vast network of interconnected devices. Most IoT devices are resource limited, but can perform operations such as sensing, monitoring, preprocessing, and information exchange [1]. By facilitating communication among devices, the IoT is able to manage diverse scenarios efficiently and precisely [2]. Recent advancements in communication technologies and in hardware/software components have spurred the rapid proliferation of IoT devices. Currently, the Internet of Things (IoT) is widely utilized in areas such as healthcare, industrial manufacturing, and smart home solutions. The projections suggest that the number of IoT devices will exceed 75 billion by 2025 [3], and reach 500 billion by 2030 [4].

Despite their potential, IoT devices typically have limited processing power and operate in diverse environments [5], making them vulnerable to unauthorized entry and cyber attacks [6]. An attacker who compromises a single weak device can jeopardize the security of an entire IoT system [7]. Therefore, it is essential to implement strong security measures to protect the privacy and data of IoT users and to secure their infrastructure and devices. Authentication systems are a primary defense to mitigate attacks on IoT systems [8], and numerous authentication schemes have been developed for IoT devices [9]. Among these, biometric authentication has become one of the most widely accepted methods [10]. Compared to traditional keys or passwords, biometric methods are more convenient and less burdensome for users. Moreover, modern wearable IoT devices can continuously collect physiological data from users, which can be leveraged for seamless and continuous authentication without explicit user interaction [9].

Currently, fingerprint and facial recognition are the predominant authentication techniques in consumer smart devices. However, integrating cameras or fingerprint sensors into small, low-power IoT devices is challenging due to resource and size constraints [11,12]. Furthermore, fingerprint and facial recognition require periodic reauthentication by users to maintain system security [13], which could disrupt the user experience. To overcome this drawback, one possible solution is passive authentication. This method gathers biometric information from portable devices that the user wears, allowing continuous authentication through data such as location and activity, without interruption [14]. Among passive authentication techniques, electrocardiogram (ECG) authentication emerges as a prominent candidate

* Corresponding author.
E-mail address: sysubonanzhang@gmail.com (B. Zhang).

https://doi.org/10.1016/j.comcom.2025.108201
Received 30 December 2024; Received in revised form 24 April 2025; Accepted 25 April 2025
Available online 10 May 2025

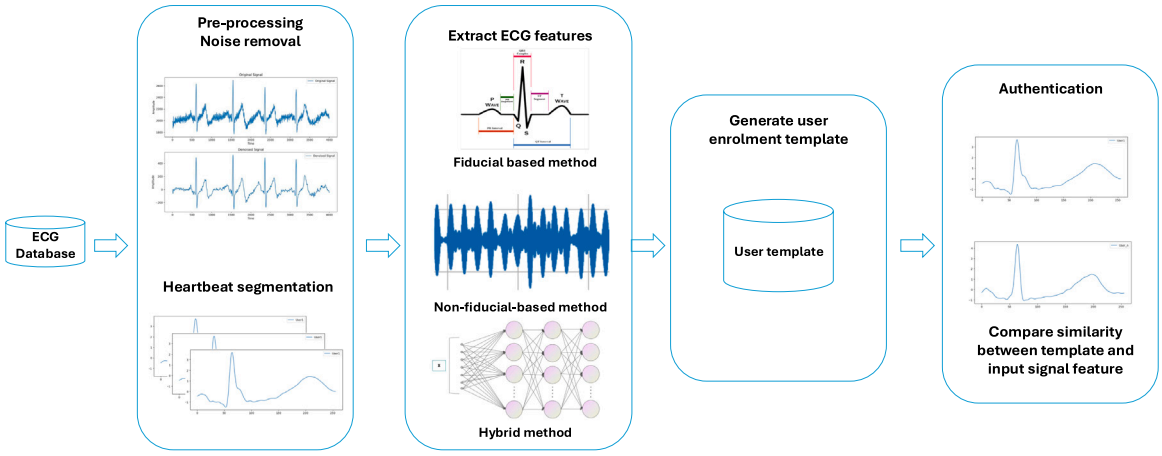


Fig. 1. Workflow of ECG based authentication.

from biosignals that portable devices can collect. This is attributed to the simplicity of the collection device, its validity testing, uniqueness, and resistance to replication [15].

A significant amount of research has already been devoted to ECG-based authentication, and many approaches have been proposed to extract distinctive ECG features and build reliable authentication models. In fact, extracting identifying features from ECG signals is relatively straightforward compared to some other biometrics, leading to a proliferation of ECG authentication methods in the literature [16,17]. However, there remain important gaps in how these methods are evaluated. ECG signals are influenced by many factors – including age, physical fitness, emotional state, and other time-dependent variations – that can alter the signal [18,19]. Despite this, most existing evaluation schemes use segments from the same recording session for both registration and testing, which means that the performance of an algorithm is often only validated on short-term data from the same session. Long-term performance between sessions of ECG authentication algorithms (e.g., verification of a user days or months after enrollment) is rarely considered. Moreover, the practicality of implementing these methods on IoT devices with limited resources has not been thoroughly examined.

To address these challenges, this research introduces a standardized evaluation framework and data set for ECG-based authentication on IoT devices. We develop a comprehensive ECG dataset tailored for long-term, cross-state evaluations, and propose a framework to assess ECG authentication systems under conditions reflective of IoT deployments. This work makes the following key contributions:

- Using currently available real-world ECG databases, we constructed a standardized ECG dataset to thoroughly assess how different authentication algorithms perform in a range of conditions and scenarios. This curated data set enables consistent and fair evaluations of algorithms in diverse time spans and user states.
- We introduce a detailed evaluation framework for ECG-based authentication on IoT devices, covering four critical dimensions of performance: scalability, adaptability, efficiency, and cancelability. This framework is designed to reflect the practical requirements and constraints of IoT applications, providing a standardized way to evaluate and compare authentication schemes for these devices.
- We replicated four representative ECG authentication algorithms from the literature and comprehensively evaluated their performance using our framework. The selected algorithms span both traditional feature-based and modern deep learning approaches. We analyze their performance under varying conditions and also examine how factors such as user age and gender impact the results, offering insights into each model's strengths and limitations in an IoT context.

The organization of the rest of this paper is as follows. Section 2 provides an overview of the development of ECG authentication algorithms in recent years. Section 3 details the performance metrics of the evaluation model that we have proposed. In Section 4, we describe our evaluation experiments in detail. Section 5 offers a comprehensive evaluation of the performance of current ECG authentication algorithms within this evaluation framework. In Section 6, we discuss potential mitigation measures. Finally, Section 7 concludes the paper and outlines the directions for future work.

2. ECG-based authentication for IoT device

ECG-based biometrics has been widely studied as a means of user authentication, and its adoption in IoT devices (wearables, smartwatches, health monitors) is promising. In order to realize ECG authentication, unique features of each individual need to be extracted from waveform signals to differentiate between different users. The process of using ECG signals for authentication is shown in Fig. 1. The authentication process is divided into four parts: preprocessing ECG signals, extracting signal features, generating registration templates, and authentication. Prior research on ECG-based authentication can be broadly categorized into fiducial, non-fiducial, and hybrid methods. This section reviews each category and highlights representative studies. We then discuss the common shortcomings of previous work that motivate the need for a standardized IoT-focused evaluation framework.

