TED UNIVERSITY

CMPE 491-O

Senior Project I

Detection of AI-Generated ECG Signals

High Level Design Report

Team Members:

Ekrem Elbasan - 10756169050

Eren Tuncer - 12386887182

Ata Yiğit Apaydın - 3570175055

Contents

1. Introduction....2
1.1 Purpose of the system....2
1.2 Design goals....3
1.3 Definitions, acronyms, and abbreviations....3
1.4 Overview....3
2. Proposed software architecture....3
2.1 Overview....3
2.2 Subsystem decomposition....4
2.3 Hardware/software mapping....4
2.4 Access control and security....6
2.5 Boundary conditions....6
3. Glossary....7

1. Introduction

1.1 Purpose of the system

In the future, as biometric authentication systems become more widespread, there will always be adversaries attempting to compromise the authentication process. Our proposed

system PulsePrint, aims to address this challenge by detecting and distinguishing between authentic and synthetic ECG signals. The results of this detection will play a crucial role in enhancing the security of biometric authentication.

1.2 Design goals

The main focus of the project is to ensure the robust, secure and efficient solution to the threat possessed by the AI generated ECG signals against modern authentication systems. This solution will eventually mitigate the risk of these authentication systems and eventually will maintain trust in biometric systems.

1. Accuracy and Reliability: The system should be able to distinguish between real and fake AI generated signals with high accuracy. This is critical in terms of maintaining trust in biometric systems.
2. Real-Time Processing: The system shall process ECG signals efficiently to respond to real-time applications with necessary agility. Low latency is essential for certain use cases such as biometric authentication during secure access.
3. Scalability: The architecture must be scalable enough to accommodate future developments, which may be necessary in order to handle increasing volumes of requests from varying third parties.
4. Security: Ensuring the security of ECG data is the top priority for the project. The system will implement necessary encryption algorithms.

1.3 Definitions, acronyms, and abbreviations

1.4 Overview

PulsePrint is designed to find efficient solutions to distinguish between authentic and AI generated synthetic ECG signals. By training our model on AI generated ECG signals data created from AI-models fed with authentic data we aim to achieve reliable authentication service and accurate distinction between real and synthetic data.

2. Proposed software architecture

2.1 Overview

PulsePrint is designed to provide an efficient solution to distinguish between authentic and synthetic ECG data. The architecture consists of different subsystems that provide accuracy, reliability, and authentication.

The key components of the system are:

Signal Preprocessing: The ECG data is cleaned and preprocessed to ensure it is suitable for training the machine learning model.

Machine Learning: The AI model that will be trained using the preprocessed ECG data.

API: The API will provide the necessary ECG data.

2.2 Subsystem decomposition

There are five subsystems in PulsePrint. These are input management, signal processing, classification, results and security systems. These subsystems have their own responsibilities and tools they interact with the whole.

Input management interacts with the ECG devices and collects the data for usage in the PulsePrint. These are then transferred to the processing system by an API.

Processing System receives the data and stores it in a way that can be used easily with its own applications like data matrices or data frames. Then data is removed of noise, normalized and the best features are selected to fit our trained model.

After data is processed, it is sent to classification model to check if its synthetic or genuine ECG signal. By comparing the hidden patterns in real data with artifacts in the synthetic ones PulsePrint model can classify it accurately. This result is sent back to the relevant apps for validation purposes by the result management susbsytem.

The security system ensures that heartbeat data is secure and private. Only users with relevant authority can access the API and data is encrypted so that personal information is not leaked during the process. All the actions are logged for security purposes

Subsystem	Responsibilities	Tools/Tech Stack	Interfaces
Input Management	Collect ECG data from devices, forward to processing	API, Client SDKs	REST API
Signal Processing	Clean, normalize, and extract features	SciPy, NumPy	Internal
AI Classification	Classify ECG as authentic or synthetic	TensorFlow, PyTorch	Internal
Result Management	Return classification results to users/apps	Flask, Spring Boot	REST API
Security	Encrypt data, manage access, log activities	Homomorphic encryption libraries	All interactions

Table 1: Subsystem information

2.3 Hardware/software mapping

Hardware Resources

1. Computation (Servers and Cloud infrastructure)

   a. Purpose: It is necessary for both training and prediction.
   b. Usage:
      i. CPU: Handles signal processing when necessary
      ii. GPU: For running deep neural networks models (e.g., using Tensorflow, PyTorch) for ECG classification, where parallel processing is required.
      iii. Memory: Sufficient RAM is required in order to store and process ECG signals.
2. Client Devices (ECG Collection Devices)
   a. Purpose: Devices like wearable ECG monitors, hospital equipment, or mobile devices that collect ECG signals.
   b. Usage: Sends the ECG data to the system via an API or data upload mechanism.

