ECG-Based User Authentication Using Deep Learning Architectures

by

Vibhav Agrawal
BTech, SRM Institute of Science and Technology, India, 2020
M.A.Sc., University of Victoria, 2023

A thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

Master in Applied Science

in the Department of Electrical and Computer Engineering

ECG-Based User Authentication Using Deep Learning Architectures

by

Vibhav Agrawal
BTech, SRM Institute of Science and Technology, India, 2020
M.A.Sc., University of Victoria, 2023

Supervisory Committee

Dr. Fayez Gebali, Co supervisor
(Department of Electrical and Computer Engineering)

Dr. Haytham Elmilligi, Co supervisor
(Department of Electrical and Computer Engineering)

Dr. Mehdi Hazratifard, Department Member
(Department of Electrical and Computer Engineering)

ABSTRACT

Personal authentication security is an essential area of research in privacy and cybersecurity. For individual verification, fingerprint and facial recognition have proved particularly useful. However, such technologies have flaws like fingerprint fabrication and external impediments. Different AI-based technologies have been proposed to overcome forging or impersonating authentication concerns. Electrocardiogram (ECG)-based user authentication has recently attracted considerable curiosity from researchers. The Electrocardiogram is among the most reliable advanced techniques for authentication since, unlike other biometrics, it confirms that the individual is real and alive. This study utilizes a user authentication system based on electrocardiography (ECG) signals using deep learning algorithms. The ECG data is collected from users to create a unique biometric profile for each individual. The proposed methodology utilizes Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) to analyze the ECG data. The CNNs are trained to extract features from the ECG data, while the LSTM networks are used to model the temporal dependencies in the data. The evaluation of the performance of the proposed system is conducted through experiments. It demonstrates that it effectively identifies users based on their ECG data, achieving high accuracy rates. The suggested techniques obtained an overall accuracy of 98.34% for CNN and 99.69% for LSTM using the Physikalisch-Technische Bundesanstalt (PTB) database. Overall, the proposed system offers a secure and convenient method for user authentication using ECG data and deep learning algorithms. The approach has the potential to provide a secure and convenient method for user authentication in various applications.

Contents

List of Tables

List of Figures

ACKNOWLEDGEMENTS

I would like to thank:

Dr. Fayez Gebali, my supervisor, for his supervision, enthusiasm, motivation, and encouragement throughout my Master's program. I want to thank him for providing me the opportunity to work with him. I am really grateful to him for the continuous guidance, support, and feedback during this research.

Dr. Haytham Elmiligi, for being my committee member and mentor. I am really grateful to him for guiding and providing the feedback throughout this research work.

My family, for encouraging and inspiring me all through my journey. It would be impossible to realize this dream without their immense support and love.

Vibhav Agrawal

Chapter 1

Introduction

1.1 Problem and Context

The problem is to develop an authentication system that uses electrocardiogram (ECG) signals as the biometric identifier. The context for this system is to provide a secure and unique way for individuals to access their personal devices, accounts, and other sensitive information.

ECG signals are generated by the heart's electrical activity and are unique to each individual. It makes them an effective biometric identifier, as they cannot be easily replicated or faked. However, there are challenges associated with using ECG signals for authentication. For example, the signals can be affected by various factors such as body position, movement, and heart rate variability. Additionally, the signals can vary over time, so the system must adapt and accurately identify individuals even when their ECG signals have changed.

To overcome these challenges, the authentication system will need to use advanced algorithms and machine learning techniques to accurately and reliably identify individuals based on their ECG signals. It will require collecting and analyzing large amounts of ECG data from diverse individuals to train the system and improve its accuracy. The system will also need to incorporate user-friendly interfaces and be easy to use so that individuals can quickly and conveniently access their devices and information.

1.2 Overview

One-dimensional biomedical signals, such as the electrocardiogram (ECG) or electroencephalogram can be used as biometric characteristics [1]. ECG traces reveal information on electric cardiac transmission and are utilized to identify specific users. ECGs are strongly tied to the individual features of each person's heart. It is well recognized that each person's heart has distinct physiological features due to genetic variances. Such minor variations impact how the cardiac beats in each user's ECG pulse. Many methods have been implemented to benefit from these variations while using vital signs for user verification [2].

To verify identity in a platform, biometric technology uses biological information. Facial images, fingerprinting, eyes, vision, palm veins, speech, and even the form of the ears are some of the most popular data sources [3]. Moreover, several challenges must be overcome by Electrocardiography biometric technology, such as i) elevated pairwise variations brought on by pulse signs and conducted actions; (ii) a distinct lack of studies demonstrating the discrimination ability in massive data, (iii) protracted modifications in a person's ECG's features. Particularly uncontrolled collection conditions can significantly degrade the efficacy of ECG biometric devices. Fig. 1.1(a) shows the position of the electrode to record an ECG signal while Fig.1.1(b) shows the ideal ECG signal with no problems. It shows the traditional method in which the electrical impulses that enable the heart to pump are recorded using chest-mounted electrodes. In this new era of technology, a wearable electrogram consists of different sensing systems to collect the ECG data from the patient wrists or fingertips.

1.3 Artificial Intelligence using Biomedical Signals

Artificial intelligence (AI) is a field of computer science that aims to give computers human-like intelligence, allowing them to learn, think, and resolve issues when confronted with various information. AI plays an essential role in identifying and diagnosing healthcare problems. Various physiological signals, such as the ElectroCardioGram (ECG), PhonoCardioGram (PCG), and BallistoCardioGram (BCG), which disclose the electrical, acoustical, and physical heartbeat, accordingly, are used to identify the cardiac muscle function. ECG signals were chosen for this project due to technological limitations and their well-known waveform, which allows for improved recognition. However, the great variety of form, structure, and intensity variations

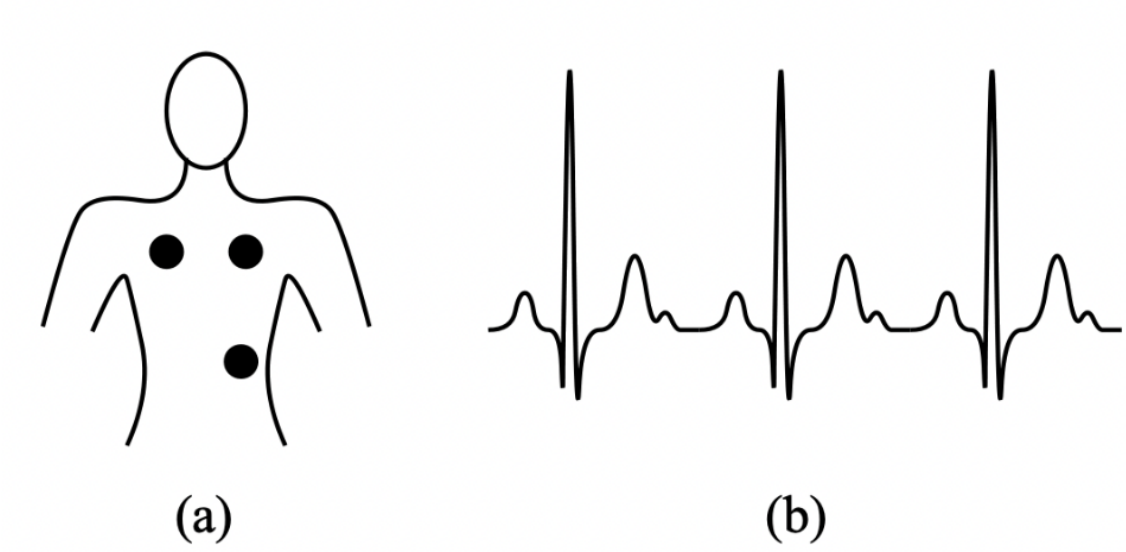

Figure 1.1: (a) Electrodes position for ECG recording (b) ideal ECG signal.

between and among individuals continue to be a challenging problem to address. Recent advances in AI's machine learning and deep learning have entirely changed how neuropsychological operations are performed. They include features like extracting features, extraction of features, attribute selection, categorization, and data pretreatment. The study found that due to AI, medical doctors might depart the operating theatre with greater assurance of a patient's diagnosis.

Artificial intelligence has subsequently become a vital method for studying and restoring diverse biological data. The rapid development of biological and biomedical signal processing techniques in various fields, including intelligence image analysis, surface-enhanced spectroscopic methods, and electroencephalography (EEG), has been made possible by the development of practical machine learning and deep learning algorithms. Signal processing is a crucial stage in assessing and accurately reconstructing biomedical signals that are frequently severely disturbed. Therefore, building a complicated approach for maximum performance frequently takes several impacts and attempts, extensive computations, as well as in computational equations for optimum selections. Traditional signal processing techniques offer a plausible option. DL precisely duplicates the intended result, enabling a speedy and effective service. Based on the most current developments in learning strategies, supervised, self-supervised, and unsupervised approaches may all be used to provide the required

results. With the advancement of techniques like biosensing, medical imagery, and informatics, AI is currently playing an increasingly crucial role in both biomedical and biological sciences.

Several medical specialties, including cancer, radiology, ophthalmology, neurology, and cardiology, employ artificial intelligence (AI). In order to provide advanced e-Health mechanisms that take advantage of the expansion of online interconnection for a medical condition, current approaches are increasingly investing in the fusion of various technologies, such as machine learning and Deep Learning algorithms with IoT technology, Cloud computing, and big data. Deep learning (DL) is a machine learning technique with a multi-layered structure where additional pattern recognition stages are carried out.

The output layers examine and categorize patterns, while the intake layers extract characteristics. Deep discriminatory models include convolutional neural networks (CNNs), and deep belief networks (DBNs). And recurrent neural networks (RNNs). Cycles of ECG signals may be used to identify cardiac conditions using the DL network. A DL approach works similarly to the human brain and is based on complex algorithms. By training on input and output data to build patterns between them, mathematical functional principles seek to understand and recognize patterns among numerous elements. The system can recognize the entities on which it has been trained on during the training process.

1.4 ECG and fingerprint Authentication

Reliable identification and authentication procedures are essential to secure the authenticity of systems and confidential material. Although they have enabled security controls and verification, passwords have also revealed some weaknesses. Biometric technology is the best authentication method due to its comfort, precision, and the possibility of minimal subversion. Fingerprint recognition systems work by capturing an image of an individual's fingerprint and then using pattern recognition algorithms to compare the captured fingerprint to a database of known fingerprints. When a person places their finger on a fingerprint scanner, the scanner captures an image of the fingerprint and converts it into a digital template. This template is then compared to the templates in the database to find a match. If a match is found, the person is authenticated. Fingerprint recognition systems can provide a high level of security, as fingerprints are unique to each individual and are difficult to forge.

ECG (electrocardiogram) authentication systems use sensors to measure the electrical activity of the heart, which is unique to each individual. The sensors, which are typically placed on the skin, capture the ECG signal and convert it into a digital template. This template is then compared to a database of known ECG templates to find a match. If a match is found, the person is authenticated. ECG-based authentication systems can provide a high level of accuracy and can offer continuous authentication, as the ECG signal is constantly being generated by the heart. Additionally, ECG measurements can be taken non-invasively, making them a convenient and secure means of verifying an individual's identity. Deep learning models can be used in ECG-based authentication systems to improve the accuracy and efficiency of the authentication process. By training a deep learning model on a large dataset of ECG signals, the model can learn to recognize patterns in the signals that are unique to each individual. This allows the model to accurately distinguish between different individuals and to identify the person whose ECG signal is being measured.