2.1. Fiducial-based ECG authentication

The ECG waveform in a heartbeat consists of five distinct waves. Atrial depolarization leads to the formation of the P wave, while ventricular depolarization is responsible for the QRS complex, and the cycle concludes with the T wave from ventricular repolarization. The initial step in fiducial-based processes involves accurately identifying the precise position of these waves. Subsequently, the features of the heartbeat are analyzed and extracted from these wave positions. These features may include the distances between waveforms, the angles and magnitudes of the waves, as well as their associated areas, among others. Furthermore, distinguishing between different users can also be accomplished through heart rate variability and beat patterns, such as the RR interval [17]. The advantage of this approach lies in the physical significance of its characteristics, making them accessible to those outside the medical field. However, it requires a precise localization

of the waveform points by the algorithm. Inaccuracies in positioning could severely compromise the accuracy of feature extraction.

Due to its simplicity and low computational requirements for IoT devices, many different authentication algorithms based on fiducial-based methods have been proposed. The method proposed by Juan et al. [20] is based on extracting the intervals between the waveforms and the amplitude differences between the R peak and the Q and S peaks to construct an authentication model. This model achieved a true acceptance rate of 84.93% and a false acceptance rate of 1.29% in a dataset from four different databases comprising 73 different users. The advantage of this method compared to others is that it requires only 4 s of ECG signal to complete the authentication. The scheme designed by Yang et al. [21] focuses on extracting the time interval between two consecutive R peaks as a feature to register each user. During the authentication phase, the authentication is achieved by comparing the similarity between the authentication template and the input signal. This scheme was successfully implemented on a Raspberry Pi and achieved an equal error rate (EER) of 8.67% in the PTBDB database.

2.2. Non-fiducial based method

The primary distinction between non-fiducial-based methods and the previous method is that the extraction of features does not require the localization of each waveform's position. This category of methods typically involves the conversion of time-domain signals into frequency-domain signals, using popular techniques like the Fourier transform [22] and wavelet decomposition [23]. Following this transformation, features such as spectral energy, averages, standard deviations, skewness, and kurtosis are extracted and used to create an authentication template. Moreover, wavelet decomposition coefficients can be utilized as authentication features in specific contexts. This category of features exhibits greater robustness compared to other approaches, as it is not significantly impacted by alterations in cardiovascular status. Moreover, they offer increased adaptability in implementation because they do not require exact fiducial positioning. Nonetheless, a requirement for high dimensional features to ensure accuracy may significantly elevate the intricacy of the authentication process [17].

Binish et al. [22] employ Fourier decomposition to decompose the ECG signal into Fourier intrinsic band functions. The energy distribution is extracted as a feature from these functions. In addition, features of different phases of the ECG signal are extracted through phase transformation. This method achieved an accuracy of more than 91.07% across three different databases. Huang [24] and their collaborators developed an ECG authentication method for IoT devices, employing singular value decomposition to separate essential and orthogonal components within ECG data. This method substantially reduces the impact of noise in the authentication process. In experiments using small data sets, this scheme achieved a F1 score of 97%.

2.3. Hybrid method

Hybrid approaches typically initiate the process by identifying fiducial points to partition the ECG into segments of equal length, aligned with the cardiac cycle. Subsequently, signal processing techniques are used to extract features from these segments individually. Convolutional neural networks (CNNs) are the most commonly employed method for feature extraction. Training a CNNs model for the user identification task enables the network to learn the extraction of ECG features for authentication. The benefit of these methods lies in the flexibility of their algorithm implementation, which typically requires merely identifying the most prominent R wave across all waveforms for data segmentation. However, these schemes generally have weak generalization capabilities, as existing schemes are trained and tested on single datasets. This can easily lead to overfitting of the model [25,26].

CNN algorithms have demonstrated exceptional performance in the field of authentication recognition, leading to the proposal of numerous ECG-based authentication schemes for IoT devices. In [25], Eduardo and others proposed an authentication scheme specifically for off-person collected ECG signals. This scheme utilizes two CNN models to extract authentication features from both the raw ECG signals and their spectrograms. The scheme achieved EER of 1.33% and 14.27% in two off-person collected ECG databases, CYBHI and UofTDB, respectively. The method proposed by Labati et al. [27] employs CNN models to derive features from ECG signals, utilizing the Hamming distance in the authentication phase to assess the similarity between features of the input signal and the stored template. This system achieved a 100% authentication accuracy rate in the PTB Diagnostic database.

2.4. Limitations of prior work

Despite progress in ECG-based authentication, previous approaches have notable limitations when viewed from an IoT deployment perspective. Key limitations of existing work include:

- Same-Session Bias: Many studies evaluated their methods on data from a single recording session or sessions collected back-to-back. This means the authentication models were not rigorously tested on ECG data recorded hours, days, or weeks apart. In reality, ECG characteristics can drift over time due to changes in electrode positioning, heart rate, stress levels, or other physiological factors [28]. Robust IoT authentication requires algorithms to maintain performance over long periods and varied conditions.
- Limited Adaptability: Few works have explored how ECG authentication systems adapt to temporal changes or user state fluctuations. Most systems assume a static enrollment template or model that does not update unless the user re-enrolls. In practice, an individual's ECG may evolve due to factors like aging, medication, or increased physical fitness, potentially reducing the matching score against an old template. An effective IoT authentication framework should test adaptability.
- Computational Constraints Ignored: Most ECG authentication algorithms developed in research primarily focus on maximizing accuracy, with little consideration given to device resource limitations in practical applications. While this may be acceptable in offline experiments or smartphone applications, deploying such algorithms on IoT devices can be challenging.

In summary, previous research has demonstrated that ECG-based authentication is feasible and can achieve high accuracy under certain conditions. However, the lack of standardized, rigorous testing in prior work leaves uncertainty about real-world readiness. These limitations have inspired our work to design a standardized comprehensive assessment framework suitable for IoT environments. Such a framework should enable objective comparisons of algorithms on a common basis and ensure that performance claims are valid in real-world usage scenarios.

3. Performance evaluation framework

To systematically assess ECG-based authentication for IoT devices, we define an evaluation framework with four key criteria: scalability, adaptability, efficiency, and cancelability. Traditional performance metrics such as the true acceptance rate (TAR), false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER) are useful for measuring accuracy on a given dataset. However, these metrics alone do not capture the practical challenges of deploying authentication algorithms on real IoT devices. In this study, we propose the following evaluation criteria for ECG authentication on IoT devices.

3.1. Scalability

It refers to the system's ability to accommodate an increasing number of authentication users without the need to retrain the model. In the IoT ecosystem, the number of users and devices typically increases over time. When new users join the system, retraining the authentication model locally is often impractical due to the limited computational resources of IoT devices. However, uploading user ECG data to a server for centralized training introduces significant privacy risks.

Several prevalent authentication algorithms achieve implementation by converting the authentication task into a user classification problem [22,29]. These algorithms are developed and evaluated on closed datasets using machine learning techniques. When there is a requirement to incorporate a new user into the system, it necessitates complete retraining of the model. This process is unsuitable for scenarios involving the utilization of IoT devices.