Software Resources

1. API Management Software (REST API)
   a. Purpose: Exposes the API that allows third-party applications (e.g., healthcare or authentication services) to send ECG data for analysis.
   b. Usage:
      i. API Gateway: Routes requests from clients to the backend.
      ii. REST API: Developed with web frameworks (e.g., Spring Boot, Flask) to receive ECG data and send responses (such as prediction results and confidence scores).
2. Signal Preprocessing Software
   a. Purpose: Handles the preprocessing of incoming ECG signals, such as noise filtering, normalization, and segmentation.
   b. Usage:
   c. Preprocessing Libraries: Libraries (e.g., SciPy, NumPy) that perform signal cleaning, artifact removal, and feature extraction (e.g., heart rate variability, ECG morphology).
3. ML model
   a. Purpose: Executes AI models to classify ECG signals as either genuine or AI-generated.
   b. Usage:

i. AI: A trained machine learning model (e.g., neural network) built using frameworks like TensorFlow or PyTorch.
ii. Inference Framework: Software that takes incoming ECG data and passes it through the model to generate predictions.
iii. Model Management: Ensures the proper versioning, updating, and serving of AI models (e.g., using tools like MLflow or TensorFlow Serving).

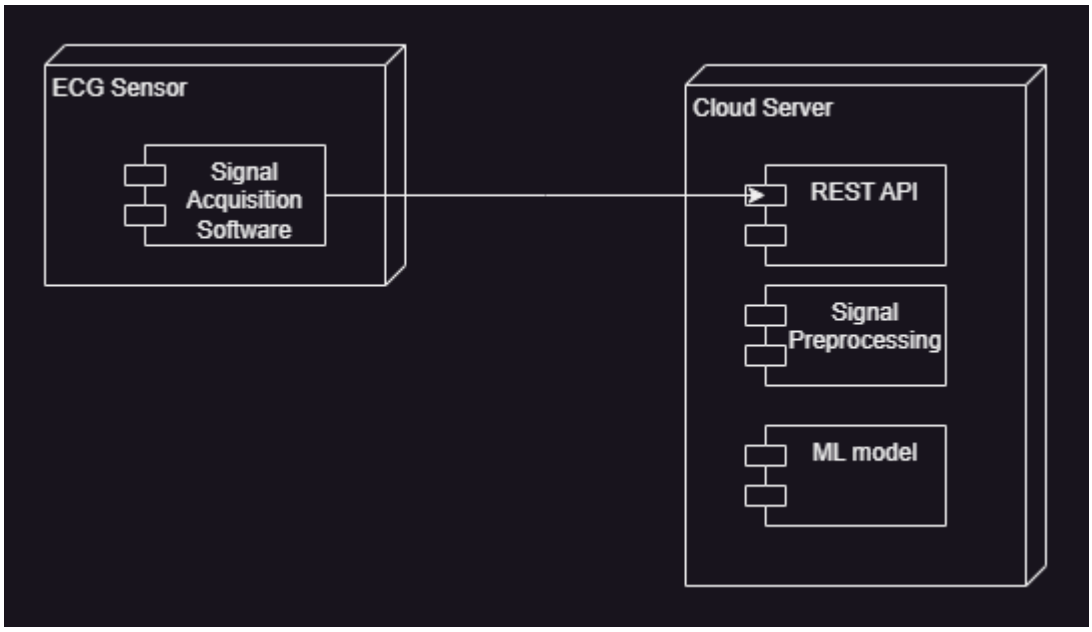

Figure 1: High-Level System Architecture of PulsePrint

2.4 Access control and security

The following measures are implemented in order to provide access control and security:

• **Data Encryption:** The ECG data is highly sensitive and must be protected. Homomorphic encryption will be employed to ensure that the data remains confidential while still enabling processing and analysis without exposing the raw data.

• **Audit Logging**: User activities will be logged in order to detect any unauthorized access.

• **Data Anonymity:** Data is anonymized to ensure privacy in compliance with regulations GDPR and HIPAA.

2.5 Boundary conditions

Unpredictable ECG signal due to heart problems

Users who have heart-related problems may have unpredictable ECG patterns and therefore these signals may possess certain challenges for our project. It may significantly affect our system's ability to distinguish genuine and AI generated signals with high confidence.

Challenges:

- Increased False Positives: Unpredictable signals might mimic characteristics of AI-generated data, leading to incorrect classifications.
- The variability of the signals may cause low confidence scores which may affect reliability.

We may exclude from the dataset ECG signals that come from people with health conditions. If the system can't classify a signal with high confidence, it may send an alert indicating that the result is uncertain.

3. Glossary

Term	Definition
API (application programming interface)	Connection interface that allows us to send data
Biometric Authentication	Security process that identifies with unique biological features.
ECG (Electrocardiogram)	A recording of electrical activity of heart
False Positive	Data incorrectly classified to be positive by the system
Machine Learning (ML)	Field of ai that aims to make models learn and make predictions

GDPR (General Data Protection Regulation)	European Union regulation designed to protect personal data and privacy
Synthetic Data	Artificially generated data that mimics real data.
TensorFlow	Framework for building and training AI models.
Preprocessing	Cleaning and preparing raw ECG data for model training