The use of ECG (electrocardiogram) signals for authentication has several potential advantages over the use of fingerprint recognition. Firstly, ECG signals are unique to each individual and can provide a high level of accuracy for authentication purposes. Secondly, ECG signals can be measured non-invasively, using sensors on the skin, whereas fingerprint recognition requires physical contact with a scanner. Thirdly, ECG signals can provide continuous authentication, allowing for continuous monitoring of an individual's identity, whereas fingerprint recognition requires periodic re-scanning. Overall, ECG-based authentication systems can offer a convenient and accurate means of verifying an individual's identity.

1.5 ECG authentication system under consideration

The electrocardiogram (ECG) is made up of three major segments that correspond to various cardiac operations: atrial depolarization (P wave), ventricular repolarization (T wave), and ventricular depolarization (QRS complex). There are three ECG feature types: hybrid, non-fiducial, and fiducial. Fiducial features retrieve discrete-time properties from the Electrocardiography[4], which are calculated as time frames, pulse width, angles, and dynamical intervals based on the distinctive locations inside the ECG waveform. Non-fiducial characteristics alter the feature points using trans-

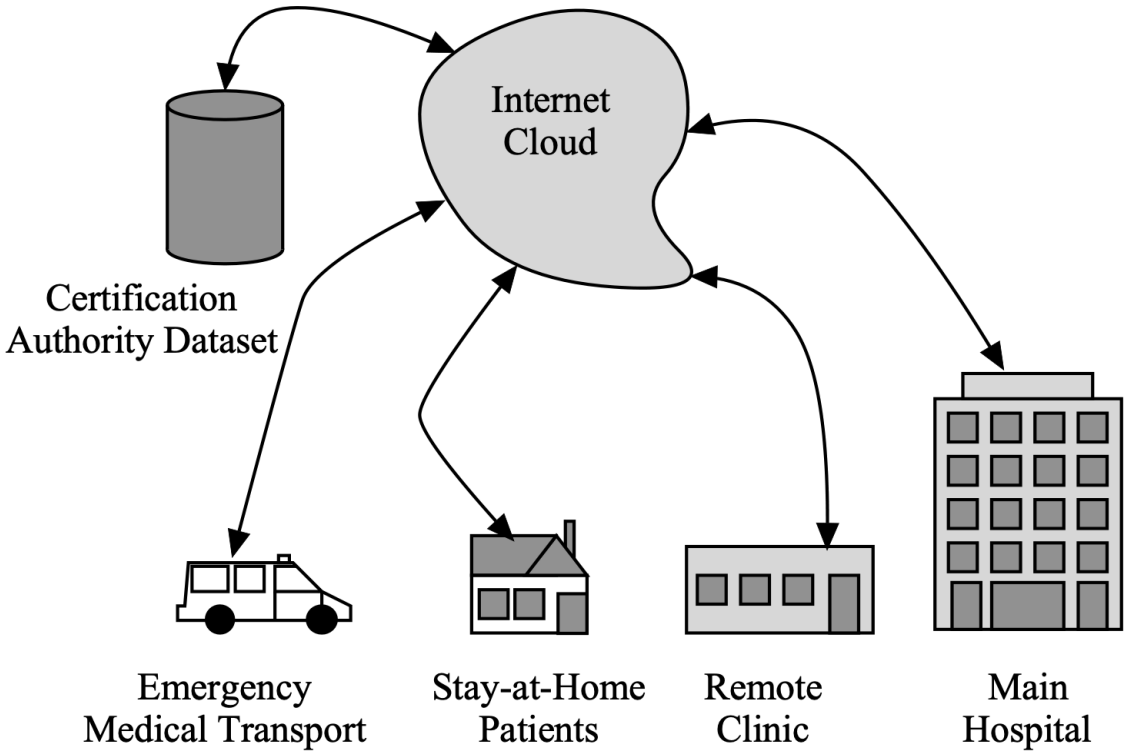

Figure 1.2: Telehealth system under consideration

formation functions, whereas hybrid characteristics integrate fiducial and non-fiducial techniques. Researchers consider fiducial techniques because they only employ readings of fiducial markers of an Electrocardiogram as characteristics inside the temporal domain [5]. The Electrocardiogram is a diagnostic technique that is frequently used to examine the muscular and electrical functions of the cardiovascular system by monitoring the heart rate and activity. Fig. 1.2 presents the Telehealth system connected through cloud services with local hospitals, clinics, emergency services and patients at home. Healthcare practitioners may check a person's health over time from a distance thanks to wearable technology, unobtrusive sensing, and telemedicine, which can assess symptoms and early illness warning indicators. This would enable improved management through the early detection and surveillance of illness signs, thus eliminating the requirement for face-to-face interaction [6, 7].

Several challenges have been identified in using telehealth systems in the last decades. Some of the main problems include the following:

- Security concerns: Telehealth systems handle sensitive medical information and personal data, so they must be secure to protect against unauthorized access

and data breaches. This can be challenging, especially given the increasing sophistication of cyber threats.

- Interoperability issues: Telehealth systems often need to integrate with many other systems, such as electronic health record systems, insurance providers, and lab systems. Ensuring interoperability between these systems can be complex and time-consuming.

- Limited user acceptance: Some people may be hesitant to use telehealth systems due to concerns about their privacy, the perceived invasiveness of the technology, or a lack of understanding about how the systems work.

- Limited accessibility: Telehealth systems may not be accessible to everyone, particularly in areas with limited broadband connectivity or other infrastructure challenges.

- Regulation and compliance issues: Telehealth systems are subject to a wide range of regulations and requirements, which can be complex and time-consuming.

- Technical challenges: Telehealth systems can be complex and require specialized infrastructure and support to function effectively. Ensuring that the systems are reliable, scalable, and user-friendly can be challenging.

The authentication method has new possibilities because of the recent advancements in deep learning (DL) and machine learning (ML) classification algorithms. The branch of artificial intelligence known as ML uses training data to create statistical formulas, most often regression (predictions) systems and decision modeling techniques (e.g., categorization and feature identification) [8, 9, 10, 11]. One of the many uses for ML is the analysis of pictures, audio, videos, and ECG information. DL have been applied to the top ML algorithms to enhance their accuracy. Deep neural networks perform better in application scenarios than conventional categorization methods. They effectively resolve complex issues because they can evaluate various input features. The findings have demonstrated that the DL neural models can likely offer greater prediction accuracy and efficient performance [12, 13].

The research works in this part demonstrate the efforts to create various CNN designs to recognize people using ECG data. Still, handling such complicated data requires a precise approach. We suggest that using CNN and LSTM architectures

would create efficient and precise identification using ECG signals. In order to obtain characteristics that allow for closed-set recognition, biometric identification, and recurring verification, this paper offers DL frameworks based on CNNs and LSTMs. Open-access database from the Physionet dataset is used to test the suggested technique using quality metrics. The following are the study's main contributions:

1.6 Research Contributions

1. We illustrate the implementation of bidirectional Recurrent neural networks based on Long Short-Term Memory (LSTM) in addition to 1D-CNN for ECG authentication by achieving state-of-the-Art accuracy.
2. We performed data pre-processing to improve the performance of our DL models. To speed up the convergence of our model, the redundant values are deleted.
3. We conduct thorough tests and exams on widely known baseline methods and compare our technique to state-of-the-art methods.
4. We demonstrated that our models could be applied to ECG data obtained under various circumstances, delivering superior or equivalent reliability to the top-performing state-of-the-art techniques.

1.7 Thesis Outline

Chapter 1 This first chapter presents the problem and context, overiew and different techniques for authentication system, research contributions, and a thesis outline.

Chapter 2 incorporates the key concepts of preliminary literature review of the state-of-the-art authentication systems based on machine learning and deep learning methods. It also presents the related work in this area of research.

Chapter 3 presents the proposed methodology used in this research study.

Chapter 4 incorporates the expiremental setup and data preprocessing steps performed on the data.

Chapter 5 presents the conclusion and future works.

Chapter 2

Literature review

Electrocardiogram (ECG) signals have been proposed as a biometric modality for authentication purposes. ECG signals are unique to each individual and can provide a high level of accuracy for authentication. In addition, ECG measurements can be taken non-invasively, making them a convenient and secure means of verifying an individual's identity. Several studies have investigated the use of ECG signals for authentication. The ECG-based authentication systems can provide a high level of accuracy, with a low false acceptance rate and a low false rejection rate. Another study showed that ECG-based authentication systems can provide continuous authentication, allowing for the continuous monitoring of an individual's identity.

In recent years, the use of deep learning algorithms for ECG-based authentication has gained attention. These algorithms can learn to recognize patterns in ECG signals that are unique to each individual, allowing for highly accurate identification. Additionally, the use of deep learning algorithms can improve the efficiency of the authentication process, allowing for real-time authentication. Overall, the use of ECG signals for authentication has the potential to offer a convenient and secure means of verifying an individual's identity. The use of deep learning algorithms can further improve the accuracy and efficiency of ECG-based authentication systems. There are previous related works that have used traditional image processing, ML, and DL methods for user authentication using Electrocardiogram data.

2.1 Machine Learning based Authentication

Machine learning algorithms can be used to create a biometric authentication system based on ECG data. This involves training a machine learning model on a large dataset of ECG readings from many different individuals. To use this system, a person must provide their ECG as input to the machine learning model. The model would then compare the input ECG to the patterns it has learned from the training data and predict as to whether the input ECG belongs to the person who is trying to authenticate. Many machine learning algorithms could be used for this task, including support vector machines, decision trees, and deep learning networks. The choice of algorithm would depend on the ECG data's specific characteristics and the authentication system's performance requirements.

Hamza *et al.* [14] provide a two-step process, consisting of data extraction and classification, for conducting person authentication using ECG data. Three additional forms of feature indices, zero crossing rate (ZCR), and entropy, are combined in the initial stage. The support vector machines (SVM) have been utilized for the categorization scheme in stage two. They evaluated the model on two public benchmark databases, obtaining the highest precision and accuracy values. Zaghouani *et al.* [15] proposed a security-based framework to safeguard the private information sent across ECG communication links, sometimes referred to as "unreliable channels." In the suggested technique, the ECG characteristics are hidden via linear prediction encoding rather than being sent to the recipient end. Therefore, the cryptographic keys are produced on the recipient's end rather than being transmitted. The proposed method showed outstanding results by keeping the patient's privacy in safe hands.

Akeem *et al.* [16] proposed an improved Electrocardiography biometrics verification scheme for applications. They employed a regression-based interpretable ML technique to establish the database bounds and obtain high-quality data for training. A collaborative regression analysis was then employed to create the benchmark functionality for every Electrocardiogram data entity (i.e., identification). The developed program's authenticating performance was determined using a confusion matrix with the amgecg toolkit in MATLAB, which investigates two crucial variables. The recommended system shows high performance during testing. Hamza *et al.*[17] suggested combining various techniques to identify people. Their algorithim focuses primarily on a mixture of attributes, including the prosodic and acoustic properties of every section of the ECG waveform. SVM is used to assess the effectiveness of

the suggested strategy for recognizing people. The proposed system has an average accuracy of 92.5% with ECG-ID benchmark data, and with the MIT-BIHA collection, it has an accuracy rate of 98.6%.