The evaluation of scalability is divided into two aspects: first, whether the authentication model can add new authentication users without retraining. Second, whether the authentication performance is significantly affected as the number of users in the system increases.

3.2. Adaptability

Adaptability refers to the performance of the authentication system under various real-world conditions. Evaluations of authentication performance traditionally concentrate on a singular ECG recording session, potentially limiting their applicability to real-world situations. In practical use cases, authentication frequently occurs across different sessions, times, and states. The duration between user registration and verification can vary, spanning from a single day to multiple months or even longer. Moreover, it cannot be presumed that a user's physical state during the authentication attempt is identical to that during registration. To thoroughly evaluate the adaptability of an authentication algorithm, its performance is analyzed from two primary perspectives.

- Cross-Time Authentication Performance: This aspect evaluates the robustness of the algorithm over time. In particular, the algorithm is evaluated using ECG signals that are collected at different time intervals, including one week, one month, three months, and six months, after initial registration. This process helps to assess the model's ability to manage temporal variations in ECG signals and maintain consistent authentication performance over extended periods.
- Cross-State Authentication Performance: This aspect investigates the algorithm's capability to manage variations in the users' physical states. Templates were developed from ECG signals obtained while users were calm and seated. Validation tests are then performed using signals recorded in more dynamic states such as standing or physical activity. This allows us to test whether the algorithm is able to adapt to physiological changes caused by different postures or activity levels.

3.3. Efficiency

This metric primarily evaluates the deployability of the authentication model on IoT devices. IoT devices are often constrained by limited computational resources and insufficient power supply, so it is crucial to evaluate the model's performance in these environments. The primary dimensions for evaluation encompass memory utilization, energy expenditure, execution duration, and computational overhead necessary for operating the model.

In particular, for deep neural network models that are computationally demanding, like CNNs, the algorithm's computational efficiency is quantified by FLOPs (Floating Point Operations). FLOPs reflect the total amount of computations required during one inference process, including the count of all multiplication and addition operations. FLOPs serve as a crucial metric for evaluating the computational complexity of a model because they clearly indicate the computational demands on devices during model execution. In the CNN model, the formulas employed to determine the anticipated FLOPs for each layer are presented below:

$$C\_FLOPs = 2 \times I \times F \times K \times O. \tag{1}$$

$$P\_FLOPs = C \times F \times K. \tag{2}$$

$$F\_FLOPs = 2 \times F \times O. \tag{3}$$

C_FLOPs, P_FLOPs, F_FLOPs represent the computation of FLOPs for convolutional, pooling and fully connected layers, respectively. Here, I represents the count of input channels, F indicates the total output features, K denotes the kernel size, and O signifies the number of output channels.

3.4. Cancelability

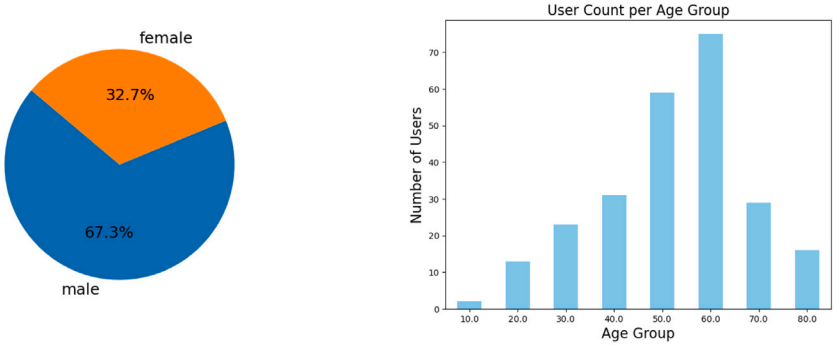
It refers to the ability of users to replace their biometric authentication templates when necessary. Biometric templates are generally stable, which is crucial for maintaining authentication effectiveness. Nonetheless, the compromise or theft of a template can present a significant risk to the security of the system. For IoT devices, template theft may be caused by malware on the device, physical theft, or interception during data transmission. Using a stolen template, an attacker can impersonate and pass through the user's authentication system. Furthermore, the attacker might infer the user's actual signal information, compromising the security of the user's biometric authentication method.

To address these scenarios, cancelability mechanisms should include non-invertible transformations applied to the biometric template during enrollment—ensuring that even if the transformed template is exposed, the original biometric cannot be recovered. One common strategy is to apply a keyed transformation, allowing the template to be reissued by simply changing the transformation key [30]. In this way, multiple unlinkable templates can be generated from the same underlying ECG data without retraining the model. This ensures continued security and usability of the authentication system. Two key evaluation criteria for such systems are Cancelability and unlinkability.

- Cancelability ensures that the system allows users to update their authentication templates without compromising the effectiveness of the authentication process. An ideal system should enable the generation of multiple new templates, each independently valid.
- Unlinkability ensures that there is no significant traceable relationship between the old and new templates. This prevents attackers from deducing the new template based on the old one, thereby reducing potential security risks. Unlinkability is critical for defending against correlation-based attacks. It is typically quantified using the Pearson Correlation Coefficient between the original and updated templates. A lower correlation indicates weaker linkability and stronger security.

4. Experiment setup

The main aim of our study is to thoroughly assess the efficacy of different ECG authentication approaches when implemented in IoT devices. This section outlines the details of the creation of the standardized evaluation database and the ECG authentication algorithm used in the evaluation. The experiment will focus on methods and procedures to analyze the scalability, adaptability, and overall performance of an ECG-based authentication system within an IoT context.



(a) Gender distribution (b) Age group distribution

Fig. 2. Distribution of the dataset in different dimensions.

Table 1
Distribution of subjects in the PTBDB database.

	Time interval				
	Train&Eval	One week	One month	Three months	Six months
subjects	225	27	15	15	13

Table 2
Distribution of subjects in the UofTDB database.

Weeks	Condition				
	sit	stand	exercise	supine	tripod
0	1012	0	0	0	0
1	72	72	0	0	0
2	76	5	71	0	0
3	63	0	0	0	0
4	0	0	0	63	63
5	65	65	0	0	0

4.1. Datasets setup

In this experiment, we construct a standardized database specifically curated to evaluate the efficacy of ECG authentication techniques on IoT devices. This standardized approach involves the use of two distinct datasets: the PTB Diagnostic Database (PTBDB) [31] and the University of Toronto ECG Database (UofTDB) [32]. These data sets are chosen for their diverse and comprehensive collections of ECG recordings, which are crucial to testing the adaptability and robustness of various authentication algorithms in different demographic groups and temporal scales.

4.1.1. PTB diagnostic database

The PTB Diagnostic Database (PTBDB) is widely used to evaluate the reliability of various ECG authentication approaches. The database includes 549 records from 290 participants, with each ECG recording approximately 2 min in duration. In particular, the longest interval between recordings in this data set extends up to four years, providing a robust framework for the analysis of long-term variability in ECG data.

