MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

University of Cyprus

HUMAN-CENTERED INTELLIGENT USER INTERFACES - MAI648

Marios Belk

2022

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Intelligent Biometrics

CONTENTS

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Learning Outcomes

- Know definitions in intelligent biometrics
- List the main categories of intelligent biometrics
- Understand opportunities and challenges of designing intelligent user interfaces in biometric technologies

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

What are biometrics?

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

What are biometrics?

- *ISO/IEC 2382-37 definition: ”automated recognition of individuals based on their biological and behavioural characteristics”*

- *Wikipedia: “Biometrics are body measurements and calculations related to human characteristics”*

“Information technology — Vocabulary — Part 37: Biometrics,” standard, International Organization for Standardization, Geneva, CH, 2012.
https://en.wikipedia.org/wiki/Biometrics

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Biometric identifiers

- Distinctive, measurable characteristics used to label and describe individuals

- **Types of biometrics**
  - Physiological characteristics
  - Behavioral characteristics

https://en.wikipedia.org/wiki/Biometrics

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Physiological characteristics

- Characteristics of the human body
- *Examples:*
  - Fingerprint
  - Face
  - DNA
  - Palm print
  - Hand geometry
  - Iris

https://en.wikipedia.org/wiki/Biometrics

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Behavioral characteristics

- Patterns of human behavior
- *Examples:*
  - Mouse movement
  - Typing rhythm
  - Gait
  - Signature
  - Behavioral profiling

https://en.wikipedia.org/wiki/Biometrics

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

What are intelligent biometrics?

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

What are intelligent biometrics?

- Mechanisms and techniques using artificial intelligence aiming to identify, recognize, and/or authenticate individuals based on the analysis of their physiological and/or behavioral biometric characteristics

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Intelligent biometrics

- Intelligent biometrics are used as a form of identification and access control
- Users provide information about what they are, *e.g.*, face data, voice data, fingerprint data, behavioral data to authenticate, make payments, etc.
- Increased convenience and user experience

https://www.ey.com/en_gl/digital/how-biometrics-could-finally-replace-pins-and-passwords-when-we

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Examples of intelligent biometrics

- Biometric identification and authentication for user identification and access control
  - Apple Face ID for unlocking smartphones
  - Fingerprint technology on laptops, smartphones, etc.
- Continuous user identification
  - Behavioral analysis based on users' smartphone usage
- Surveillance

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

TRUSTID Project

- Intelligent and Continuous Online Student Identity Management for Improving Security and Trust in European Higher Education Institutions

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

TRUSTID Overview

- Part of the actions of Erasmus+ 2020 and in particular the Call *"Strategic Partnerships in **Response to the COVID-19 Situation**: Partnerships for Digital Education Readiness in the field of Higher Education (KA226)"*
- *Duration:* June 2021 - May 2023 (**24 Months**)
- Currently pursuing **Month 13** of the project

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Project Partners

- Department of Electrical and Computer Engineering, University of Patras, Patras, Greece *(Project Coordinator)*
- Department of Computer Science, University of Cyprus, Nicosia, Cyprus *(Project Partner)*
- Institute of Systems and Robotics, University of Coimbra, Coimbra, Portugal *(Project Partner)*
- Cognitive UX GmbH, Heidelberg, Germany *(Project Partner)*

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Covid-19 outbreak: Problem and Challenges in HEI's

- **Before** the **Covid-19 outbreak many HEI's followed a blended learning educational model**

Ambiguities

Environment
Physical and Digital

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Covid-19 outbreak: Problem and Challenges in HEI's

- **Challenges**
  - **Continuously and seamlessly identify students while preserving their privacy and** without interrupting or interfering with the current learning activities of each HEI
  - **Provide insights to instructors** in order to take informed decisions for their classes and attendees
  - **Provide alternative integration capabilities and modes** of TRUSTID in order to better adapt to specific requirements of each HEI

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

TRUSTID Vision

Design, develop and evaluate a **multi-tier continuous student identification framework**, bootstrapped to HEIs' needs, that will consist of state-of-the-art **intelligent image, voice and interaction data** processing **while preserving their privacy**

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Core Objectives

- **Literature review** on current practices and procedures related to student identity management of EU HEIs and **triangulate findings** with stakeholders' studies at the participating HEIs
- **Design and develop an integrated framework** for student identity management
- Validate the solution through a **User-Centered Design (UCD) methodology**; two formative studies are planned, during the software development process; and one summative study is planned, after the final release of the software

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Core Objectives

- Create a **repository** that will support **knowledge building**
- **Dissemination and exploitation** activities – *research papers, workshops, seminars, LTTAs, etc.*

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Intellectual Outputs

- **Intellectual Output 1:** Analysis & validation of the TRUSTID framework for HEIs' continuous student identity management *(**Conceptual**)*
- **Intellectual Output 2:** Implementation of an open-source software toolkit *(**Operational**)*
- **Intellectual Output 3:** Evaluation and validation reports in the context of three case-studies at different HEIs *(**Lessons Learned and Guidelines**)*
- **Intellectual Output 4:** Knowledge building online community and repository *(**Sustainability**)*

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Needs Analysis and Design of the Theoretical Framework for Intelligent and Continuous Student Identity Management

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Needs Verification at HEIs

- Aims
  - Verify the needs analysis with the active involvement of the participating HEIs
  - Identify the current authentication and identity management practices and their drawbacks within the online/distance learning domain
- Conduct a series of semi-structured interviews with stakeholders with the university partners
- Sample: 31 stakeholders participated from all partner HEIs

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Needs Verification at HEIs

- Three-phase methodology
  - Phase A: Needs Analysis
  - Phase B: Needs Verification Analysis
  - Phase C: Countermeasures and Features

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Deployed tools of HEIs during critical academic activities

- In-house developed LMS systems
- Nation-wide developed LMS systems
- Off-the-shelf (e.g., Moodle) LMS systems
- LMS have been used during the COVID-19 period, adapted to the current situation

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Deployed tools of HEIs during critical academic activities

- All universities have a common pattern for student identification purposes
  - Tools for conducting meetings are used for student identification purposes, *e.g.*, Zoom, Microsoft Teams, etc.

