TED UNIVERSITY

CMPE 491-O

Senior Project I

Detection of AI-Generated ECG Signals

Analysis Report

Team Members:

Ekrem Elbasan - 10756169050

Eren Tuncer - 12386887182

Ata Yiğit Apaydın - 35701750558

Contents

1. Introduction

Recent bioinformatics developments show that heartbeat signals for each individual are different enough from each other that it can be used to identification like fingerprints. Therefore, counterfeit or AI generated ECG [see *ECG*] signals possesses great threat to platforms that may use ECG signal as the credentials to authenticate or authorize in the future. Our solution for this problem involves a machine learning models to detect between fake and authentic ECG signals with high accuracy and precision increasing the safety of bio-authentication systems.

For the detection of fake signals, first we will create a dataset of fake signals generated by Generative AI models such as GAN [see *GAN*] trained on real ECG signal data collected. This dataset will be trained together with the genuine heartbeat signals will be the main source of data that will be used in our machine learning models. Training will be done on multiple types of supervised algorithms and best performing algorithm will be chosen for the final product.

To demonstrate the product, we will develop a prototype app that will showcase our model's ability to detect AI generated ECG signals. Main program will be reached with a call to our API and app will be the proof of concept that allows us to present functionalities and performance of our system.

2. Proposed system

2.1 Overview

2.2 Functional Requirements

1. **ECG Signal Submission:**
    a. Users should be able to send ECG signal data via a REST API endpoint.
    b. Users should be able to send the sample rate as metadata along with the ECG signal data.
    c. The API shall be able to ECG signals in binary .txt format for processing.
2. **Prediction:**
    a. The application shall process submitted ECG signals and distinguish between AI-generated and genuine signals using a trained machine learning model.
    b. Prediction results shall be provided with a confidence score between 0% and 100%, indicating the certainty of the prediction.
3. **API Response:**
    a. The API must return detailed responses, including:
        i. prediction outcome
        ii. confidence score
        iii. processing time
        iv. timestamp

2.3 Nonfunctional Requirements

1. **Performance**
    a. The system shall be able to process up to 50 requests simultaneously.
    b. The system shall be able to process 15 seconds of ECG signal data within 5 seconds.
2. **Accuracy**
    a. The machine learning model shall achieve at least 95% accuracy and precision in distinguishing between AI-generated and genuine ECG signals.
3. **Reliability**
    a. System should be available for users with 99% percent uptime in a 30-day period.
    b. The system should be able to handle errors, such as incorrect data upload or models being overloaded, without interrupting the rest of the working system by sending the correct HTTP error codes.
    c. Prediction models and the API will be backed up regularly to ensure availability during server failures and model downtime.
4. **Security**

   a. The model must use Homomorphic Encryption in order to guarantee computations can be performed on encrypted data without exposing underlying algorithm or data, providing protection against reverse engineering.

5. **Maintainability**
   a. Clear API documentation must be provided to users. The system should be easy to implement on other platforms.
   b. Modular design should be used for ease of development and future updates
6. **Scalability**
   a. As the number of ECG data increases, the model will be updated with the new data.
   b. The application can be deployed to new cloud instances, scaling to accommodate an increased user base.

2.4 Pseudo requirements

- **Compliance with standards:**
  The application must comply with HIPAA[2] for handling PHI.
  The application also must comply with GDPR for protection and privacy of personal data.
- **Deployment restrictions**:
  The system must be accessed via Google Cloud.

2.5 System models

2.5.1 Scenarios

Customers want additional security in their system. Uses ECG verification for this problem and uses our model for validation.

ECG Signal Submission

1. A user [see *Note*] sends an ECG signal to the API along with metadata specifying a sample rate of 500 Hz in binary .txt format.
2. A user sends wrong format or corrupted binary file which does not contain valid ECG signal data. The API detects the error and returns an appropriate HTTP error code, informing the user of the incorrect data format.
3. A user sends ECG signal data without including the sample rate as metadata. The API returns an error code indicating that required metadata is missing.