Biran *et al.* [18] present an automation system enabling person identification utilizing randomly chosen Electrocardiogram signals. The proposed approach is based on a mix of short-time Fourier transforms for separating frequency information and Fréchet Mean Distance (FMD) for recognizing individual objects. Repeated measurements using this technology have shown good subject identification outcomes. The proposed architecture achieves an average of 96% accuracy in the evaluation process. For intelligent healthcare systems, Zhang *et al.* [19] developed a comparable approach with a few peculiarities. The features depend on fiducial data as well as non-financial information. The large and small maximum for each subspace are the two production methods for detection. The results of appropriate tests that evaluate a recommended method's performance reveal that it operates with noticeably more accuracy and effectiveness than other conventional approaches.

The Khan *et al.* [20] cardiac project's objective is to find heart problems by examining ecg images. Several machine learning and image analysis applications have shown the effectiveness of deep neural networks. This article covers the pertinent analyses and research in-depth with a focus on diagnosing cardiac disease. The article offers an all-inclusive method for managing all ECG file formats. Using the solitary image recognition Neural Network architecture, cardiovascular illness was found. With a 98% accuracy rate in differentiating and identifying four central cardiac abnormalities, this study showed outstanding findings.

Kim *et al.* [21] proposed an electrocardiogram (ECG) biometric verification for healthcare identification that would change ECG impulses by dividing them based on the period between pulse rates. Each layer of the data was used as a training parameter for the model. Using the specified criteria, they can attain efficiency of up to 95%. Overall performance is the result of adding the results of many authentication methods. The intrinsic representation and transparency of decision tree based systems is a crucial advantage that may help determine whether to admit or reject an individual within the health care.

2.2 Deep Learning based Authentication

Deep learning algorithms can analyze ECG signals and extract useful information from them. It typically involves training a deep-learning model on a large dataset of ECG signals. The model can then make predictions or classifications based on new ECG signals it presents. The deep learning model is then trained on this dataset using a supervised learning algorithm, which adjusts the model's internal parameters to minimize the prediction error on the training data.

Nabil *et al.* [22] proposed a novel biometric authentication system EDITH that identifies individuals using electrocardiography (ECG) data. This technique can provide a safe and dependable method of authenticating people based on their distinct ECG patterns. The key benefit of EDITH is that it analyzes ECG data using deep learning algorithms, providing a high level of precision in identifying individuals. Furthermore, because ECG signals are distinctive to each individual, it is difficult for someone to imitate another person using this technology. The necessity for specialized hardware, such as ECG sensors, to gather and interpret ECG data is one possible area for improvement with EDITH. However, as this technology becomes more popular and accessible, deploying EDITH in several scenarios may become more practicable.

A system developed by [23] to evaluate data from the Internet of Things (IoT) devices in a healthcare environment is the Event-driven IoT architecture for data analysis of trustworthy healthcare applications employing complicated event processing. This system analyzes data from IoT devices, such as sensors and wearable devices, using an event-driven architecture and advanced event-processing algorithms. One of the system's key benefits is its capacity to analyze massive volumes of data in real-time, allowing for rapid and accurate examination of healthcare data. The application of complicated event processing algorithms also enables the discovery of patterns and correlations in data, which may be beneficial in detecting trends and predicting outcomes. This system's capacity to grow to accommodate many IoT devices is another advantage, making it suited for application in various healthcare settings. Furthermore, the event-driven architecture integrates many data sources, such as electronic medical records and sensor data, to give a more comprehensive perspective of a patient's health.

Lee *et al.* [24] used an ensemble of 2D CNN and LSTM ECG data to achieve personally identifiable information. As a first stage, noise reduction and standard variation correction were carried out. After contrasting and comparing 1 LSTM layer

and 2 LSTM layer, the only ECG having distortion was eliminated and classified using 2 LSTM layers with greater accuracy. The overall efficiency of every 2D CNN and LSTM was enhanced via ensemble learning, the identification accuracy increasing from 1.06% to 3.75% relative to a single framework.

Kim *et al.* [25] presented a new LSTM Deep RNN design based on ECG classification and conducted an operational assessment for the algorithm using different databases. The outcomes demonstrate that the recommended methodology is more effective than other traditional approaches and surpasses them. The tests reveal that the suggested model outperforms the traditional LSTM technique in terms of classification precision and performance by achieving the F1 score of 0.99, the precision, recall, and accuracy of 99.8%.

Prakash *et al.* [26] provides BAED which is a protected biometric authentication system based on ECG signals and deep learning techniques. BAED is a biometric identification technique that recognizes persons using electrocardiography (ECG) signals and deep learning techniques. BAED's usage of ECG signals, which are unique to each individual and give a high level of security, is one of its key benefits. BAED's deep learning algorithms allow great accuracy in identifying individuals based on their ECG data. One advantage of BAED is that it employs secure protocols to preserve ECG data and prevent unwanted access. The system guarantees that the system is safe and that people's privacy is respected.

An elderly health monitoring system based on biological and behavioral indicators is a system developed to monitor the health of senior adults using biological and behavioral markers proposed by Hosseinzadeh *et al.* [27]. This system collects data on numerous indicators such as heart rate, blood pressure, and sleep habits using IoT devices such as sensors and wearable devices. It can provide real-time monitoring of a person's health, allowing for quick action in the case of a health problem. The utilization of many indicators, including biological and behavioral markers, provides a complete picture of an individual's health. Another advantage of this system is its capacity to remotely monitor older people, which is especially beneficial for those who live alone or have mobility concerns. This can offer caregivers and family members peace of mind while lowering the chance of falls or other incidents.

Labati et al. [28] proposed a new technique called Deep-ECG for biometric identification based on an Electrocardiogram signal. This method can be used mainly for three biometric tasks: confined recognition, proof of identity, and periodical reauthentication. In order to obtain a selection of characteristics, a deep CNN net-

work is used to evaluate groups of QRS waves that have been recovered using ECG data. Simple and binary templates are compared using Hamming distances and Euclidean. The proposed technique achieves high performance and efficiency. Salloum *et al.* [29] suggested using RNNs to create a feasible option for classification and identification issues in ECG-based identification. Compared to earlier techniques that utilized the ECG-ID or MITDB databases, this work has shown that LSTM RNNs provide an efficient approach to ECG biometric authentication and identification.

Karpinski *et al.* [30] created and validated a novel approach relying on auto-encoder neural network models to detect and eliminate ECG pulse abnormalities. The processed and standardized ECG data is sent into the auto-encoder algorithm. The input and reconstructed data are evaluated, and the root-mean-square loss is computed. The error function is employed to find inaccurate information. The research findings have been contrasted with previously created methods. Belo *et al.* [31] have demonstrated the value of Deep Neural Networks for improving existing biometric technology. To enhance the outcomes of both the recognition (actual man) and verification (actual identification) procedures, the following two structures are proposed: Recurrent Neural Network (RNN) and Temporal Convolutional Neural Network (TCNN). Overall, the results demonstrate that the TCNN surpasses the Recurrent neural network, reaching nearly 100% and 90% efficiency for recognition and 0.1% and 2.2% equivalent margin of error for authenticating operations.

Chapter 3

Research Methodology

This section offers an in-depth analysis of the suggested technique with algorithms. The literature review stated above served as an inspiration for the suggested method in this part. We employed deep learning (DL) techniques to address every study question. Each DL model's parameters and several layers have been altered to get the best accuracy. Figure 3.1 provides a visual representation of the preprocessing, training, and assessment phases of ECG identification. The suggested technique is based on deep learning algorithms that are trained and optimized utilizing a wide range of hyperparameters. The learning rates and biases in neural networks are optimized accordingly.

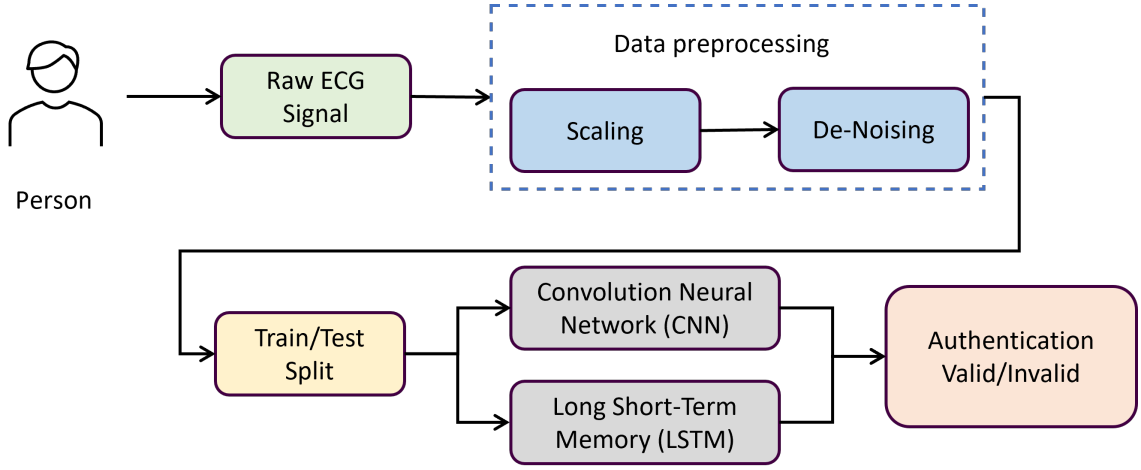

Figure 3.1: Block diagram of proposed methodology.

Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks are popular deep learning architectures that have been used in a variety of

applications including image classification, speech recognition, and natural language processing. In the context of authentication using ECG signals, CNNs can be used to extract features from the ECG signal by performing convolution operations on the signal. These features can then be used to classify the signal as belonging to a particular individual or not.

LSTM networks, on the other hand, are good at handling sequential data and can be used to model the temporal dependencies in the ECG signal. By analyzing the sequence of ECG signals over time, the LSTM network can identify patterns and extract features that can be used for authentication. The Rectified Linear Unit (ReLU) activation function is commonly used in deep learning architectures like CNNs and LSTMs because it is computationally efficient and has been shown to work well in practice. ReLU activation function helps to introduce non-linearity into the network, which is important for modeling complex relationships between the input and output

3.1 Convolution Neural Networks

The most sophisticated DL-based algorithms for learning robustness and automatically distinguishing features are CNNs. Deep learning uses numerous convolutional layers to reflect learning features based on data. CNN has been used for various cognitive activities, including computer vision [32], natural language [33], and others. Many Convolutional networks, including Caffe-Net [34], Alex-Net [35], and VGG-Net [36], have been created for large-scale image recognition. Each phase of this convolution layer encoder collects the features from the input layer. A vector of a predetermined length is created by condensing the data. The database contains a wide range of inputs. Max-Pooling, Convolution, and Dense layers are used to achieve the results.