For this experiment, we chose time intervals of one week, one month, three months, and six months to evaluate the performance of the algorithm in cross-time scenarios. If a subject had measurements within ±20% of the designated time intervals, their data was included in the evaluation. Subsequently, we excluded these subjects' data from the overall dataset, using the remaining data for training and performance evaluation. The distribution of subjects included in the analysis is summarized in Table 1

In addition, in this experiment, we seek to investigate whether there are significant performance differences in ECG authentication between various age and gender groups. After excluding users with long time gaps in their recordings, the age and sex distribution of the remaining data set is illustrated in Fig. 2.

4.1.2. University of Toronto ECG database

The University of Toronto ECG Database is currently the largest off-person collection database. This database contains a total of 1020 subjects. Unlike the collection methods used in medical scenarios, this method is implemented by placing electrodes on the user's thumb. Data collection spanned six months, with each signal lasting between 2 and 5 min.

Our decision to utilize this data set is based on three key factors. Firstly, it includes a substantial variety of ECG signals from a broad demographic, spanning ages 18 to 52. Secondly, the extensive data collection period of six months provides longitudinal data in several time intervals, offering a deeper understanding of temporal variations in ECG patterns. Lastly, beyond the capture of data in a seated state, the data set comprehensively records ECG signals in four additional postures, allowing us to assess the robustness of authentication algorithms in various physical states of users.

In this database, while 1020 subjects contributed to the collection of ECG data, not all were involved in all the states and sessions of the testing process. The distribution of participation is detailed in Table 2, where the first session saw the highest level of participation, involving 1012 users. This subset of data was specifically used to assess the efficacy of various ECG authentication algorithms across data sets. Additionally, to evaluate the performance of these algorithms under different physical conditions, we included data capturing both seated and various other postures.

4.2. Authentication model

In this research, we replicated and evaluated four authentication algorithms based on ECG data, chosen due to their high citation rates and their representation of state-of-the-art technology. During the reproduction phase of the authentication algorithm, we adhered as closely as possible to the methodologies and data processing procedures described in the original publications. Based on the particular requirements of each algorithm, we carried out resampling, normalization, and rescaling of the signals. In this paper, we reproduce the following authentication algorithms.

ECG Mobile [20] is a fiducial-based ECG authentication system. It works by extracting the positions of various waves in the ECG signal. The positional relationship between these waves and their peak amplitudes is then calculated as features. In the registration phase, the system records the mean values of these features to create a registration template. To perform authentication, the system evaluates the input signal against the stored template by determining their similarity to confirm if the current user matches the registered one.

Table 3
Performance of different ECG authentication model.

Authentication model	Type	Subjects	Feature	Performance (ACC)
ECG Mobile	Fiducial based	73	P, Q, R, S, T wave location	81.82%
EDITH	Hybrid	290	Embedding feature	99.70%
ECGIoT	Hybrid	290	Embedding feature	99.16%
CancelableECG	Non-Fiducial based	290	Features extracted by the VGG-16 model	99.56%

Table 4
Scalability evaluation under different numbers of users. Best TAR and best FAR highlighted.

Authentication model	10%		30%		50%		70%		100%	
	TAR	FAR	TAR	FAR	TAR	FAR	TAR	FAR	TAR	FAR
ECG Mobile	80.07%	1.62%	85.15%	2.81%	85.99%	3.70%	84.96%	3.35%	87.43%	4.08%
EDITH	**100%**	2.48%	**98.19%**	3.73%	**98.81%**	4.53%	**99.30%**	4.03%	**99.41%**	3.82%
ECGIoT	97.85%	2.55%	96.99%	3.37%	97.43%	3.16%	97.48%	3.04%	96.37%	2.95%
CancelableECG	90.92%	**0.21%**	87.44%	**0.10%**	86.90%	**0.06%**	84.05%	**0.03%**	84.45%	**0.02%**

EDITH [26] is an ECG authentication algorithm that employs CNNs in its framework. The system comprises two primary components. The initial component uses a CNN to obtain features from pre-segmented ECG fragments. Following this, a Siamese network assesses the similarity between the input signal and the stored template, to decide if the authentication is valid.

ECGIoT [33] is a specific ECG authentication solution designed for IoT devices, employing a CNN-based methodology. Unlike traditional methods that focus on the extraction of characteristics from individual heartbeat cycles, this scheme amalgamates signals from ten consecutive heartbeat cycles to enhance the extraction of features. To accommodate the limited resources of IoT devices, the scheme incorporates optimized pruning and quantization techniques, ensuring efficient operation within these constrained environments.

CancelableECG [30] is a cancelable authentication template for ECG verification. The method initially utilizes a pre-trained VGG-16 model to extract features from each cardiac cycle. Subsequently, it employs the Blum–Blum–Shub generator to create a cancelable key for each user [34], and generates a new template through inner product computations. Finally, the algorithm uses an SVM model to classify the legitimacy of user access.

Table 3 shows a comparison between the four algorithms that we reproduced. The reproduced code can be accessed via this link.[1]

5. Experiment result

In this section, we will conduct a comprehensive evaluation of four commonly used ECG algorithms to determine if they meet the requirements for use on IoT devices. In this study, the replicated algorithms were implemented using Pytorch on a computer system equipped with a 16-core AMD Ryzen 7950X CPU, 64 GB of RAM and an NVIDIA RTX 4080 GPU with 16 GB of memory. Our evaluation will primarily focus on Scalability, adaptability, efficiency and cancelability.

5.1. Scalability evaluation

In this experiment, we evaluated the scalability of four ECG-based authentication algorithms. All algorithms function by extracting features from ECG signals and storing the features of the registration signal as a template. During authentication, the device compares the features of the input signal with the stored template to determine whether authentication is successful. This design ensures that all algorithms satisfy the scalability criterion of supporting the addition of new users without requiring retraining of the model.

To assess whether the number of users affects system performance, we tested the algorithms at varying levels of user participation, specifically at 10%, 30%, 50%, 70%, and 100% of the total user population. For user proportions smaller than 100%, we randomly selected the corresponding percentage of users for each test. Each experiment was repeated 10 times and the results were averaged to minimize the impact of random selection on performance evaluation.

The evaluation metrics used for this scalability test were as follows:

- TAR: The proportion of legitimate authentication attempts that are correctly accepted.
- FAR: The proportion of fraudulent authentication attempts that are incorrectly accepted.

For all models, except ECG Mobile, thresholds were established according to the EER to ensure consistency in the evaluation. The results of scalability performance for the four models are summarized in Table 4.

Table 4 shows that all models exhibit strong scalability, effectively managing user groups of various sizes. Before analyzing the specific performance, it is important to clarify that for the CancelableECG algorithm, each time a new user is added to the system, the authentication model needs to be retrained. In contrast, other algorithms can add new users to the system without retraining the model. For the CancelableECG algorithm, the necessity to retrain the model with each addition of a user keeps the FAR consistently low. However, the TAR gradually decreases as the number of users increases. For other three algorithms, as the number of users grows, there is a minor rise in the FAR for models, yet the rates remain consistently low. All models demonstrate robust security performance. Among the models, EDITH stands out if a high TAR is prioritized, as it consistently delivers near-perfect results regardless of the user proportion. ECGIoT offers a balanced choice, effectively maintaining a low FAR while achieving high TAR. Meanwhile, ECG Mobile slowly improves in TAR as it accommodates a wider range of users, although it is crucial to monitor the increase in FAR that comes with this expansion. If the number of users in the system does not increase, using the Cancelable ECG algorithm can ensure an extremely low probability of identity spoofing.