Note: *By the **user** it means the user who interacts with any authentication system which uses ECG signals to authenticate the user. The given user doesn't **directly** interact with the proposed system but rather actuates the proposed system through the authentication systems. Authentication services can interact with the proposed system.*

2.5.2 Use case model

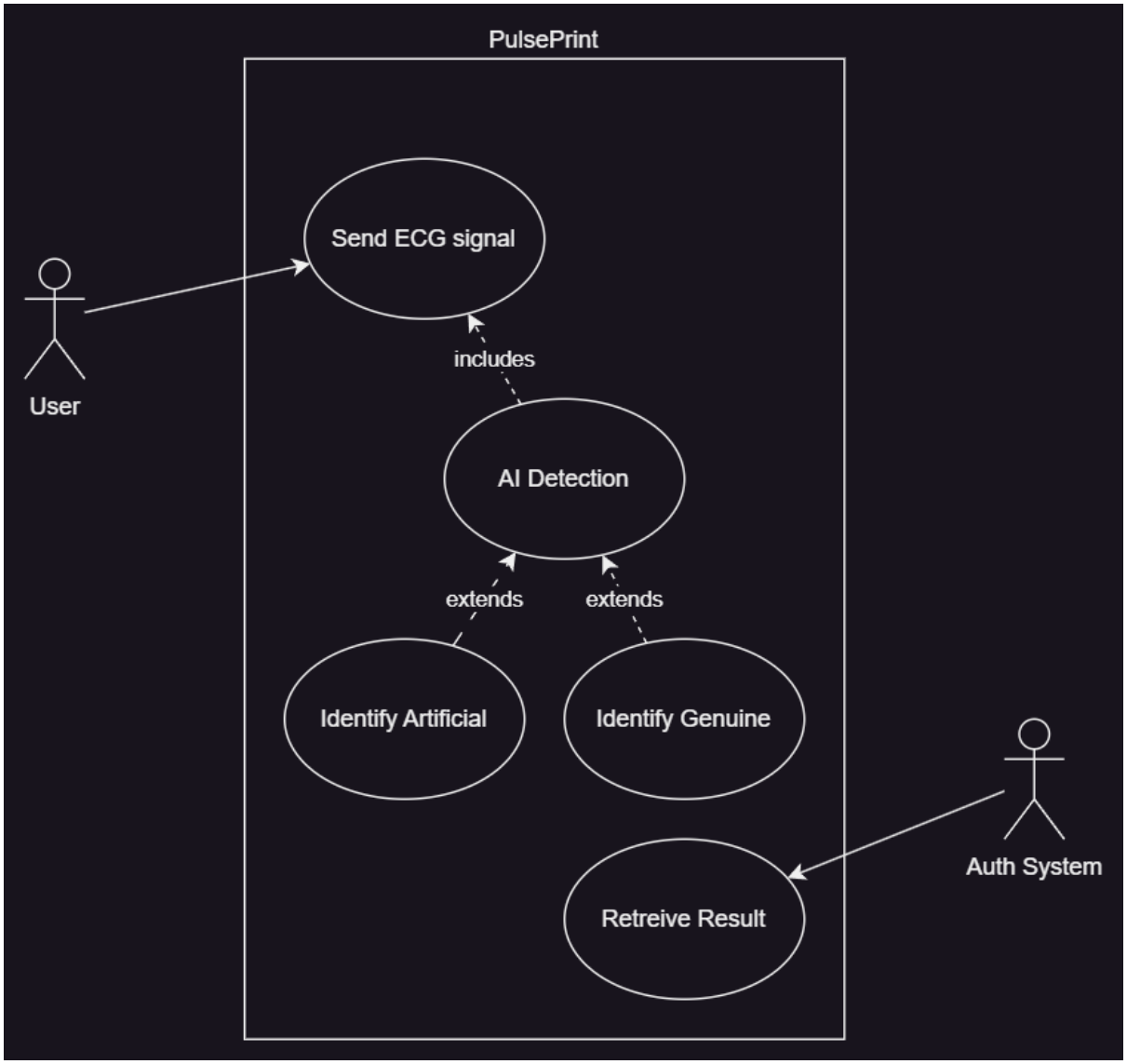

Diagram 1: Use Case Diagram

2.5.3 Dynamic models

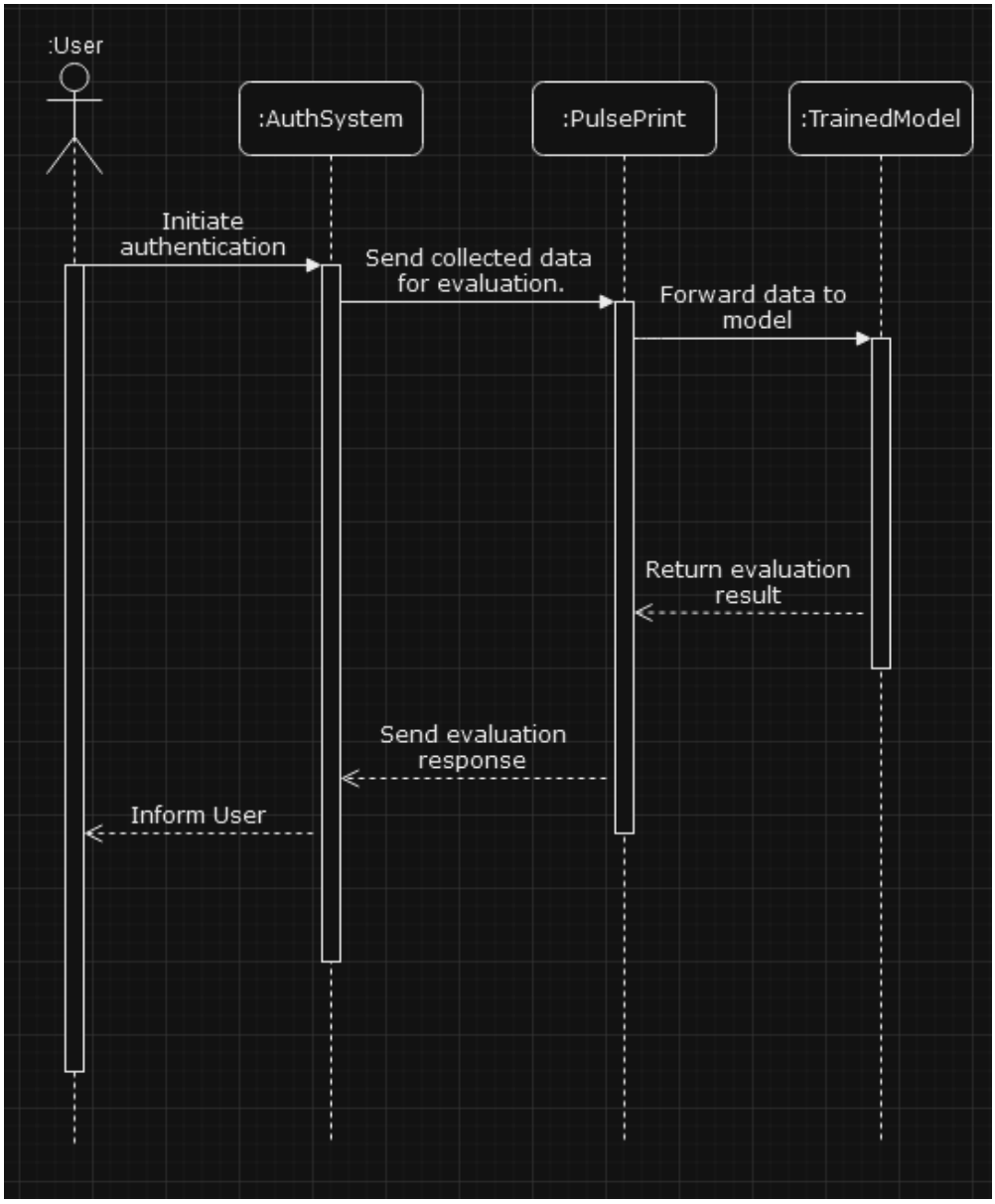

Diagram 2: Sequence Diagram

3. Glossary

ECG: Electrocardiogram is a test that records the electrical activity of the heart, including the rate and rhythm. [1]

GAN: Generative adversarial networks

AuthSystem: An authentication system which uses PulsePrint [see *PulsePrint*].

PulsePrint: Name of the proposed system. It is an API service which detects whether given ECG signals AI generated or not.

HIPAA: Health Insurance Portability and Accountability Act

PHI: Protected Health Information

GDPR: General Data Protection Regulation

4. References

1. *NHS. (2023, November 9). Electrocardiogram (ECG). NHS choices. https://www.nhs.uk/conditions/electrocardiogram/*
2. 45 CFR 164.312 -- Technical safeguards. (2024). Ecfr.gov. https://www.ecfr.gov/current/title-45/part-164/section-164.312#p-164.312(a)(2)(iv)