The CNN is presented with a batch of ECG signals and their corresponding labels (permitted or denied). The CNN processes the ECG signals through a series of layers, starting with the input layer and ending with the output layer. Each layer consists of several units, which are connected to the units in the previous and next layers by weights. The CNN processes the ECG signals, it learns to recognize features characteristic of authenticated and not-authenticated signals. These features are learned through convolution, which involves sliding a kernel (a small matrix of weights) over the input data and computing dot products between the kernel and the input data at each position. The dot products are then passed through an activation function, which determines whether or not the unit should be activated (i.e., whether it should

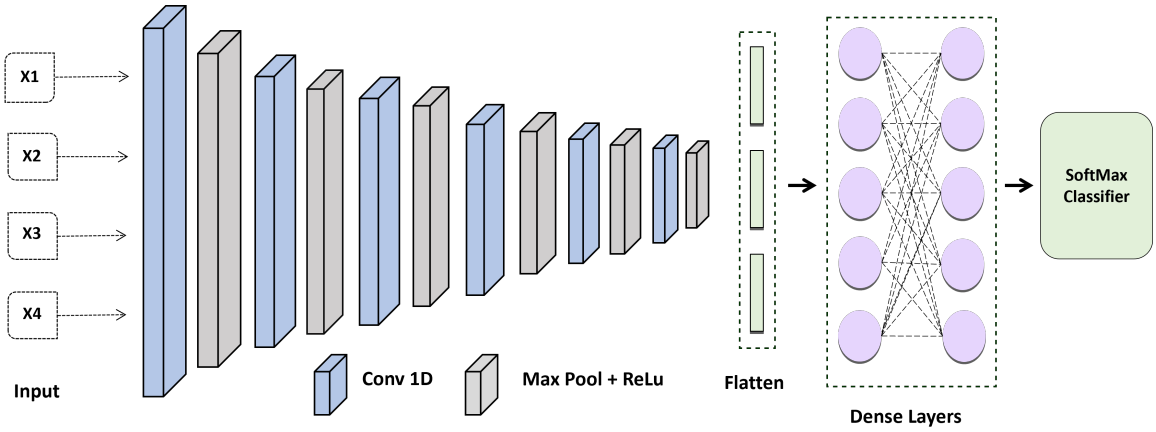

Figure 3.2: Proposed Convolution Neural Network Model for ECG-based Authentication

contribute to the output of the layer).

As the CNN processes the ECG signals, the units' weights are adjusted to minimize the difference between the predicted and true labels. This process, known as backpropagation, continues until the CNN has learned to classify the ECG signals accurately. Once the CNN has been trained, it can be used to classify new ECG signals and determine whether or not they are authenticated. This is done by presenting the CNN with the new ECG signal and using the output of the CNN to make a prediction

The design of the proposed CNN shown in Figure. 3.2 was employed in this investigation to create the ECG feature patterns. It has five convolutional layers, with a max pooling layer, a fully connected layer, and a soft-max layer following each one. In all networks, the fully connected layer has the same design. Because local response standardization does not enhance the efficiency of our Electrocardiogram collection but rather causes an increase in computation time and memory usage, all fully connected layers are provided with Rectified Liner Unit (ReLU) activation.

The CNN was configured with the following layers: Inputs → Convolution-1D (16 features, map size 7, ReLu) → Max Pool Layer(stride 3,2) → Convolution-1D (32 features, map size 5, ReLu)→ Max Pool Layer(stride 3,2) → Convolution-1D (54 features, map size 5, ReLu)→ Max Pool Layer(stride 3,2) → Convolution-1D (128 features, map size 7, ReLu)→ Max Pool Layer(stride 3,2) → Convolution-1D (256 features, map size 7, ReLu)→ Max Pool Layer(stride 3,2) → Convolution-1D (256 features, map size 8, ReLu)→ Max Pool Layer(stride 3,2) → Flatten Layer → Dense (100 units) → SoftMax. The Adam optimization technique with categorical cross

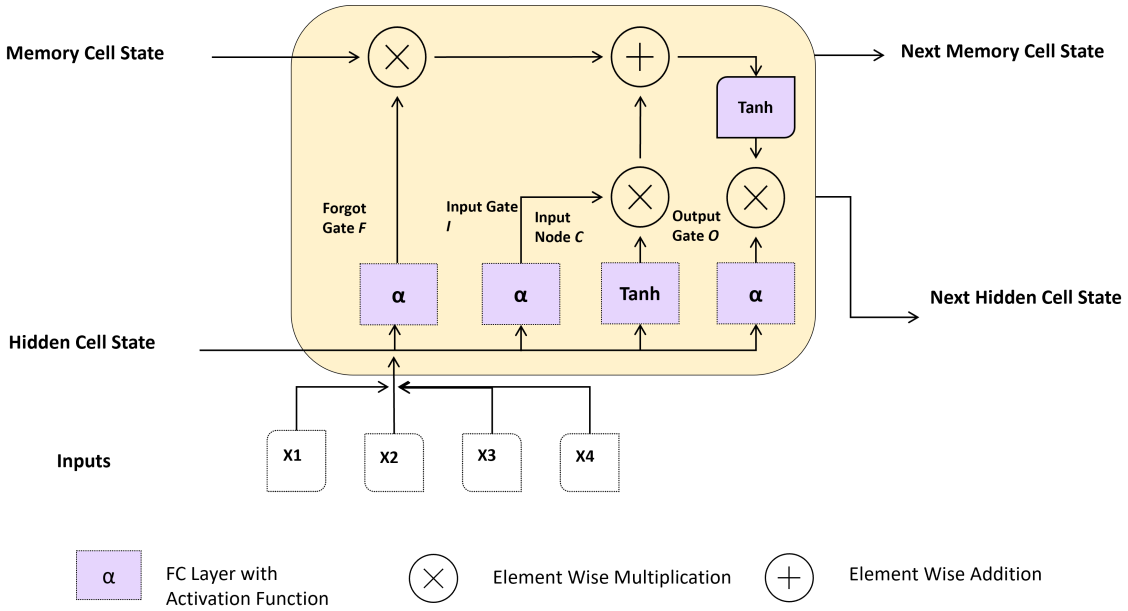

Figure 3.3: Main components Long Short-Term Memory (LSTM) Cell

entropy produces better outcomes.

3.2 Long Short-Term Memory Networks

The LSTM (DL) model for serial and time analysis is the most popular DL model, which solves the poor memory problem. With the aid of the gates referred to in its internal structure, which are employed to control the flow of information, LSTM solves this poor memory problem. The LSTM model works best for time series data, such as translating, meteorology, and voice recognition. Its operating method of gating carries forward the crucial data inside the lengthier data set to produce precise and effective predictions [37].

The long-term dependence issue of a RNN was proposed to be resolved by an LSTM with architecture more sophisticated than an RNN [38], [39]. An LSTM has an input gateway, forget gate, and outlet port to avoid data redundancy. Using the output value, the sigmoid transfer function returns a number between zero and one, indicating how much information there is. As a result, it can add or remove cell state information. An LSTM's activation functions are the sigmoid [40] and Relu nonlinear activation functions [41]. In contrast to the forget gate, which controls whether previous data is removed from the cell state, the input gate controls whether

new data is retained in the cell state. The output gate chooses which information from the cell state should be output in the meanwhile.

LSTM networks retain information from previous time steps in the data by using a particular unit called a memory cell, designed to retain information over an extended time. Each memory cell in an LSTM network has three gates: an input gate, an output gate, and a forget gate. The input gate determines which information from the current time step should be added to the memory cell. In contrast, the forget gate determines which information from the previous time step should be discarded. The output gate determines which information from the memory cell should be used to predict the current time step. Figure 3.3 shows the main components of LSTM cell.

The information retained in the memory cell is combined with the input data at the current time step to produce an output, which is then passed to the next layer of the LSTM network. This process is repeated at each time step, allowing the LSTM network to retain information from previous time steps and use it to make predictions at future time steps. In the case of ECG data for authentication systems, the LSTM network would be trained to learn features from the ECG signals indicative of authenticated and not-authenticated signals. As the LSTM network processes the ECG signals, the memory cells would retain information about the characteristics of the signals, which would be used to make predictions about the authenticity of the signals at each time step.

The alpha function is also known as the Rectified Linear Unit (ReLU) with a negative slope. The alpha function is a piecewise linear function that outputs the input if it is positive, and a linear function of the input if it is negative. The formula for the alpha function is:

where alpha is a hyperparameter that determines the slope of the negative part of the function.

$$f(x) = \begin{cases} x & \text{if } x > 0 \\ \alpha \cdot x & \text{if } x \leq 0 \end{cases} \tag{3.1}$$

The tanh function is commonly used in neural networks for several reasons. First, it is a symmetric function, meaning that it has an equal range of positive and negative outputs. Second, the tanh function is steeper around zero than the sigmoid function, which can make it more effective in learning complex relationships between the input

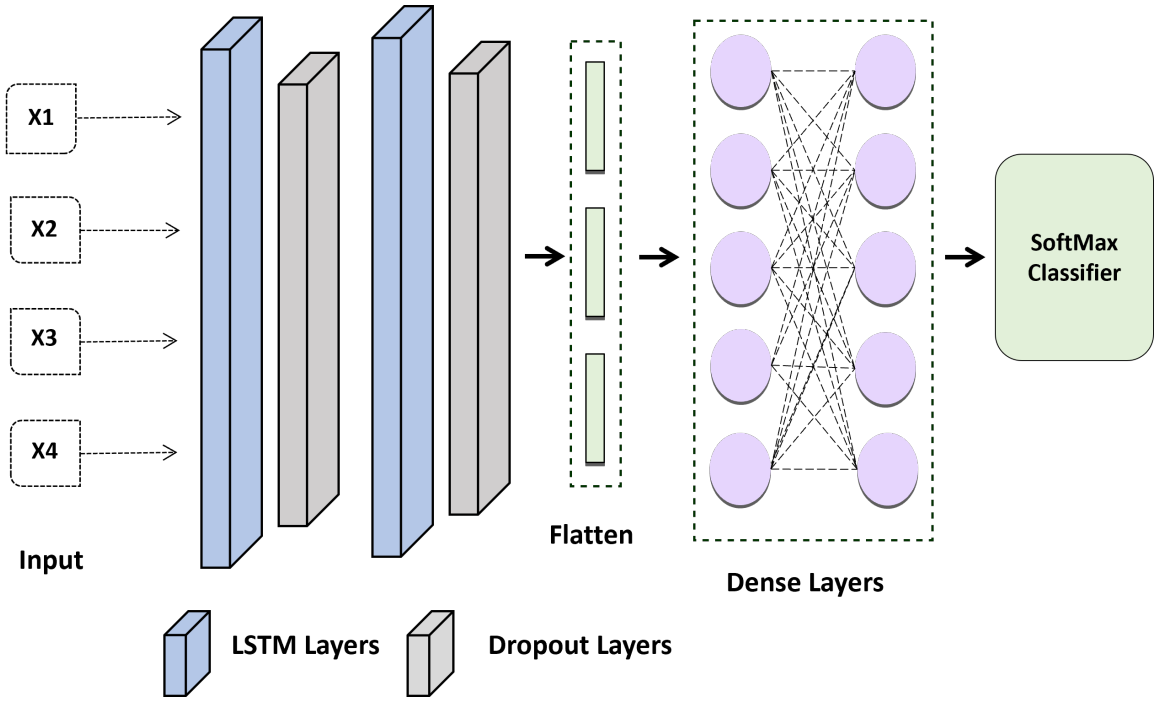

Figure 3.4: Proposed LSTM Model for ECG-based Authentication

and output. The tanh function, short for hyperbolic tangent, is a nonlinear activation function that outputs values between -1 and 1. The formula for the tanh function is:

$$f(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{3.2}$$

In addition to being used as an activation function, the tanh function is also used in LSTM cells to update the memory cell. The tanh function is used to scale the input values between -1 and 1, allowing the model to more easily learn the long-term dependencies in sequential data

Therefore, in this study, the proposed method considered the result at each time-stamp rather than only collecting the concealed factor at the output. Model 2 in Figure. 3.4 represents the LSTM model's suggested design. Each time-output stamp from the LSTM cell is added together and then transmitted via a dropout layer. After that, a fully linked layer receives the outputs of the single hidden layer. Last but not least, the chance that an ECG sequence belongs to a person is determined using a Softmax function. The candidate individual is chosen as the one whose likelihood is at its highest.