In summary, apart from the CancelableECG algorithm, the other three algorithms offer scalability, allowing new users to be added without retraining. However, their performance varies significantly with changes in the size of the user group. The CancelableECG algorithm, on the other hand, can provide more reliable security. Users can choose the appropriate authentication algorithm based on their specific needs.

5.2. Adaptability evaluation

To evaluate the adaptability of algorithms, we will perform a thorough analysis of their performance in real world situations, considering multiple dimensions: temporal variability (cross-time performance), physical conditions (cross-state performance), gender differences and variations associated with age.

[1] https://github.com/Wise-Horo/Standardizing-the-Evaluation-Framework-for-ECG-Based-Authentication-in-IoT-Devices

Table 5
Cross-time performance of different authentication systems. Best TAR and FAR for each time period are highlighted in bold.

Authentication model	Train & Eval		7 Days		30 Days		90 Days		180 Days	
	TAR	FAR	TAR	FAR	TAR	FAR	TAR	FAR	TAR	FAR
ECG Mobile	87.43%	4.08%	33.56%	3.36%	23.71%	3.12%	18.06%	2.17%	22.23%	4.22%
EDITH	**99.41%**	3.82%	15.41%	12.46%	30.44%	28.72%	0%	0%	7.07%	7.07%
ECGIoT	96.37%	2.95%	53.27%	3.52%	44.51%	2.30%	23.49%	5.90%	**28.26%**	**2.33%**
CancelableECG	90.92%	**0.21%**	**53.47%**	**1.82%**	**66.36%**	**1.88%**	**44.59%**	**4.03%**	17.33%	7.36%

5.2.1. Cross-time performance

In contrast to static biometric characteristics such as fingerprints or facial features, human ECG data are dynamic and can vary over time. This intrinsic variability presents a considerable challenge in maintaining reliable identity authentication for long periods. In order to assess the long-term efficacy of ECG-based authentication, experiments were conducted using ECG signals obtained at various time intervals. These experimental results are presented in Table 5.

From the experimental results, it is evident that the authentication performance of all four algorithms tested deteriorates significantly over time.

- ECG Mobile Algorithm: The ECG Mobile algorithm also experiences a decline in TAR as the time interval increases. However, unlike EDITH, its FAR remains stable across all time intervals.
- EDITH Algorithm: Among the three algorithms, EDITH exhibits the most pronounced decline in performance. Authentication with ECG signals recorded just one week after registration becomes completely ineffective. This severe drop in performance is likely due to the algorithm's reliance on a CNN-based similarity evaluation method, which is prone to overfitting.
- ECGIoT Algorithm: In terms of long-term stability, the ECGIoT algorithm has better stability. Although its TAR gradually decreases over time, the rate of decline is slower compared to the other algorithms. Furthermore, ECGIoT maintains a relatively low FAR throughout the evaluation period.
- CancelableECG Algorithm: Among all the algorithms, the Cancelable ECG algorithm demonstrates the best long-term performance. When the time interval is less than 90 days, this algorithm shows the best TAR and FAR performance among the four algorithms. Similar to other algorithms, the performance of this algorithm experiences a significant decline when dealing with data that has time intervals. However, it maintains similar performance levels within the period of 7 to 90 days. A second significant decline in performance occurs after the time interval reaches 180 days.

These findings underscore the essential need to consider temporal variability in ECG-based authentication systems. Designing algorithms capable of adapting to the dynamic characteristics of ECG signals is vital for ensuring consistent and reliable authentication in real-world applications over the long term.

5.2.2. Cross-state performance

It has been established in prior research that ECG waveforms can exhibit substantial changes during physical activity, driven primarily by fluctuations in heart rate and respiratory patterns [35]. Given that users may not consistently remain inactive during authentication, evaluating the algorithm's performance reliability under active conditions becomes a crucial part of its assessment. To assess the performance of the four algorithms under different physiological conditions, this section of our experiment used ECG signals obtained from the UofTDB database. We develop user authentication templates based on ECG recordings collected while subjects were seated. For testing, we used ECG signals recorded from subjects in standing and exercise conditions. In order to reduce performance disparities that could result from time intervals, the registration and testing signals for each user were obtained from the identical session, maintaining consistency in the experimental conditions.

Table 6
Cross-state performance of different authentication systems. Bold values indicate the best TAR and best FAR under each condition.

Authentication model	Sit		Stand		Exercise	
	TAR	FAR	TAR	FAR	TAR	FAR
ECG Mobile	77.81%	8.02%	38.69%	6.48%	18.37%	4.14%
EDITH	**99.89%**	82.24%	**81.74%**	79.78%	**73.44%**	76.39%
ECGIoT	92.45%	17.77%	80.84%	20.70%	54.00%	18.90%
CancelableECG	49.21%	**0.57%**	32.01%	**0.89%**	13.09%	**1.22%**

Table 6 demonstrates the performance differences among the four ECG authentication algorithms when evaluated with data sets gathered from different devices and conditions. The effectiveness of the EDITH algorithm significantly decreases, probably due to its CNN modules being exclusively trained on one dataset, which renders them prone to overfitting and reduces their efficacy when applied to varied datasets. This results in extremely high FAR across different states. ECG Mobile also exhibits a slight increase in FAR, but with relatively minor overall fluctuations. Although its performance in a seated condition aligns closely with that seen in the PTBDB dataset, there is a significant drop in the TAR when the user's condition changes. The ECGIoT algorithm similarly exhibits increased FAR in all tested states, yet maintains better robustness than the EDITH algorithm, suggesting some resilience despite the observed challenges. The accuracy of the Cancelable ECG algorithm also deteriorates due to changes in the user's activity status. Its TAR performance is the worst among all algorithms. However, it is worth noting that it has the lowest FAR performance of all the algorithms.

The results of the experiments clearly indicate that all four ECG authentication algorithms struggle to maintain consistent performance when faced with the challenge of cross-state authentication. We believe there are three main reasons for the significant performance decline. First, there is a difference in signal quality. The PTBDB dataset signals were collected using medical-grade devices, whereas the UofTDB dataset signals were gathered through wearable devices, making them more susceptible to motion artifacts and noise [36]. The second reason is that during physical activity, the position of the electrodes on the user's body constantly changes, which can significantly degrade signal. Lastly, previous research has demonstrated that changes in a user's activity state can lead to dramatic variations in their ECG signals [37]. These three factors contribute to the poor performance of the authentication system in cross-state scenarios. However, in practical usage scenarios, these issues are difficult to avoid. This indicates a requirement for further improvements to enhance their adaptability to various physical conditions of users.

5.2.3. Cross-gender performance

In line with previous research that indicates significant variations in ECG patterns due to differences in age and sex [38]. This section aims to assess how these variations influence the effectiveness of ECG authentication algorithms. In this study, each user is considered an autonomous unit, allowing us to measure performance differences individually. Following this, statistical analyzes are performed according to their respective groups.