- Identified three main type of examinations
  - Oral
  - Written online
  - Written hardcopy

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Threat Scenarios in Online Academic Activities within Existing Learning Management Systems

Phases in an Online Examination

Student Identity Verification

Examination Session

Threat Scenarios

- **Impersonation activities**, refer to actions of a person imitating or replicating the behavior or actions of another person.
- These scenarios can happen **during the student identification phase** or even **throughout the examination session**, *e.g.*, subject fakes his/her identity proofs during enrolment

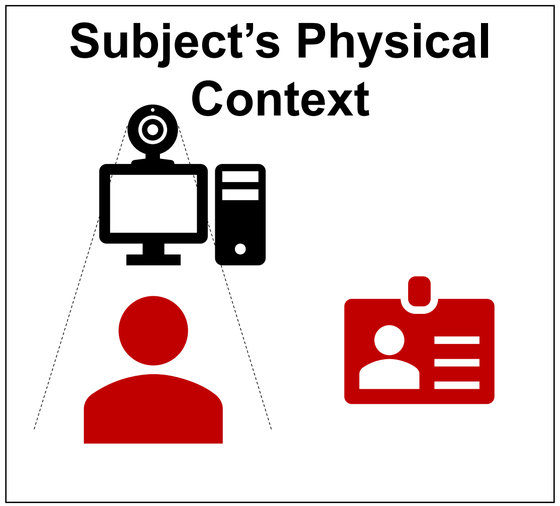
- **Forbidden collaboration and/or communication scenarios with other persons**, either within the physical or remote context
  - **In-situ** collaboration activities: related to suspicious activities that take place in the subject's physical context
  - **Computer mediated** collaboration activities: related to suspicious activities that involve remote collaboration and/or communication with other persons
- **Forbidden access to material**, either within the physical or remote context

Co-financed by the European Union
Connecting Europe Facility

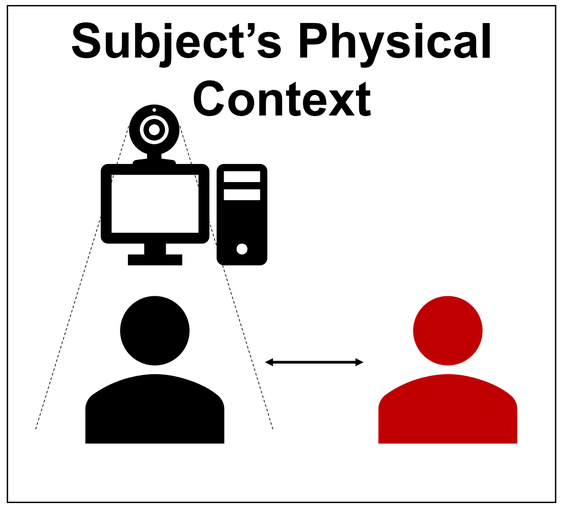
This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

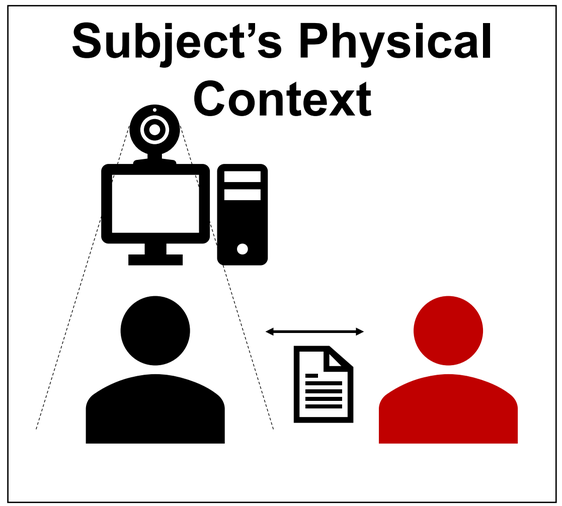
Identification of Impersonation Threat Scenarios



Subject fakes his/her identity proofs during enrolment



Subject switches seats with another person after enrolment



Exchange of hardcopy written messages

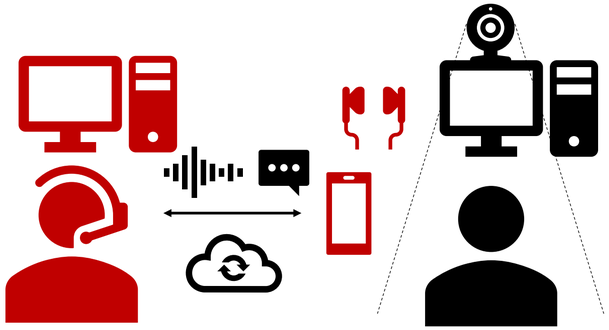
Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

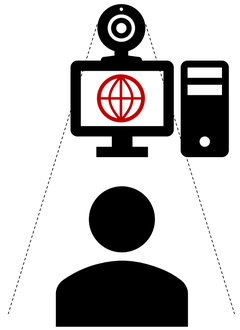
CONTENT 9

Identification of Communication, Collaboration and Resource Access Threat Scenarios

- Computer Mediated Scenarios



Remote communication/collaboration between a smartphone or another computer of the subject and another remote computer
B_1: *Communication through voice or chat*
B_2: *Collaboration through mobile application (e.g., remote desktop connection)*



Subject seeks for help from online resources, search engines, which are not allowed based on the examination policy

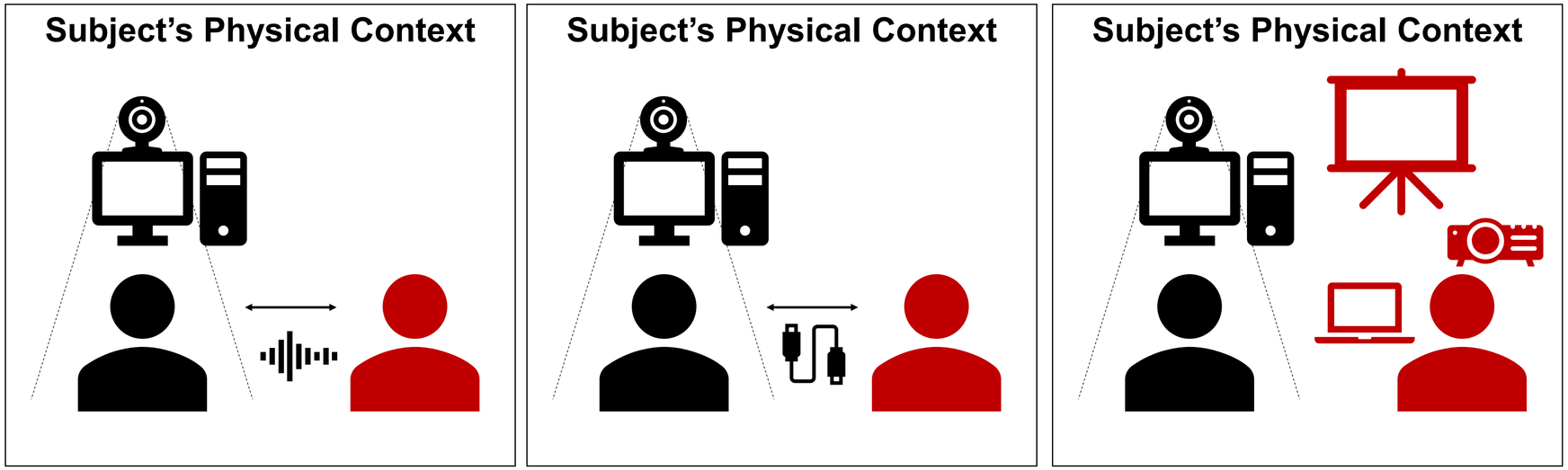
Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Identification of Communication, Collaboration and Resource Access Threat Scenarios