An LSTM layer is added to the most recent algorithm implementation to check

whether the results were noticeably better than those of other networks. The layer of the network was set up as follows: LSTM Layer (64 filters) → Dropout (0.2 rates) → LSTM Layer (32 filters) → Dropout Layer (0.2 rates) → Flatten Layer → Dense Layers → SoftMax. Better results are obtained using the Adam optimization strategy with categorical cross-entropy.

3.3 Authentication System

The process of confirming and guaranteeing an object's identity is known as authentication. Given the significance of data in the healthcare system, authentication can offer access control by determining whether a user's credentials match the readily available records on the server. ML and DL provide the key to using evolving authentication. To reduce security barricades and deal with security issues, ML can be established. A key measure to prevent unwanted administrator privileges is to use ML to authenticate only those individuals, such as IoT devices, medical professionals, and patients, before allowing them to communicate with system resources.

Deep learning classifiers calculate the resemblance of a data set to every data classification process. Then, based on their definition of a probability measure, select the category with the highest probability based on similarity. In contrast, classifier-based authentication models train exclusively using valid class samples. The first class will be chosen for the classifier in both scenarios in Table 3.1 because it has the highest probability value. In contrast, the authentication model requires a two-stage algorithm that follows the flowchart in Figure 3.5. The sample gathered from the individual is submitted to the trained classifier, which determines whether or not the predicted and claimed labels match. If the sample fits the claimed label within the limits of the threshold (θ), the system will identify the individual and authenticate it further; otherwise, the suggested classifier will reject the sample, and the entrance will be denied.

Table 3.1: Two scenarios for the membership probability according to similarity to each class distribution in a 5-class problem.

Probabilities	1	2	3	4	5
Scenario A	0.91	0.01	0.01	0.01	0.01
Scenario B	0.45	0.33	0.15	0.01	0.01

Authentication-based systems help to ensure the security and safety of telehealth

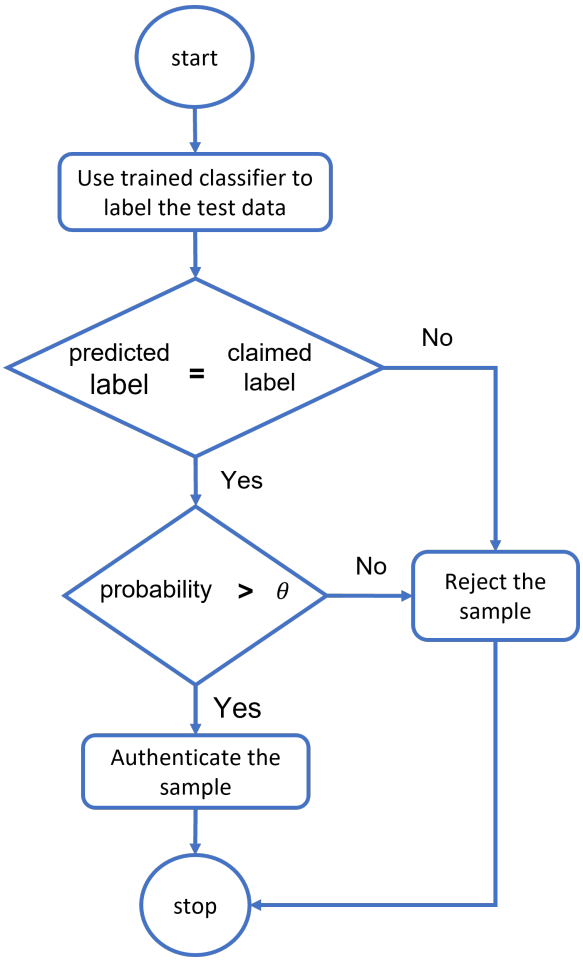

Figure 3.5: The flowchart of threshold-based classifiers for authentication

systems by verifying the identity of users who access the system. It helps to prevent unauthorized access to patient information and other sensitive data and can also help to prevent fraud and abuse. There are several different ways that telehealth systems can use authentication to verify the identity of users. For example, they may require users to enter a username and password, or they may use biometric authentication methods such as fingerprint scanning or facial recognition. In addition to verifying the identity of users, telehealth systems may also use encryption and other security measures to protect patient information and other sensitive data from being accessed or intercepted by unauthorized parties. It helps ensure that patient privacy is maintained and that telehealth systems are safe and secure for use by both patients and healthcare providers.

Chapter 4

System Implementation

The ECG authentication system can be used in two modes: verification (authentication) or identification (recognition). The verification mode is used to validate an asserted identity. It is used to determine whether a person is whom he or she claims to be. This mode is used to authenticate a mobile user. The score is compared to a preset threshold during verification, and the claimed identity is approved if the score is more significant. The identification method is used to categorize and identify an unknown identity. It answers inquiries such as "who is this person?" and "is this person in the database?" This method is commonly used in cybercrime. During identification, the highest matching score is taken into account. ECG biometric design is divided into two stages: enrollment and authentication. Finally, the assessment criteria will be used to make a choice. Figure. 3.5 presents the schematics of authentication methodology.

The ECG data is gathered, analyzed, and saved as a reference template throughout the enrollment phase. The ECG test sample is checked against the stored reference template(s) in the Authentication phase to ascertain the similarity or dissimilarity score provided by machine learning technique(s) against a predetermined threshold. Firstly, ECG signals are acquired by putting electrode leads on the person's body (on the person) or through wearable devices (dry electrodes, off-the-person). After recording the ECG signals, they are pre-processed before feature extraction. Finally, the samples are saved in a feature database and categorized using classifiers like decision trees, support vector machines, CNN, etc.

The ECG is a diagnostic tool that measures and records the heart's electrical activity. Figure 4.1 represents the essential components of ECG signal. The ECG signal comprises several waveform components, each corresponding to a specific event

in the heart's electrical activity. Some of the essential components of the ECG signal include:

- P wave: The P wave represents the depolarization of the atria or the heart's upper chambers. It is typically a small, positive waveform that precedes the QRS complex.
- QRS complex: The QRS complex represents the depolarization of the ventricles or the heart's lower chambers. It is typically a larger, more complex waveform that follows the P wave.
- T wave: The T wave represents the re-polarization of the ventricles. It is typically a small, positive waveform that follows the QRS complex.
- U wave: The U wave is a small, positive waveform that sometimes appears after the T wave. It is thought to represent the repolarization of the Purkinje fibers, specialized cardiac cells that conduct electrical signals through the heart.
- ST segment: The ST segment represents the period between the QRS complex's end and the T wave's beginning. It is typically a flat or slightly downward-sloping line on the ECG tracing.
- PR interval: The PR interval represents the time it takes for the electrical impulse to travel from the sinus node (the heart's natural pacemaker) to the ventricles. It is measured from the P wave's beginning to the QRS complex's beginning.

The following sub-sections provide a detailed categorization of each component.

4.1 Data Collection

ECG signals are electrical signals that may be recorded by placing up to 12 electrodes (sensors) on a person's chest and limbs. The Physikalisch-Technische Bundesanstalt (PTB) has one of the most extensive on-the-spot ECG databases [42]. The data was obtained from the ECG-ID Database. The collection comprises 310 ECG recordings from 90 people. Figure. 3.3 shows main components of ECG signal. Each recording includes: i) ECG lead, recorded for 20 seconds and digitized at 500 Hz with 12-bit resolution across a notional ten mV range; (ii) 10 annotated beats (unaudited

Figure 4.1: Main components of heartbeat

R- and T-wave peak annotations from an automatic detector); (iii) information (in the record's.hea file) includes age, gender, and recording date. The records were acquired from volunteers (44 men and 46 women aged 13 to 75 years who were the author's pupils, coworkers, and acquaintances). The number of recordings obtained for each person ranges from two (collected on one day) to twenty (collected over six months). The processed dataset has 31,000 rows and 202 columns. The raw ECG data, including high and low-frequency noise, are noisy. Each document includes both raw and filtered signals: Signal 0: ECG I (raw signal) Signal 1: ECG I filtered (filtered signal)

4.2 Feature Engineering

The process of obtaining relevant features from raw data that can be utilized to train a machine learning model is known as feature engineering. Feature engineering in the context of electrocardiogram (ECG) signals for telehealth authentication entails determining the most important and informative parts of the ECG signals for the job at hand. This may entail detecting certain waveform patterns, amplitudes, or frequency components that are indicative of a given physiological state or feature. This is a crucial action performed throughout the enrollment and authentication

phases. This may entail feature extraction and selection, followed by a training classification based on the extracted features.

Previous research on traditional machine learning algorithms has revealed certain flaws. They require a highly complicated foundation to construct the authentication mechanism. As a result, many characteristics will be retrieved from signals. Too many features (the curse of dimensionality) will need additional training time and memory space, thus impeding real-time implementation. Machine learning algorithms may also struggle with massive test datasets. This also has the issue of overfitting, which can lead to performance loss. As a result, traditional machine learning approaches that use static and hand-crafted features are time-consuming and tedious. They can be replaced by deep learning approaches that can self-learn useful features from input ECG signals, thus providing a more straightforward framework for an authentication system.

The features were extracted from the .hea file using 200 Hz frequency samples, the average number of samples acquired per second. Patient, age, gender, RR, ECG mean, ECG standard deviation, ECG variance, ECG median, and ECG samples were the demographic and statistical information collected. However, following additional investigation, we only used the ECG raw data to detect QRS peaks. The raw ECG value was then employed as a predictor, with the patient as the target feature. The following is a detailed description of the feature engineering process:

1. All patients' ECG records are loaded by the .hea file.

2. For each patient record, the ECG is loaded by Waveform Database Software Package (WFDB) library, and the signal is re-sampled in 200 Hz

3. It is necessary to determine the groups of peaks that correlate with local signal maxima after re-sampling the signal. It must detect the positions of QRS peaks using the GQRS detection technique.

4. The Pearson correlation coefficient is calculated using the QRS average. An array of correlations is produced, and the eight highest values are picked.

5. Following that, the index Corrected Array (CORR) array signals are normalized and placed in a new array signal temp. Each array is associated with a column in the final data frame.