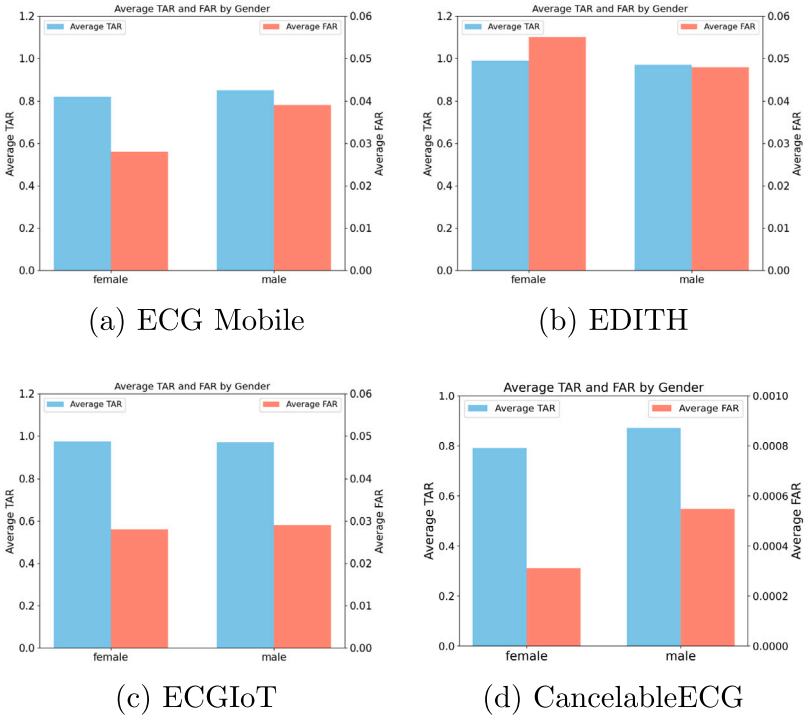


Fig. 3. Performance Differences of Authentication Algorithms by Gender.

Table 7
Cross-gender t-test results for the four models. Bold values indicate statistically significant results ($p < 0.05$).

Authentication model	ECG Mobile	EDITH	ECGIoT	CancelableECG
TAR (p-value)	0.233	0.087	0.755	0.0846
FAR (p-value)	**0.0430**	0.605	0.898	0.447

Table 8
Cross-age t-test results for the four models. Numbers indicate p-values.

Authentication model	ECG Mobile	EDITH	ECGIoT	CancelableECG
TAR (p-value)	0.079	0.294	0.642	**0.004**
FAR (p-value)	**0.005**	**0.002**	**0.003**	0.835

Fig. 3 illustrates that the FAR metric of the ECG Mobile algorithm shows a significant discrepancy between male and female users. In comparison, the performance of other algorithms remains consistent across gender groups. To examine these differences more thoroughly, we performed a t-test to determine whether the performance variations between gender are statistically significant. Detailed outcomes of this analysis are presented in Table 7. The analysis indicates that only the FAR metric in the ECG Mobile algorithm exhibits a statistically significant gender dependence, with a p-value less than 0.05, while all other algorithms displayed no significant gender differences.

5.2.4. Cross-age performance

Medical studies have shown that the characteristics of ECG signals change with age, particularly after age 50. These changes include a flattening of the signal amplitude and a reduction or disappearance of the trends of interval variation [39]. To assess how these age-related differences affect the performance of ECG authentication, we categorized users into 10-year age brackets and examined the performance discrepancies between these groups. Furthermore, for statistical analysis purposes, we split the age groups into two segments: those younger than 50 years and those 50 years and older. The results of these evaluations are presented in Fig. 4 and Table 8.

Fig. 4 reveals substantial differences in authentication performance across different age groups. Specifically, the EDITH and ECGIoT algorithms tend to have uniform TAR performance across various age groups, but their FAR performance gradually increases with age. The ECGmobile algorithm shows the opposite trend, exhibiting lower FAR as age increases. The CancelableECG algorithm's TAR decreases gradually with age, and its FAR also progressively increases.

After conducting T-tests on different age groups at Table 8, the same conclusion was reached: the p-values for the FAR of ECG Mobile, EDITH, and ECGIoT algorithms across various age groups are all less than 0.05, demonstrating a significant correlation between age and FAR performance. For CancelableECG, the TAR significantly varies with age. FAR does not vary significantly. This confirms that age has a substantial influence on authentication performance. To address this, algorithms should consider performance gaps between age groups and implement appropriate optimizations to enhance their robustness.

5.3. Efficiency evaluation

Evaluating the efficiency of an algorithm is a crucial aspect in determining its suitability for deployment on resource-constrained IoT devices. In this study, we evaluate the efficiency of the algorithms from three main aspects: the complexity of the algorithm, the time required to complete an identity verification attempt, and the memory usage. The measurement approach involves running the model for 1000 authentication attempts and then averaging the time consumed and the computation consumed per attempt to ensure robust and consistent measurements. The results of these experiments are summarized in Table 9.

The table shows that among all the algorithms, the ECG Mobile algorithm is the most efficient in terms of memory usage and complexity, making it most suitable for deployment on lightweight IoT devices. Similarly, the EDITH and ECGIoT algorithms offer a good balance of high computational efficiency and moderate memory usage, making them suitable for IoT devices or environments with limited resources. Of all the algorithms, the CancelableECG algorithm requires the most memory and computational power for deployment. Although

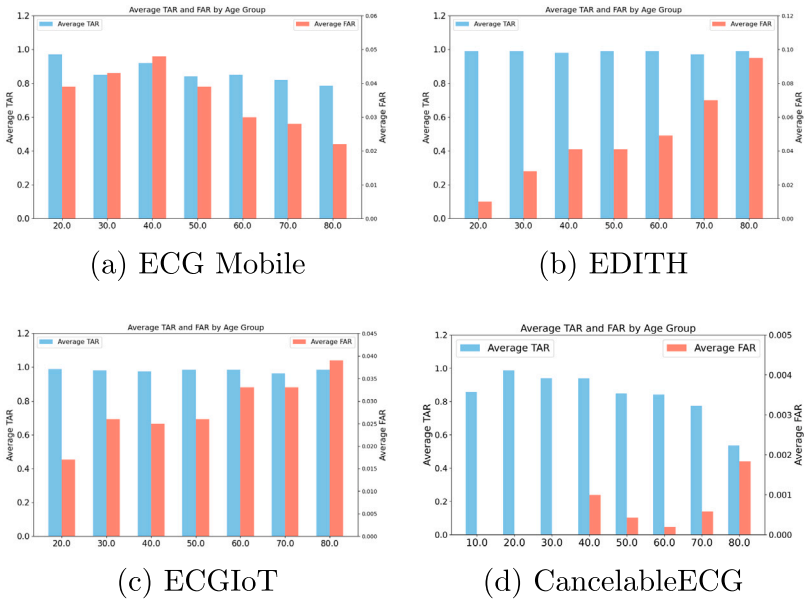


Fig. 4. Performance Differences of Authentication Algorithms by Age.