- In-situ Scenarios



Interaction with another person in the same room through voice

Projection of answers on a whiteboard

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

15-minute discussion

- In groups of two think about ways on how intelligent biometrics can be used to address the identified threat scenarios

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Design and Implementation of Open-source Privacy-preserving Toolkit and Application Programming Interfaces

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Key Objectives

- **Implement the algorithms** for continuous user identification based on a mixed model of voice, face and user interaction analytics
- **Preserve the privacy** of utilized user biometric data
- Design and develop an **open-source Identity-as-a-Service solution**
- Design and develop an **interactive dashboard** for service integration and analytics

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

TRUSTID High-level Framework

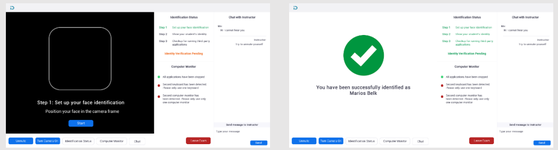
This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

TRUSTID High-level Framework

TRUSTID Client

Student view

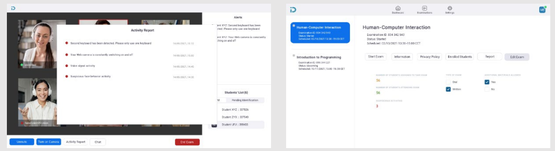
Features
– Enrollment with face and voice biometrics
– Integration with Universities' LMS
– Access to LMS examination



Countermeasure Features
– Face-/voice-based identification
– Detect authentic video streams
– Monitor student's digital context
– Monitor student's behavior
– Historical impersonation analytics
– Handwriting style analytics

Instructor view

Features
– Manual student verification
– Smart data analytics
– Run-time insights
– Actionable analytics
– Smart alerts

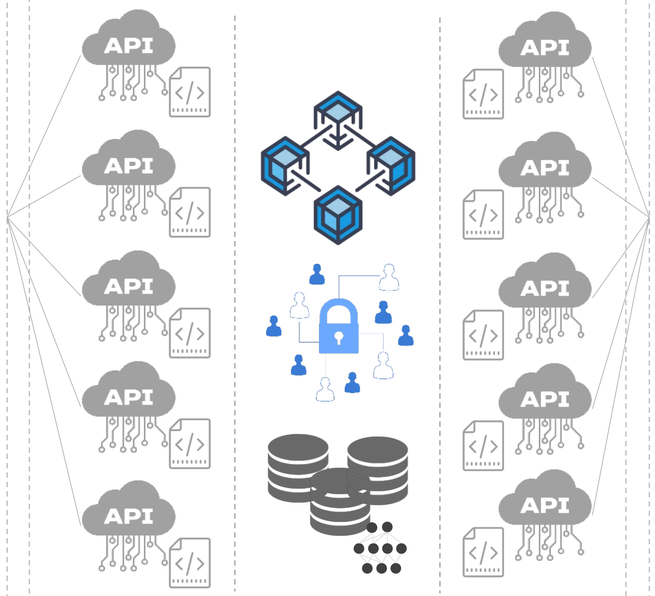


Implemented as a native Windows and MacOS application
Seamless for technical staff of HEIs
Allows control over the student's computing device

Student Interaction

TRUSTID Server

PostgreSQL, django, NGINX



Storage and processing of privacy-preserving biometric data

LMS of HEIs

moodle, Blackboard, open eclass e-learning platform

LMS Extensions

Student Data

Integration Services

Single Sign On

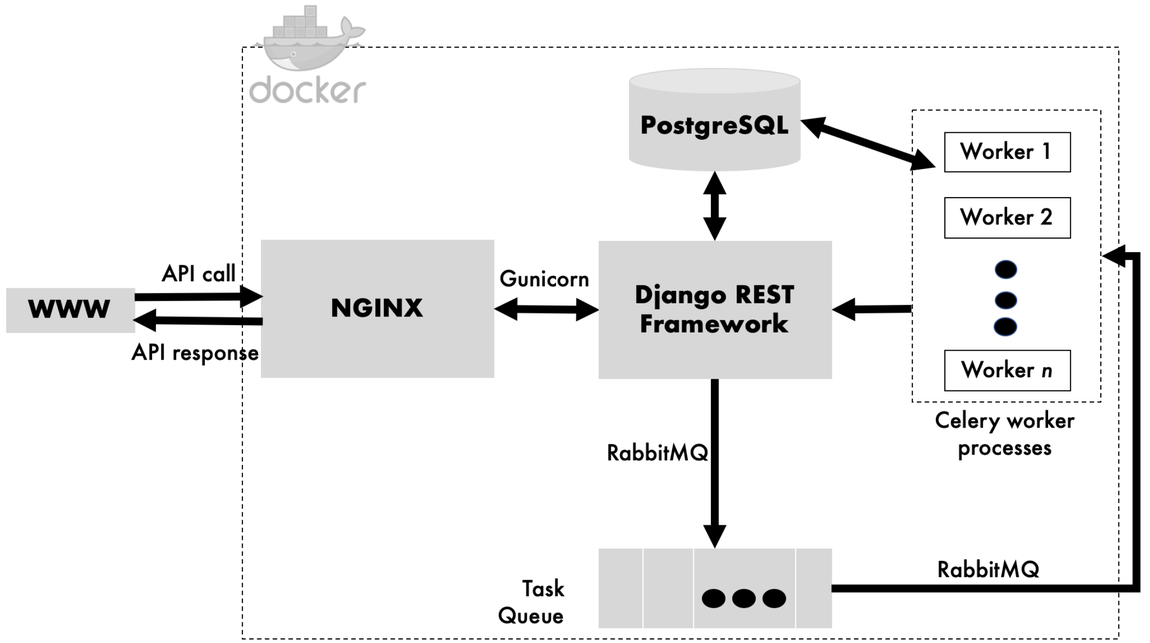
Integration of students' data and exam data

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Architectural Design and Technology Stack