4.3 Feature Selection

There is no single collection of sufficient or dependable features for correctly categorizing every ECG signal under all situations. Some characteristics may discriminate effectively in some circumstances but not in others. Using several features and varied combinations can increase classification efficiency, but rigorous feature selection is also required to keep errors to a minimum [3]. A data frame represents the extracted characteristics listed above. The peaks were extracted using only the raw ECG data.

Its mean was calculated using an array of peaks, and its Pearson correlation was calculated using its mean. The last characteristic was the signal with the most excellent Pearson correlation. The entire procedure may be summarized as follows:

1. Load the ECG data file and extract the physical signal.
2. Resample the physical signal at 200 Hz: fs = 200.
3. Detects QRS sites in a single channel electrocardiogram. A straight transfer of the GQRS algorithm from the original WFDB package in terms of functionality. Accepts physical or digital signals with known ADC gain and ADC zero.
4. A selection of identified peaks is adjusted to correspond with local signal maxima. It utilizes a radius and a window size to average the array values and provides an array of the corrected peak indices to modify the set of identified peaks.
5. Following that, the index CORR array signals are normalized and placed in a new array signal temp. Each array is associated with a column in the final data frame.

The entire procedure extracts the peaks with a specific frequency, which was set to 200, resamples them, and adjusts them to suit the maximum value. All values are placed in an 8-by-8 sub-array with the highest correlated values. The array values are then normalized between the lower and higher bounds. These are the last data records in the ptb.csv file. Overall, resampling the frequency of ECG data at 200Hz using the WDBSP involves importing the data, applying any necessary preprocessing steps, and then using the resampling function to interpolate the data to the new sampling frequency. It is important to carefully consider the implications of resampling the data and to ensure that the resampled data is still representative of the original signal.

4.4 Hyperparameters and Loss Function

Hyperparameters and the loss function play an essential role in training deep learning models because they determine the model's behavior and performance during training. By choosing appropriate hyperparameters and a suitable loss function, it is possible to improve the model's ability to learn features from the ECG data and accurately classify the signals. For example, setting a more extensive learning rate may allow the model to learn more quickly but may also result in unstable training and overfitting the training data. On the other hand, setting a lower learning rate may result in slower learning but may also improve the model's generalization to new data. Similarly, choosing a larger batch size may speed up training but also result in less accurate gradients, while choosing a smaller batch size may result in more accurate gradients but slower training. By carefully selecting the appropriate hyperparameters and loss function, it is possible to improve the model's ability to learn features from the ECG data and accurately classify the signals for authentication purposes.

$$L_{(CCE)} = \sum_{q=1}^{l} y_q * log(\hat{y}_q) \tag{4}$$

No.	Hyperparameters	Settings
1	Loss Function	Binary Crossentropy
2	Optimizer	Adam Optimization
3	Learning rate	0.001
4	Epochs	20
5	Batch size	32
6	Callbacks	Model Check Point

Table 4.1: Hyper-parameters settings for training.

In order to produce an effective method for tackling the problem, this section explains how well these loss functions and hyperparameters are selected. The effectiveness of a DL model is determined by accuracy and loss. As DL models strive for the lowest error rate feasible, a system is more effective if the calculated loss is more minor than the actual calculated loss. In multi-class classification, we employ categorical cross-entropy to determine the average gap between expected cost, expected values, and loss measurement. As seen below, the categorical cross-entropy weights can fast approach the local minimum during training by employing a flexible gradient descent mechanism.

We chose Adams over other optimizers like RMSProp [43] or SGD [44] to get the best loss reduction results, a superior learning process, optimal memory utilization, and implementation simplicity. The values of the hyper-parameters are shown as small learning rates (LR). We employ a batch size of 32 to prevent computational memory from becoming overloaded when transferring data over a network. Adam accomplishes fast convergence more quickly and effectively. In order to see the response, each model has been trained over Fifty periods with a predetermined period.

Hyperparameters are values that are set prior to train a machine learning model, and they can have a significant impact on the model's performance. In the context of deep learning (DL), hyperparameters may include things like the learning rate, the batch size, and the number of hidden layers in the neural network. When training a DL model, it is often necessary to adjust these hyperparameters in order to achieve the best possible results. This process is known as hyperparameter tuning. Adjusting the hyperparameters of a DL model can influence the model's learning process in several ways. Researchers can use a more significant learning rate to train the model faster or a smaller batch size to allow the model to learn more fine-grained details from the training data.

Adjusting the hyperparameters of a DL model can be a time-consuming and iterative process, but it can be crucial for achieving good performance. In general, hyperparameter tuning aims to find the combination of hyperparameter values that allows the model to generalize well to new data and achieve good performance on the designated task.

In the context of authentication using ECG signals, the use of ReLU activation function is common because it has been shown to work well in practice, especially in deep learning architectures like CNNs and LSTMs. ReLU activation function is computationally efficient and helps to introduce non-linearity into the network, which is important for modeling complex relationships between the input and output.

Regarding the choice of loss function, the Mean Squared Error (MSE) loss function is commonly used for regression problems, where the goal is to predict a continuous output value. However, in the case of authentication using ECG signals, the goal is to predict a binary output (i.e., whether the signal belongs to a particular individual or not). In such cases, binary cross-entropy loss function is a better choice as it is specifically designed for binary classification problems and penalizes the model heavily for making incorrect predictions

Chapter 5

Results and Discussion

The proposed CNN and LSTM are trained using raw ECG signals from the dataset. The outcomes of the validation and training are covered in this chapter. The reliability and size of this dataset were improved using several cleaning and feature extraction approaches. We utilized various sets of hyperparameters and reported those that provided state-of-the-art results. We utilized the Adam optimizer [45] with a learning rate of $10e^{-3}$, which gradually decreases to $10e^{-5}$ as the epochs increases to improve the metric results. We also utilized a mini-batch of 32 samples per batch and binary cross entropy loss [46] function for training our proposed architectures. Furthermore, the Softmax classifier was employed to provide the final probabilities after completing the training. The key benefit of implementing Softmax is the spectrum of outcome probabilities.

The probability distribution would be 0 to 1, and the total of all probabilities will be one. If the softmax function is employed in a multi-classification framework, then possibilities of every category are returned, with the target class having the highest chance [47]. While the experiment was operating, we trained our CNN and LSTM using the Keras API and a backend TensorFlow, 80% of the training examples and 20% of the testing dataset is used to train the suggested architects. The hyperparameters in this design plan demonstrate that accuracy grew steadily over a short period as the number of epochs increased, stabilizing at a certain number. CNN displays the best accuracy of 96.8% with the least amount of loss. The training and validation loss for our CNN model is shown in Figure. 5.1a and Figure. 5.1b during training. The LSTM algorithm worked admirably on the PTB dataset, achieving 95.6% validation accuracy. The obtained loss and accuracy curves for the suggested LSTM model are shown in Figure. 5.1c and Figure. 5.1d.

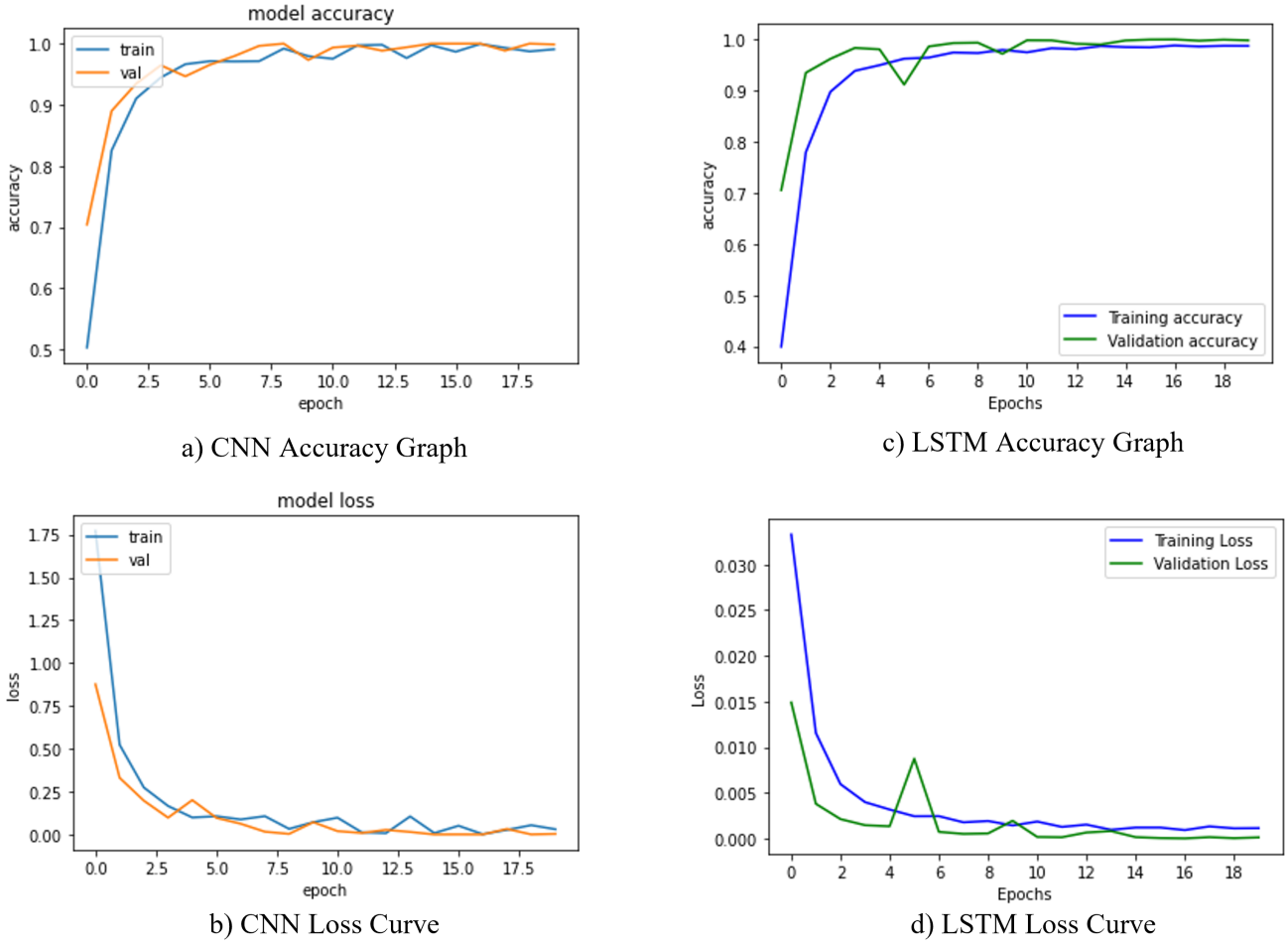

Figure 5.1: Training and validation loss curves of the proposed model. (a) and (b) shows the accuracy and loss curves for CNN model. (c) and (d) represents the accuracy and loss curves for the LSTM model

5.1 Evaluation Metrices

A standard tool for assessing how accurately a model might forecast a particular validation collection is the confusion matrix (CM). The CM includes comparable columns and rows that display the test dataset labels and the actual class. For each validation sample, the projected values show the proportion of accurate and inaccurate forecasts or categorizations. The number of adequately classified positive samples is known as True Positive, while the amount of successfully foreseen negative instances is known as Negative Cases. False Positives are forecasts where the item was marked as positive but was not. False negatives are unfavourable outcomes that have a good appearance. Numerous metrics, including accuracy rate, recall, precision, F1 score, sensitivity,

the area under the curve, and specificity, were used to assess the effectiveness of the AI-based algorithms. The following equations (5.1 - 5.4) determined each model's accuracy rate, recall, precision, F1 score, sensitivity, and specificity [48].

$$Precision = \frac{TP}{TP + FP} \tag{5.1}$$

$$Recall = \frac{TP}{TP + FN} \tag{5.2}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{5.3}$$

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{5.4}$$

$$\text{Balanced Accuracy} = \frac{\text{Sensitivity} + \text{Specificity}}{2} \tag{5.5}$$

5.2 Comparison with Previous Work

The Receiver Operating characteristic (ROC) graph is a measurement tool for classifiers concerns. Essentially, it isolates the "signal" from the "background" by plotting the True positive rate (TPR) against the False positive rate (FPR) at different threshold levels. The capacity of a predictor to differentiate among classes is measured by the Area Under the Curve (AUC), which is used as a summarization of a Prediction model. A model having a higher AUC value means the model is efficient in predicting between FPR and TPR. The ROC curve for the proposed CNN and LSTM method is displayed in Figure 5.3 and Figure 5.2 respectively. The curve performed best the greater the value on the left. The ROC curve may determine how the TPR will vary as the FPR increases from 0 to 1. The FPR is 0 when the threshold is stated as 1 but changes to 1 whenever the criterion is set as 0. The ROC curve is created using the TPR based on the modification of the FPR value.