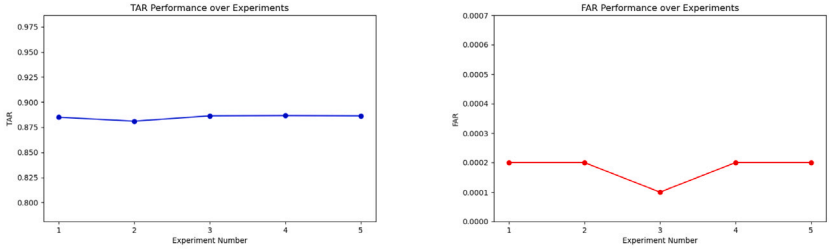


Fig. 5. Performance Differences of Authentication Algorithms by different templates.

Table 9
Efficiency evaluation of different authentication algorithms.

Authentication model	ECG Mobile	EDITH	ECGIoT	CancelableECG
Algorithm Complexity	$O(n)$	0.002 GFLOPs	0.018 GFLOPs	30.960 GFLOPs
Time Consumption	0.024 s	0.024's	0.026 s	0.035 s
Memory Usage	20.8 MB	194.30 MB	112.65 MB	527.74 MB

it uses the lightweight VGG-16 pre-trained model to extract features, its memory and computational demands still far exceed the typical design specifications of general IoT devices.

5.4. Cancelability evaluation

Among the four algorithms that we replicated, only the CancelableECG algorithm is capable of replacing the stolen template of a user. Therefore, in this section, we will primarily assess the cancelability feature of this algorithm. We will evaluate the algorithm by examining the performance changes after template replacement and the similarity between the new and old templates.

The Cancelable ECG algorithm uses the Blum-Blum-Shub generator to create cancelable keys for users. We generated a total of five different sets of keys for experimentation to test whether the authentication algorithm exhibits significant performance differences under various templates.

Fig. 5 shows the performance of the algorithm under different templates. It is evident that the algorithm achieves similar performance across various templates, without any performance degradation due to template changes. The reason why the algorithm maintains consistent performance is that it requires retraining of the authentication model each time the template is changed, ensuring consistency of performance.

In addition to assessing changes in authentication performance under different templates, we also evaluated the possibility that an attacker could infer a new template from a stolen one. Similarly, we generated five different templates and compared the cosine similarity and Pearson similarity between these five templates and the base template. The results in Table 10 show that the correlation between different templates generated by the algorithm and the base template is extremely low, all very close to 0. It is difficult for an attacker to infer the features of the new template used by the user from the old template. These two experimental results demonstrate that the CancelableECG algorithm has excellent cancelability. It can generate a new user template that is completely imponderable to attackers while maintaining essentially unchanged performance. This is highly effective in protecting user security.

Table 10
Similarity between different templates.

	Template 1	Template 2	Template 3	Template 4	Template 5
Cosine Similarity	0.0276	0.0562	0.0250	−0.0405	−0.0167
Pearson Similarity	0.0273	0.0559	0.0249	−0.0398	−0.0167

Table 11
Comparison of ECG authentication algorithms.

Authentication model	Type	Scalability	Adaptability	Efficiency	Cancelability
ECG Mobile	Fiducial based	●	○	●	○
EDITH	Hybrid	●	○	◐	○
ECGIoT	Hybrid	●	◐	◐	○
CancelableECG	Non-Fiducial based	○	◐	○	●

● = offers benefit, ◐ = partially offers benefit, ○ = does not offer benefit.

5.5. Comparative summary

To facilitate the selection and comparison of ECG authentication algorithms, Table 11 summarizes the four representative methods in key dimensions of our evaluation framework. These include their adaptability to signal variations, scalability to new users, computational efficiency, and template cancelability.

As shown in Table 11, most current ECG authentication schemes are capable of supporting user scalability without significantly compromising authentication performance. In addition, when deployed on resource-constrained IoT devices, these methods demonstrate effective control over resource consumption. However, it should be noted that most existing algorithms struggle to maintain stable performance across different time periods and physiological states. Furthermore, most authentication schemes do not incorporate cancelable biometric templates as a fundamental function of their implementations. Addressing these limitations should be a key consideration in the future development of ECG authentication algorithms.

6. Discussion

In this study, we found that existing ECG authentication schemes often perform poorly in cross-session authentication. To address the limitations, we think that several mitigation strategies can be employed. A possible solution is to consider these long-term variations during model training, using signals that reflect long-term changes in ECG patterns, allowing the model to learn the regularities of the ECG variations over time. Reliability in long-term authentication scenarios can be achieved by allowing the authentication system to periodically collect and update user templates. This strategy can significantly reduce the impact of temporal variability by ensuring the stored biometric templates closely reflect the user's current ECG characteristics [28,40].

Furthermore, authentication algorithms can be trained using ECG datasets collected under various conditions, and templates can be generated using signals from different activity states of users to enhance the model's robustness to changes in physical conditions. Incorporating adaptive thresholding techniques can further optimize authentication decisions dynamically, adjusting acceptance criteria based on real-time contextual cues, such as heart rate or detected user activities.

When appropriate training datasets are lacking, one potential solution is to enrich the registration dataset by simulating variations such as noise, heart rate changes, and other factors. This approach can help the model learn a broader range of ECG patterns, thereby reducing its sensitivity to changes caused by physical activity or emotional fluctuations [41].

7. Conclusion

The use of ECG signals for biometric authentication has become a prominent focus in the security research of IoT devices. Numerous studies have validated the feasibility of equipping IoT devices with ECG collection capabilities and authentication mechanisms. However, existing evaluation frameworks largely emphasize the authentication performance of algorithms, often neglecting their practical deployment on IoT devices. In this paper, we introduce a novel evaluation framework tailored to ECG authentication schemes for IoT devices, categorizing performance metrics into four key dimensions: scalability, adaptability, efficiency, and Cancelability. To enable a comprehensive performance evaluation, we also constructed a standard evaluation database to analyze algorithm performance. This study presents a detailed assessment of four typical ECG authentication models, identifying significant adaptation issues, particularly concerning cross-state and cross-time authentication effectiveness. We believe that this evaluation framework can inform future IoT ECG authentication research, promoting the development of more resilient and secure authentication systems.

CRediT authorship contribution statement

Bonan Zhang: Writing – original draft, Methodology, Formal analysis. **Lin Li:** Writing – review & editing. **Chao Chen:** Writing – review & editing, Supervision. **Ickjai Lee:** Writing – review & editing, Supervision. **Kyungmi Lee:** Writing – review & editing, Supervision. **Kok-Leong Ong:** Writing – review & editing, Supervision.

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

The dataset used in this paper is a public dataset and can be freely downloaded by the researcher.

References

[1] S. Mathur, A. Kalla, G. Gür, M.K. Bohra, M. Liyanage, A survey on role of blockchain for iot: Applications and technical aspects, Comput. Netw. 227 (2023) 109726.
[2] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, M. Iranmanesh, The Internet of Things (IoT) in healthcare: Taking stock and moving forward, Internet Things 22 (2023) 100721.
[3] H.F. Atlam, G.B. Wills, Technical aspects of blockchain and IoT, in: Advances in Computers, vol. 115, Elsevier, 2019, pp. 1–39.
[4] E. Carey, I. Mc Donnell, Overview: Powering an inclusive digital future, 2021.
[5] M. Zhang, X. Shen, J. Cao, Z. Cui, S. Jiang, Edgeshard: Efficient llm inference via collaborative edge computing, IEEE Internet Things J. (2024).
[6] J. Deogirikar, A. Vidhate, Security attacks in IoT: A survey, in: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC, IEEE, 2017, pp. 32–37.