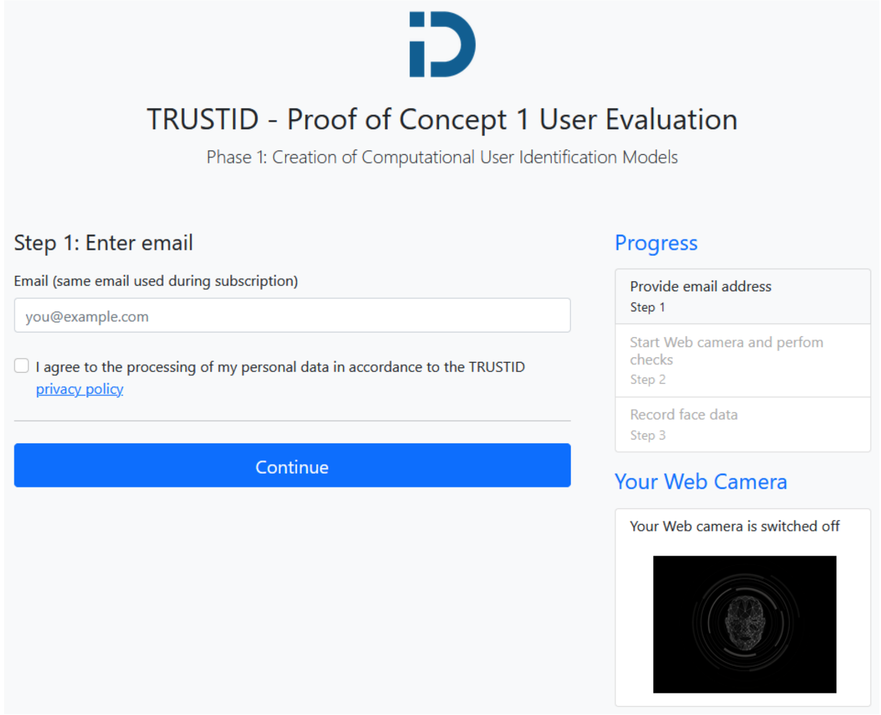
- Server-side **web API**
- **Django** REST Framework
- **NGINX** (Web server, Reverse proxy, Load balancer)
- **Gunicorn** (Application server that implements the Web Server Gateway Interface)
- **Celery** (Asynchronous task queue based on distributed message passing)
- **RabbitMQ** (Message broker)
- **PostgreSQL**
- **Docker**