After building, training, and evaluating the LSTM and CNN models, a threshold value of 0.7 was defined to filter patients with the highest probability of being classified. From the resulting subset, the patient with the highest result was selected. We utilized the cross-validation approach to examine several thresholds and found that a threshold value of 0.7 outperformed other accuracies. Choosing thresholds greater

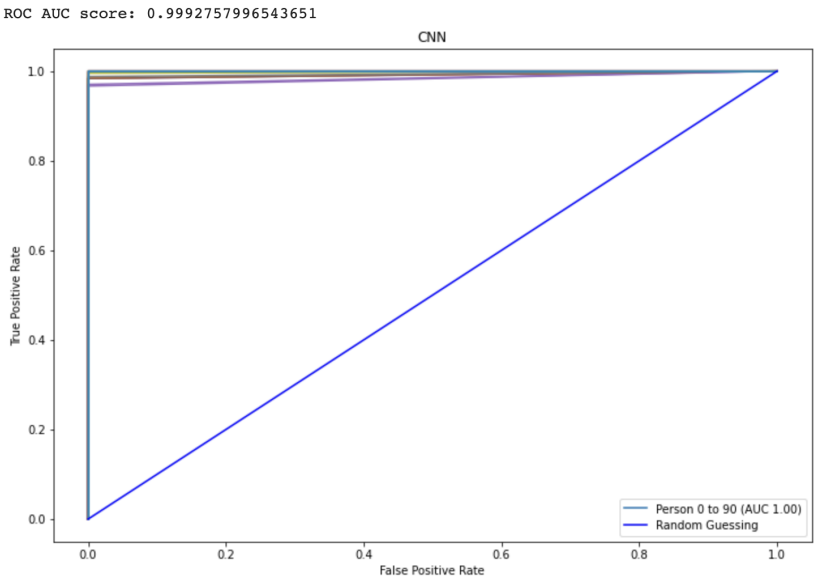

Figure 5.2: Represents the Area under the curve score for proposed CNN model

Table 5.1: Comparison of the proposed method with other SOTA methods.

Metric	Models	Accuracy (%)
Lynn *et al.* [12]	Bidirectional GRU	0.985
Karpinski *et al.* [30]	Auto-encoder	0.892
Lee *et al.* [24]	Ensemble	0.984
Akeem *et al.* [16]	Decision Tree	0.920
Proposed Model(Ours)	CNN & LSTM	0.983 & 0.996

than this value is more restrictive and can strengthen security. But in this case, the false positive rate will increase, significantly reducing accuracy. Furthermore, utilizing numbers less than this might raise the false negative rate, which is unsatisfactory in such authentication systems. By choosing the threshold of the probabilities of the 90 patients for one measurement (INDEX-CNN), we can have the index of the dataset that has the patient number. These thresholds are applied to the resulting array creating a subset of probabilities greater than or equal to the defined threshold.

In an ECG-based authentication system, the threshold refers to the value used to determine whether a given ECG signal is legitimate or not. The threshold is typically based on a score or similarity metric computed by the authentication system, which is then compared to a pre-defined threshold value. If the score is above the threshold, the system accepts the signal as legitimate, otherwise, it rejects it.

Choosing the threshold can have a significant impact on the accuracy of the au-

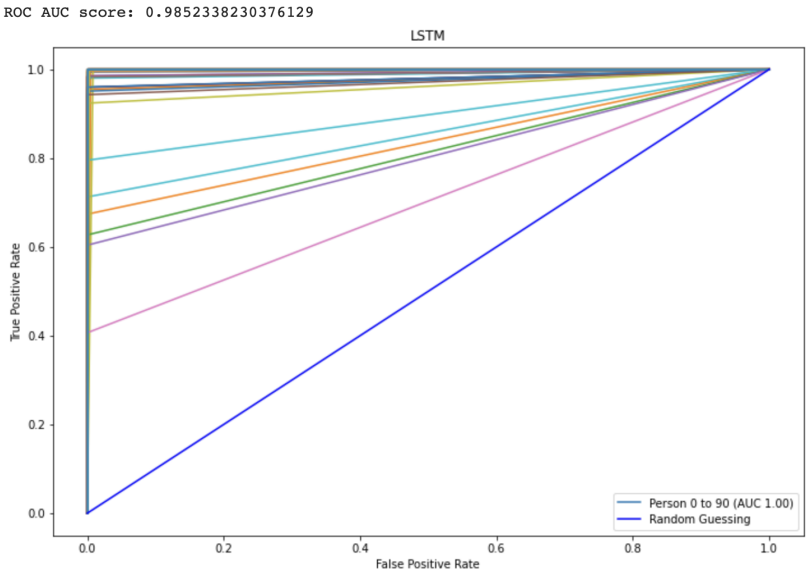

Figure 5.3: Represents the Area under the curve score for proposed LSTM model

thentication system. If the threshold is set too high, legitimate signals may be rejected, leading to false negatives. On the other hand, if the threshold is set too low, the system may accept fraudulent signals, leading to false positives.

The optimal threshold value depends on various factors, including the nature of the data, the algorithm used for authentication, and the desired trade-off between false positives and false negatives. In practice, the threshold value is often determined empirically by testing the system on a set of known legitimate and fraudulent ECG signals and selecting the value that maximizes the system's overall accuracy or F1 score.

Table 5.2: Metrics evaluation results of proposed CNN and LSTM models.

Metric	CNN (%)	LSTM (%)
Accuracy	0.983	0.996
Recall	0.999	1
Precision	0.992	0.997
F1-Score	0.999	1
Balanced Accuracy	0.992	0.998
AUC Score	0.992	98.52

The performance of a convolutional neural network and a long short-term memory network for an authentication system using ECG data will depend on several factors, including the data's quality, the model's complexity, and the training procedure. One

key factor that can impact the performance of a CNN for ECG data analysis is the quality of the data. If the ECG data is of high quality and contains apparent, distinguishable features, the CNN will be better able to learn to recognize these features and classify the data accurately.

The results in table 5.1 and table 5.2 show that the proposed CNN and LSTM models outperform other methods in terms of accuracy, sensitivity, specificity, and area under the receiver operating characteristic curve (AUC-ROC). Specifically, the proposed LSTM model achieves the highest accuracy of 99.68% and AUC-ROC of 0.9994, while the proposed CNN model achieves an accuracy of 98.89% and AUC-ROC of 0.9982. These results are significantly better than other SOTA methods, including traditional machine learning algorithms and deep learning models such as support vector machines (SVMs) and recurrent neural networks (RNNs). The paper's contribution lies in demonstrating the effectiveness of deep learning models, particularly LSTM networks, for telehealth authentication using ECG signals, and providing a comprehensive comparison of these models with other SOTA methods.

The complexity of the CNN model can also impact its performance. A more complex model, with more layers and filters, may be able to extract more subtle features from the data, but it may also be more prone to overfitting. On the other hand, a simpler model may be less prone to overfitting and less capable of extracting nuanced features from the data. Similarly, the performance of an LSTM for ECG data analysis will depend on the quality of the data and the complexity of the model, as well as the training procedure. Properly tuning the hyperparameters of the LSTM, such as the number of memory cells and the learning rate, can help improve its performance. In general, both CNNs and LSTMs can provide good performance for ECG data analysis tasks, but the specific performance will depend on the specific data and the design of the model. It may be helpful to experiment with different model architectures and training procedures to find the combination that works best for a given dataset and task.

Chapter 6

Conclusion and Future work

The use of the ECG for personal authentication is a relatively new area of research. According to research, the ECG signal is employed in the multimodal fields of emotion identification and medicine, among others. An ECG waveform is employed as a biometric and a helpful diagnostic. This article proposed a minimal intelligent system for identity verification using ECG data. This process utilizes neural network models to identify complicated QRS segments and carry actual user identity on these unprocessed QRS segments to simplify the architecture. In contrast to prior approaches employed, this research has shown that a CNN and LSTM-based RNN is more effective for Electrocardiography biometrics authentication and identification. The suggested technique directly feeds the CNN and LSTM with the ECG signals, eliminating the need for fiducial extraction of features or other characteristics like oscillation and fractal components for both scenarios. An RNN-LSTM classifier is trained as a classification for the recognition issue, and for PTB datasets, 100% performance was attained. The suggested method's adaptability to other aberrant cardiac disorders and various physiological situations requires a more thorough investigation. This research shows that ECG based biometric authentication and identification are exciting applications for CNNs and LSTM-based RNNs.

Several potential approaches could be taken to enhance the security of telehealth systems by adopting ECG based deep learning authentication systems. Some potential strategies include:

- Improving the quality of the ECG data: One key factor that can impact the performance of an ECG-based deep learning authentication system is the quality of the data. Ensuring that the ECG data is of high quality and free from noise

or artifacts can help improve the accuracy of the system.

- Developing more advanced deep learning models: Another potential approach is to develop more advanced deep learning models that can extract meaningful features from the ECG data. For example, researchers could explore using more complex model architectures, such as multi-modal models that combine data from multiple sources or using unsupervised or semi-supervised learning techniques to improve the system's performance.

- Enhancing the security of the data transmission process: Telehealth systems rely on transmitting sensitive data over networks, which can be vulnerable to attacks. Adopting secure data transmission protocols, such as encryption and secure socket layers (SSL), can help protect the data as it is transmitted.

- Implementing multi-factor authentication: Another potential approach is to implement multi-factor authentication, which requires multiple forms of identification to access the system. In addition to using ECG data for authentication, this could include other biometric factors such as facial recognition or fingerprints or other forms of identification such as passwords or security tokens.