[7] L. Babun, K. Denney, Z.B. Celik, P. McDaniel, A.S. Uluagac, A survey on IoT platforms: Communication, security, and privacy perspectives, Comput. Netw. 192 (2021) 108040.
[8] P.M. Rao, B.D. Deebak, A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions, Ad Hoc Netw. 146 (2023) 103159.
[9] C.-W. Lien, S. Vhaduri, Challenges and opportunities of biometric user authentication in the age of iot: A survey, ACM Comput. Surv. 56 (1) (2023) 1–37.
[10] A.I. Awad, A. Babu, E. Barka, K. Shuaib, AI-powered biometrics for Internet of Things security: A review and future vision, J. Inf. Secur. Appl. 82 (2024) 103748.
[11] S. Vhaduri, C. Poellabauer, Multi-modal biometric-based implicit authentication of wearable device users, IEEE Trans. Inf. Forensics Secur. 14 (12) (2019) 3116–3125.
[12] P. Liu, Q. He, Y. Chen, S. Jiang, B. Zhao, X. Wang, A lightweight authentication and privacy-preserving aggregation for blockchain-enabled federated learning in VANETs, IEEE Trans. Consum. Electron. (2024).
[13] M. Cardaioli, M. Conti, G. Orazi, P.P. Tricomi, G. Tsudik, BLUFADER: Blurred face detection & recognition for privacy-friendly continuous authentication, Pervasive Mob. Comput. 92 (2023) 101801.
[14] G. Stragapede, R. Vera-Rodriguez, R. Tolosana, A. Morales, A. Acien, G. Le Lan, Mobile behavioral biometrics for passive authentication, Pattern Recognit. Lett. 157 (2022) 35–41.
[15] D.R. Bhuva, S. Kumar, A novel continuous authentication method using biometrics for IOT devices, Internet Things 24 (2023) 100927.
[16] S. Asadianfam, M.J. Talebi, E. Nikougoftar, ECG-based authentication systems: a comprehensive and systematic review, Multimedia Tools Appl. 83 (9) (2024) 27647–27701.
[17] A.S. Rathore, Z. Li, W. Zhu, Z. Jin, W. Xu, A survey on heart biometrics, ACM Comput. Surv. 53 (6) (2020) 1–38.
[18] S. Ishaque, N. Khan, S. Krishnan, Trends in heart-rate variability signal analysis, Front. Digit. Heal. 3 (2021) 639444.
[19] F. Agrafioti, D. Hatzinakos, A.K. Anderson, ECG pattern analysis for emotion detection, IEEE Trans. Affect. Comput. 3 (1) (2011) 102–115.
[20] J.S. Arteaga-Falconi, H. Al Osman, A. El Saddik, ECG authentication for mobile devices, IEEE Trans. Instrum. Meas. 65 (3) (2015) 591–600.
[21] W. Yang, S. Wang, A privacy-preserving ECG-based authentication system for securing wireless body sensor networks, IEEE Internet Things J. 9 (8) (2021) 6148–6158.
[22] B. Fatimah, P. Singh, A. Singhal, R.B. Pachori, Biometric identification from ECG signals using Fourier decomposition and machine learning, IEEE Trans. Instrum. Meas. 71 (2022) 1–9.
[23] P.S. Addison, Wavelet transforms and the ECG: a review, Physiol. Meas. 26 (5) (2005) R155.
[24] P. Huang, L. Guo, M. Li, Y. Fang, Practical privacy-preserving ECG-based authentication for IoT-based healthcare, IEEE Internet Things J. 6 (5) (2019) 9200–9210.
[25] E.J. da Silva Luz, G.J. Moreira, L.S. Oliveira, W.R. Schwartz, D. Menotti, Learning deep off-the-person heart biometrics representations, IEEE Trans. Inf. Forensics Secur. 13 (5) (2017) 1258–1270.
[26] N. Ibtehaz, M.E. Chowdhury, A. Khandakar, S. Kiranyaz, M.S. Rahman, A. Tahir, Y. Qiblawey, T. Rahman, EDITH: ECG biometrics aided by deep learning for reliable individual authentication, IEEE Trans. Emerg. Top. Comput. Intell. 6 (4) (2021) 928–940.
[27] R.D. 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.
[28] L. Zhang, S. Chen, F. Lin, W. Ren, K.-K.R. Choo, G. Min, 1DIEN: Cross-session electrocardiogram authentication using 1D integrated EfficientNet, ACM Trans. Multimed. Comput. Commun. Appl. 20 (1) (2023) 1–17.
[29] M. Benouis, L. Mostefai, N. Costen, M. Regouid, ECG based biometric identification using one-dimensional local difference pattern, Biomed. Signal Process. Control. 64 (2021) 102226.
[30] A.S. Sakr, P. Pławiak, R. Tadeusiewicz, M. Hammad, Cancelable ECG biometric based on combination of deep transfer learning with DNA and amino acid approaches for human authentication, Inform. Sci. 585 (2022) 127–143.
[31] R. Bousseljot, D. Kreiseler, A. Schnabel, Nutzung der EKG-Signaldatenbank CARDIODAT der PTB über das Internet, 1995.
[32] S. Wahabi, S. Pouryayevali, S. Hari, D. Hatzinakos, On evaluating ECG biometric systems: Session-dependence and body posture, IEEE Trans. Inf. Forensics Secur. 9 (11) (2014) 2002–2013.
[33] G. Wang, S. Shanker, A. Nag, Y. Lian, D. John, ECG biometric authentication using self-supervised learning for IoT edge sensors, IEEE J. Biomed. Heal. Inform. (2024).
[34] C. Ding, Blum-blum-shub generator, Electron. Lett. 33 (8) (1997) 677–677.
[35] A.C. Guyton, Text Book of Medical Uhysiology, China, 2006.
[36] C. Zou, Y. Qin, C. Sun, W. Li, W. Chen, Motion artifact removal based on periodical property for ECG monitoring with wearable systems, Pervasive Mob. Comput. 40 (2017) 267–278.
[37] W. Tong, C. Kan, H. Yang, Sensitivity analysis of wearable textiles for ECG sensing, in: 2018 IEEE EMBS International Conference on Biomedical & Health Informatics, BHI, IEEE, 2018, pp. 157–160.
[38] P.W. Macfarlane, The influence of age and sex on the electrocardiogram, Sex-Specif. Anal. Cardiovasc. Funct. (2018) 93–106.
[39] E. Simonson, The effect of age on the electrocardiogram, Am. J. Cardiol. 29 (1) (1972) 64–73.
[40] T.M. Pereira, R.C. Conceição, V. Sencadas, R. Sebastião, Biometric recognition: A systematic review on electrocardiogram data acquisition methods, Sensors 23 (3) (2023) 1507.
[41] M.F. Safdar, P. Pałka, R.M. Nowak, A. Al Faresi, A novel data augmentation approach for enhancement of ECG signal classification, Biomed. Signal Process. Control. 86 (2023) 105114.