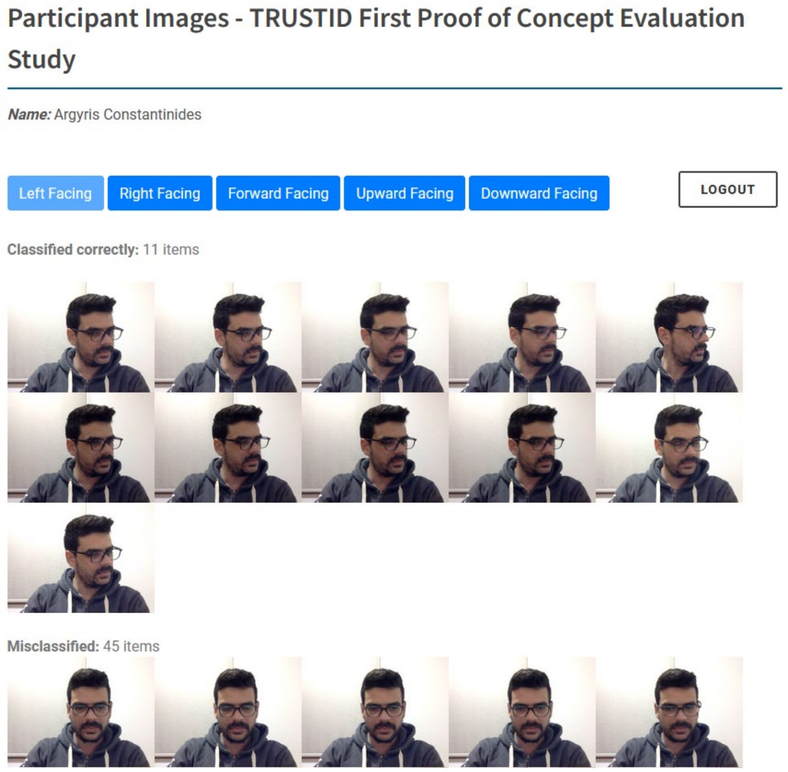


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Web-based Enrollment

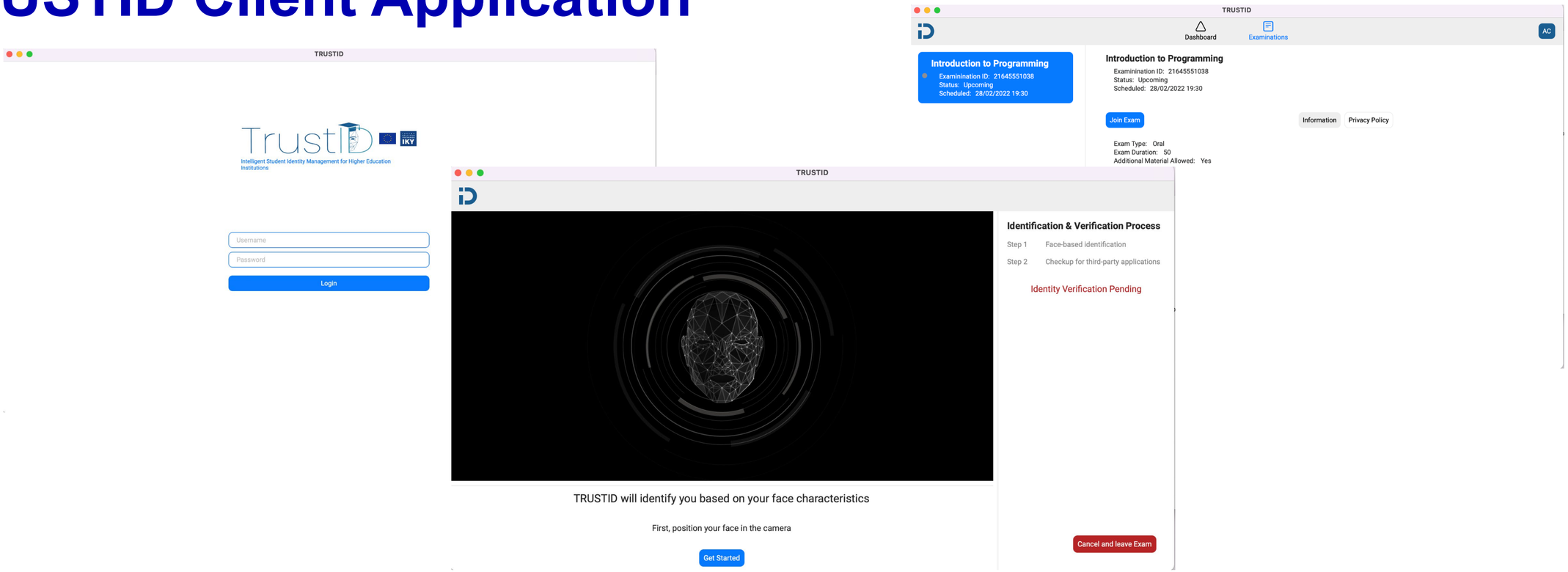




This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

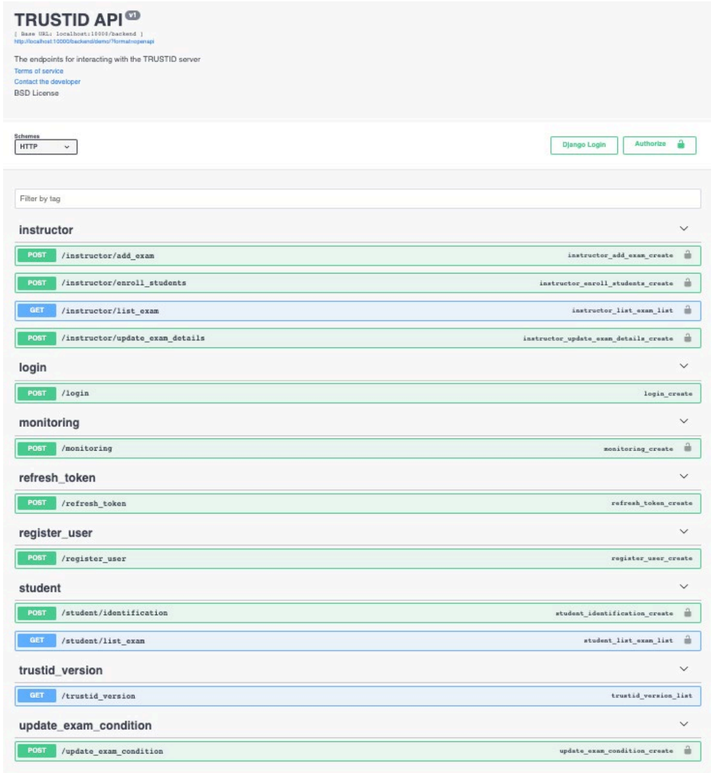
TRUSTID Client Application

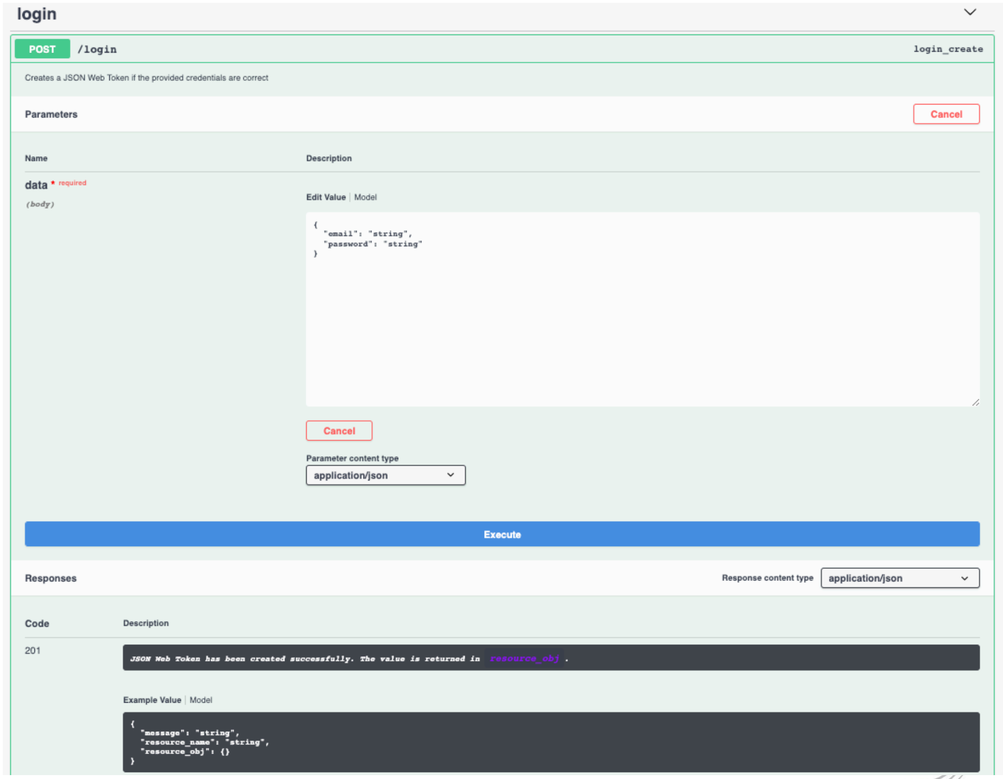


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

TRUSTID Backend – Application Programming Interface

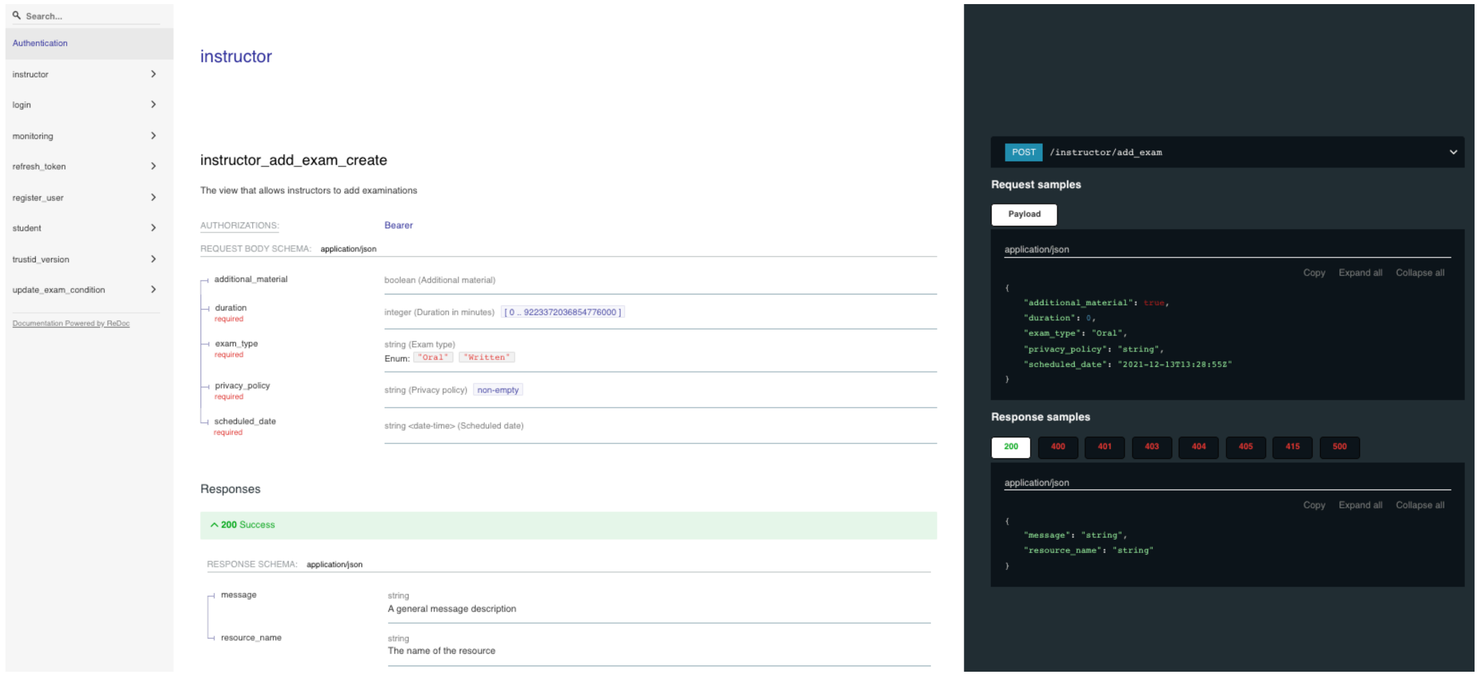




This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Web API – Documentation



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Face-based User Identification

- Image/video based Biometric system (face recognition)
- **Goal:** Identify users from pre-recorded image/video dataset
- System constrains:
  - Noisy image data (consumer grade webcams, acquisition issues, unconstrained environments, …)
  - Accurate and reliable system (requirement).