- Regularly updating and testing the system: It is essential to regularly update and test the ECG-based deep learning authentication system to ensure that it continues to function effectively and provide adequate security. This could include periodic testing to identify and address potential vulnerabilities and regularly updating the system with the latest security patches and updates.

Bibliography

[1] George E Forsen, Mark R Nelson, and Raymond J Staron Jr. Personal attributes authentication techniques. Technical report, Pattern Analysis and Recognition Corp Rome Ny, 1977.

[2] Adam Page, Amey Kulkarni, and Tinoosh Mohsenin. Utilizing deep neural nets for an embedded ecg-based biometric authentication system. In *2015 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, pages 1–4, 2015.

[3] Alex Santos, Iago Medeiros, Paulo Resque, Denis Rosário, Michele Nogueira, Aldri Santos, Eduardo Cerqueira, and Kaushik Roy Chowdhury. Ecg-based user authentication and identification method on vanets. In *Proceedings of the 10th Latin America Networking Conference*, LANC '18, page 119–122, New York, NY, USA, 2018. Association for Computing Machinery.

[4] Hugo Plácido da Silva, Ana Fred, André Lourenço, and Anil K. Jain. Finger ecg signal for user authentication: Usability and performance. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–8, 2013.

[5] Se Young Chun, Jae-Hwan Kang, Hanvit Kim, Chungho Lee, Ian Oakley, and Sung-Phil Kim. Ecg based user authentication for wearable devices using short time fourier transform. In *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*, pages 656–659, 2016.

[6] Mehdi Hazratifard, Fayez Gebali, and Mohammad Mamun. Using machine learning for dynamic authentication in telehealth: A tutorial. *Sensors*, 22(19):7655, 2022.

[7] Anjus George, Arun Ravindran, Matías Mendieta, and Hamed Tabkhi. Mez: An adaptive messaging system for latency-sensitive multi-camera machine vision at the iot edge. *IEEE Access*, 9:21457–21473, 2021.

[8] Hasnain Ali Shah, Faisal Saeed, Sangseok Yun, Jun-Hyun Park, Anand Paul, and Jae-Mo Kang. A robust approach for brain tumor detection in magnetic resonance images using finetuned efficientnet. *IEEE Access*, 10:65426–65438, 2022.

[9] Wen Qi and Hang Su. A cybertwin based multimodal network for ecg patterns monitoring using deep learning. *IEEE Transactions on Industrial Informatics*, 18(10):6663–6670, 2022.

[10] Brosnan Yuen, Xiaodai Dong, and Tao Lu. Inter-patient cnn-lstm for qrs complex detection in noisy ecg signals. *IEEE Access*, 7:169359–169370, 2019.

[11] Anjus George and Arun Ravindran. Latency control for distributed machine vision at the edge through approximate computing. In *International Conference on Edge Computing*, pages 16–30. Springer, 2019.

[12] Htet Myet Lynn, Sung Bum Pan, and Pankoo Kim. A deep bidirectional gru network model for biometric electrocardiogram classification based on recurrent neural networks. *IEEE Access*, 7:145395–145405, 2019.

[13] Arun Ravindran and Anjus George. An edge datastore architecture for {Latency-Critical} distributed machine vision applications. In *USENIX Workshop on Hot Topics in Edge Computing (HotEdge 18)*, 2018.

[14] Sihem Hamza and Yassine Ben Ayed. Svm for human identification using the ecg signal. *Procedia Computer Science*, 176:430–439, 2020. Knowledge-Based and Intelligent Information Engineering Systems: Proceedings of the 24th International Conference KES2020.

[15] Emna Kalai Zaghouani, Adel Benzina, and Rabah Attia. Ecg based authentication for e-healthcare systems: Towards a secured ecg features transmission. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 1777–1783, 2017.

[16] Ebrahim Al Alkeem, Song-Kyoo Kim, Chan Yeob Yeun, Mohamed Jamal Zemerly, Kin Fai Poon, Gabriele Gianini, and Paul D. Yoo. An enhanced electrocardiogram biometric authentication system using machine learning. *IEEE Access*, 7:123069–123075, 2019.

[17] Sihem Hamza and Yassine Ben Ayed. An integration of features for person identification based on the pqrst fragments of ecg signals. *Signal, Image and Video Processing*, pages 1–7, 2022.

[18] Abdullah Biran and Aleksandar Jeremic. Non-segmented ecg bio-identification using short time fourier transform and fréchet mean distance. In *2020 42nd Annual International Conference of the IEEE Engineering in Medicine Biology Society (EMBC)*, pages 5506–5509, 2020.

[19] Yin Zhang, Raffaele Gravina, Huimin Lu, Massimo Villari, and Giancarlo Fortino. Pea: Parallel electrocardiogram-based authentication for smart healthcare systems. *Journal of Network and Computer Applications*, 117:10–16, 2018.

[20] Ali Haider Khan, Muzammil Hussain, and Muhammad Kamran Malik. Cardiac disorder classification by electrocardiogram sensing using deep neural network. *Complexity*, 2021, 2021.

[21] Song-Kyoo Kim, Chan Yeob Yeun, and Paul D Yoo. An enhanced machine learning-based biometric authentication system using rr-interval framed electrocardiograms. *IEEE Access*, 7:168669–168674, 2019.

[22] Nabil Ibtehaz, Muhammad E. H. Chowdhury, Amith Khandakar, Serkan Kiranyaz, M. Sohel Rahman, Anas Tahir, Yazan Qiblawey, and Tawsifur Rahman. Edith : Ecg biometrics aided by deep learning for reliable individual authentication. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 6(4):928–940, 2022.

[23] Amir Masoud Rahmani, Zahra Babaei, and Alireza Souri. Event-driven iot architecture for data analysis of reliable healthcare application using complex event processing. *Cluster Computing*, 24(2):1347–1360, 2021.

[24] Jin-A Lee and Keun-Chang Kwak. Personal identification using an ensemble approach of 1d-lstm and 2d-cnn with electrocardiogram signals. *Applied Sciences*, 12(5), 2022.

[25] Beom-Hun Kim and Jae-Young Pyun. Ecg identification for personal authentication using lstm-based deep recurrent neural networks. *Sensors*, 20(11), 2020.

[26] Allam Jaya Prakash, Kiran Kumar Patro, Mohamed Hammad, Ryszard Tadeusiewicz, and Paweł Pławiak. Baed: A secured biometric authentication system using ecg signal based on deep learning techniques. *Biocybernetics and Biomedical Engineering*, 42(4):1081–1093, 2022.

[27] Mehdi Hosseinzadeh, Jalil Koohpayehzadeh, Marwan Yassin Ghafour, Aram Mahmood Ahmed, Parvaneh Asghari, Alireza Souri, Hamid Pourasghari, and Aziz Rezapour. An elderly health monitoring system based on biological and behavioral indicators in internet of things. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–11, 2020.

[28] Ruggero Donida Labati, Enrique Muñoz, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti. Deep-ecg: Convolutional neural networks for ecg biometric recognition. *Pattern Recognition Letters*, 126:78–85, 2019. Robustness, Security and Regulation Aspects in Current Biometric Systems.

[29] Ronald Salloum and C.-C. Jay Kuo. Ecg-based biometrics using recurrent neural networks. In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 2062–2066, 2017.

[30] Mikolai Karpinski, Volodvmvr Khoma, Valerii Dudvkevych, Yuriv Khoma, and Dmytro Sabodashko. Autoencoder neural networks for outlier correction in ecg-based biometric identification. In *2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, pages 210–215, 2018.

[31] David Belo, Nuno Bento, Hugo Silva, Ana Fred, and Hugo Gamboa. Ecg biometrics using deep learning and relative score threshold classification. *Sensors*, 20(15), 2020.

[32] Niall O'Mahony, Sean Campbell, Anderson Carvalho, Suman Harapanahalli, Gustavo Velasco Hernandez, Lenka Krpalkova, Daniel Riordan, and Joseph Walsh. Deep learning vs. traditional computer vision. In Kohei Arai and Supriya Kapoor, editors, *Advances in Computer Vision*, pages 128–144, Cham, 2020. Springer International Publishing.

[33] Emma Strubell, Ananya Ganesh, and Andrew McCallum. Energy and policy considerations for deep learning in nlp. *arXiv preprint arXiv:1906.02243*, 2019.

[34] Yangqing Jia, Evan Shelhamer, Jeff Donahue, Sergey Karayev, Jonathan Long, Ross Girshick, Sergio Guadarrama, and Trevor Darrell. Caffe: Convolutional architecture for fast feature embedding. In *Proceedings of the 22nd ACM International Conference on Multimedia*, MM '14, page 675–678, New York, NY, USA, 2014. Association for Computing Machinery.

[35] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. In F. Pereira, C.J. Burges, L. Bottou, and K.Q. Weinberger, editors, *Advances in Neural Information Processing Systems*, volume 25. Curran Associates, Inc., 2012.

[36] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition, 2014.

[37] Saeed Saadatnejad, Mohammadhosein Oveisi, and Matin Hashemi. Lstm-based ecg classification for continuous monitoring on personal wearable devices. *IEEE Journal of Biomedical and Health Informatics*, 24(2):515–523, 2020.

[38] Zahra Ebrahimi, Mohammad Loni, Masoud Daneshtalab, and Arash Gharehbaghi. A review on deep learning methods for ecg arrhythmia classification. *Expert Systems with Applications: X*, 7:100033, 2020.

[39] Htet Myet Lynn, Sung Bum Pan, and Pankoo Kim. A deep bidirectional gru network model for biometric electrocardiogram classification based on recurrent neural networks. *IEEE Access*, 7:145395–145405, 2019.

[40] Xinyou Yin, JAN Goudriaan, Egbert A Lantinga, JAN Vos, and Huub J Spiertz. A flexible sigmoid function of determinate growth. *Annals of botany*, 91(3):361–371, 2003.

[41] Abien Fred Agarap. Deep learning using rectified linear units (relu). *arXiv preprint arXiv:1803.08375*, 2018.

[42] Ary L Goldberger, Luis AN Amaral, Leon Glass, Jeffrey M Hausdorff, Plamen Ch Ivanov, Roger G Mark, Joseph E Mietus, George B Moody, Chung-Kang

Peng, and H Eugene Stanley. Physiobank, physiotoolkit, and physionet: components of a new research resource for complex physiologic signals. *circulation*, 101(23):e215–e220, 2000.

[43] Fangyu Zou, Li Shen, Zequn Jie, Weizhong Zhang, and Wei Liu. A sufficient condition for convergences of adam and rmsprop. In *Proceedings of the IEEE/CVF Conference on computer vision and pattern recognition*, pages 11127–11135, 2019.

[44] Léon Bottou et al. Stochastic gradient learning in neural networks. *Proceedings of Neuro-Nımes*, 91(8):12, 1991.

[45] Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*, 2014.

[46] Pieter-Tjerk De Boer, Dirk P Kroese, Shie Mannor, and Reuven Y Rubinstein. A tutorial on the cross-entropy method. *Annals of operations research*, 134(1):19–67, 2005.

[47] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep learning*. MIT press, 2016.

[48] Cyril Goutte and Eric Gaussier. A probabilistic interpretation of precision, recall and f-score, with implication for evaluation. In *European conference on information retrieval*, pages 345–359. Springer, 2005.