  - Computational performance concerns.

Source: Institute of Systems and Robotics, University of Coimbra

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Face-based User Identification

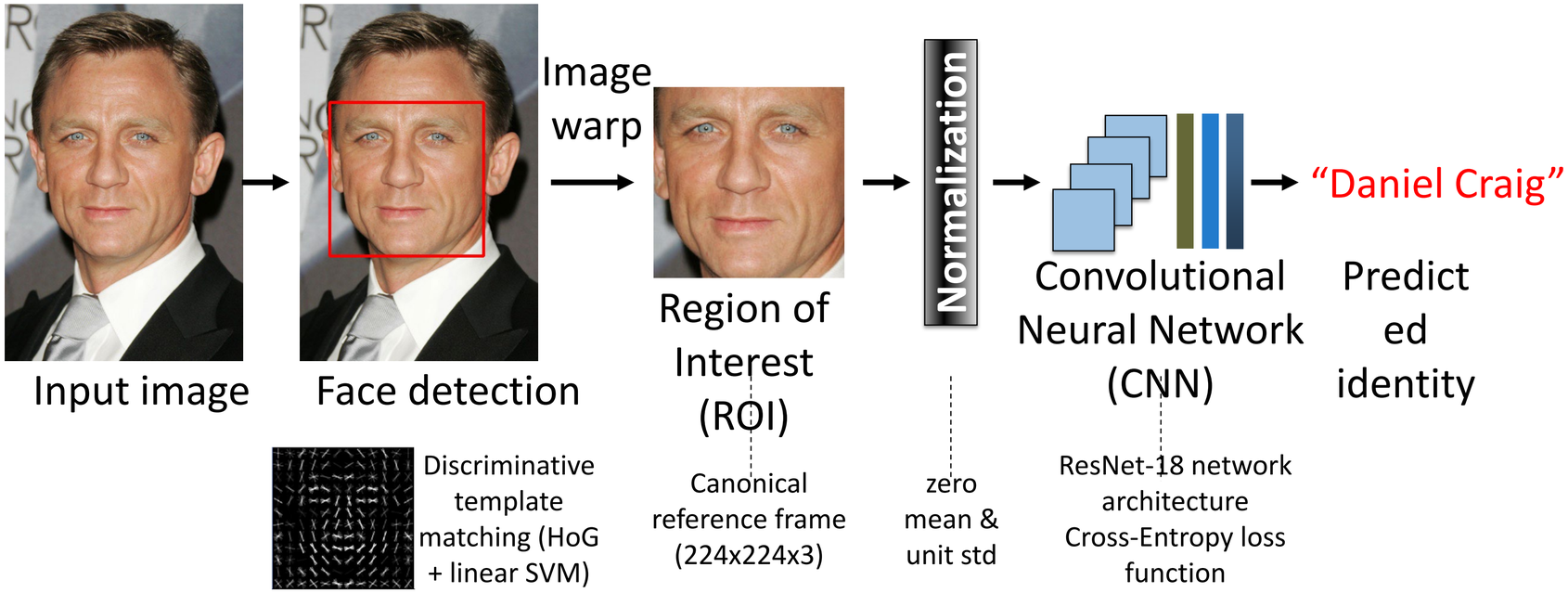
- Training stage (offline):
  - Assemble user's image database.
  - Face detection (locate faces in all images)
  - Data augmentation (add "virtual" variation to database images, p.e. geometric and color transformations).
  - Learn multiclass classifier from corresponding image/users examples.
- Testing stage (online):
  - Face detection
  - Predict user identity using the pretrained classifier model

Source: Institute of Systems and Robotics, University of Coimbra

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Face Recognition System Overview



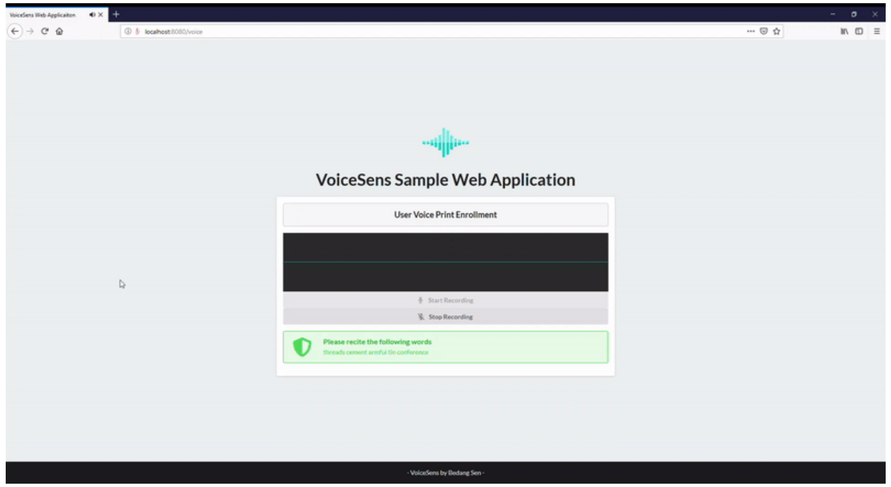
Source: Institute of Systems and Robotics, University of Coimbra

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

State-of-the-art Voice-based Identification Libraries

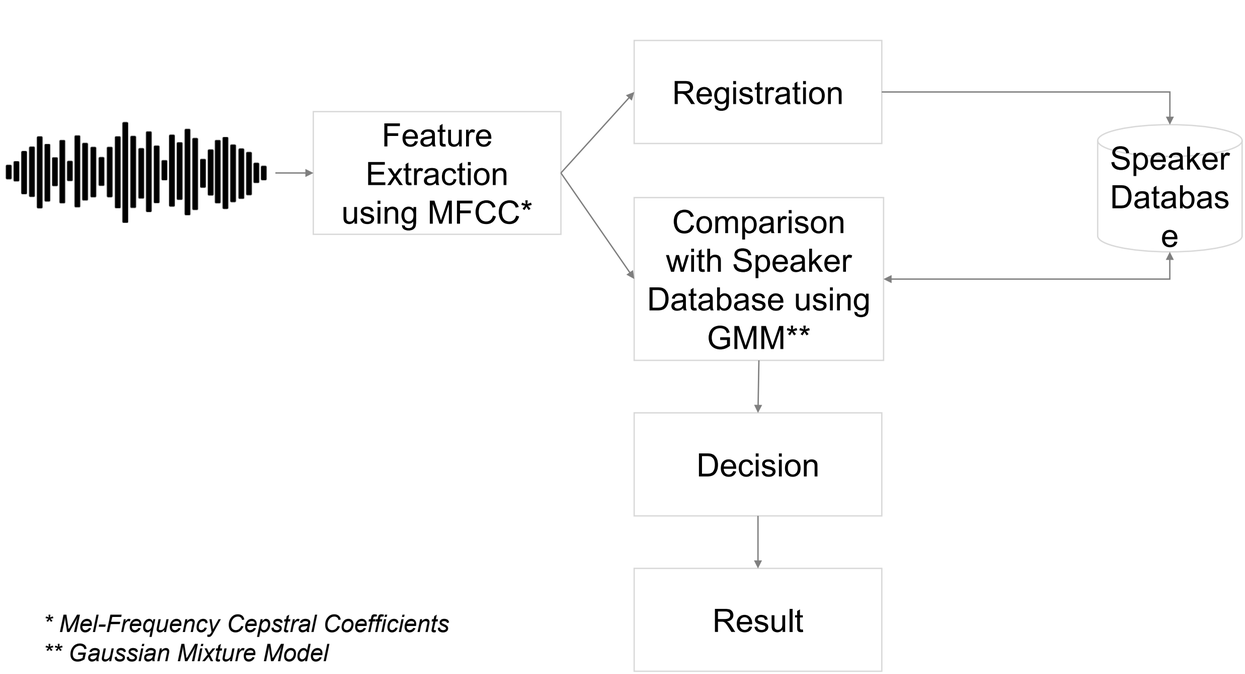
- **Kaldi**: a toolkit for speech recognition written in C++ and licensed under the Apache License v2.0. Kaldi is intended for use by speech recognition researchers
  - Python wrappers available
  - https://kaldi-asr.org
- **VoiceSens**: an open-source voice biometric solution
  - Developed in Python
  - Uses Watson Speech to Text (speech recognition)
  - https://github.com/bedangSen/VoiceSens



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Voice-based User Identification



** Mel-Frequency Cepstral Coefficients*
*** Gaussian Mixture Model*

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Challenges and ongoing development activities

- Improve the **front-end designs**
- **LMS integration and single sign on**
- Implementation of **voice-based identification mechanism**
- Implement client-side scripts for the native applications for **real-time head pose estimation and feedback**
- Investigating ways to process biometric data in an efficient and privacy-preserving manner
  - **client-side *vs.* server-side**

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Challenges and ongoing development activities

- **Sending video streams** of students and perform classification on a remote server has **several downsides**
  - entails privacy-preservation issues
  - time demanding
  - does not scale well
  - requires a lot of computing/processing/memory power to handle multiple requests
- **Investigate solutions based on federated learning approaches**
  - We will train models at the server-side based on ground truth data of students
  - Send the encrypted trained models to each client and perform classification at the client side

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

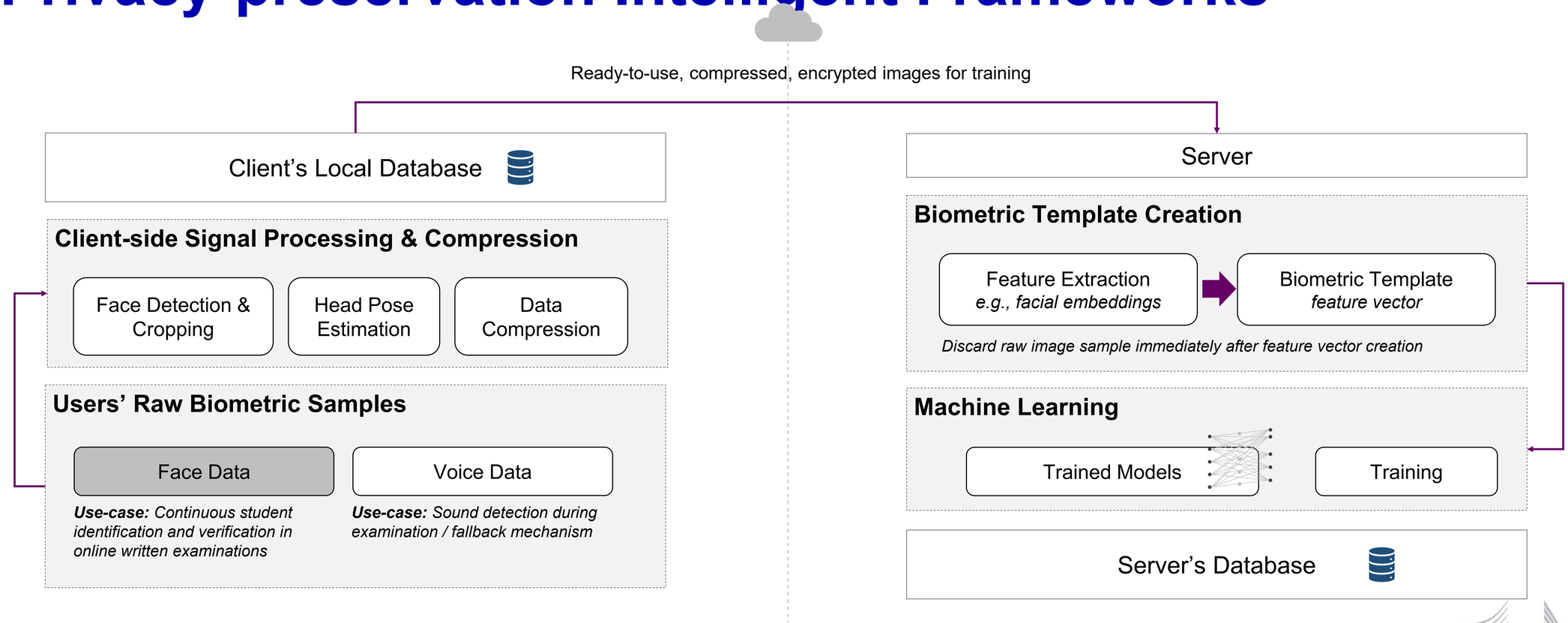
Technical Challenges

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

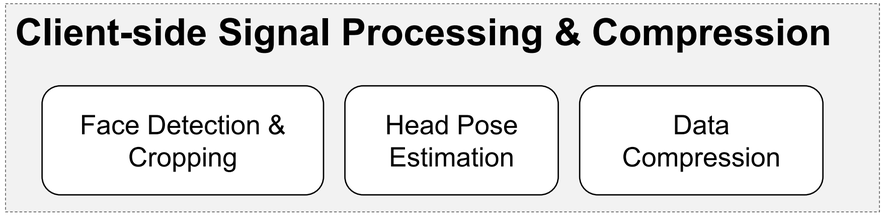
CONTENT 9

On Privacy-preservation Intelligent Frameworks



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9



- Cropping **reduces image size**
- Head pose estimation provides **instant feedback to the end-user** about the quality of sampling
  - Avoid sending the image over the network and then provide feedback; unnecessary communication
- Data compression **reduces image size even more**

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

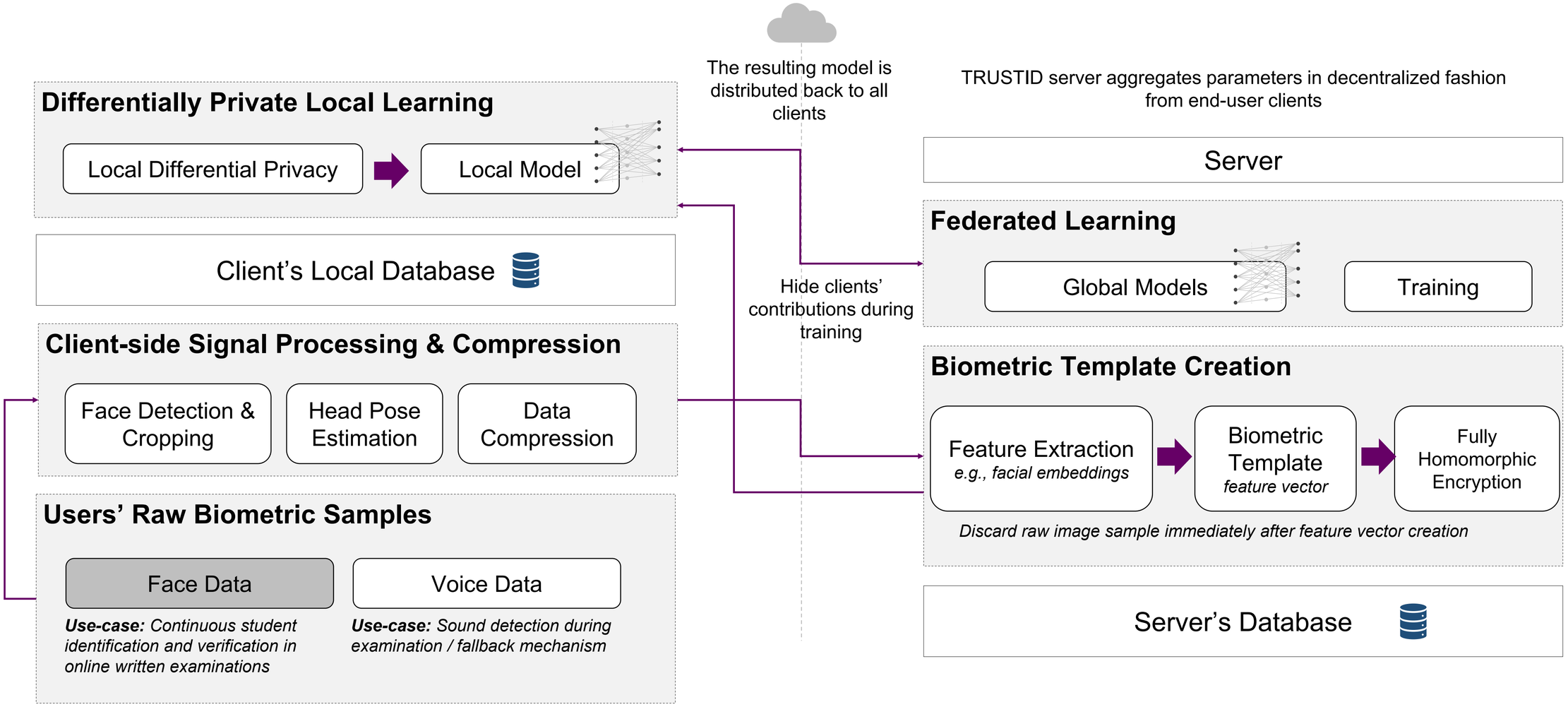
Open Issues

- Raw images are discarded after feature vector creation. Can feature vectors be used to reconstruct raw images?
  - Need to protect biometric templates by preventing attackers to reconstruct the original data
  - **Proposed solution: Homomorphic encryption -** *computing over encrypted data without access to the secret key*
- Processing data and their respective trained data models happens a centralized manner, which increases privacy-preservation issues
  - Need to train biometric data without having full and direct access to the raw data and the trained models
  - **Proposed solutions: Federated learning with differential privacy**

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Framework for Privacy-preservation



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Open Issues

- Feature extraction is a computing intensive process
  - Difficult to run at the client's side
- Homomorphic encryption is typically computationally expensive and practically infeasible
- Liveness detection

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Privacy-preservation Issues and Challenges for Storing, Retrieving and Processing Biometric Data of Students

- The suggested countermeasures primarily depend on physiological- and behavioral-based biometric technologies
  - Issues related to privacy-preservation of sensitive personal biometric data

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Privacy-preservation Issues and Challenges for Storing, Retrieving and Processing Biometric Data of Students

- **Envisioned Scenario:**
  - Students may control access to their data by following **self-sovereign data protection architectures**, which allow end-users to fully control who and what data are shared
  - Universities will act as **trusted entities** with certified procedures that will keep ground truth biometric data from their students in order to assure effective and efficient student identification, verification and monitoring

  - **Assure privacy for over-time historical analysis**, which requires the storage of large amounts of data about students
    - State-of-the-art approaches include biometric encryption techniques and distributed ledger technologies

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Privacy-preserving Biometrics

Historical biometric data analysis after the examination

Ground truth encrypted biometric templates
ready to be used

Ground truth encrypted biometric templates
for verification purposes

Biometric Template Data Protection

- Homomorphic Encryption
- Feature Extraction
- Signal Data Processing

Protect biometric templates by preventing attackers to reconstruct the original biometric template

Biometric Template Data Protection Tools & Algorithms

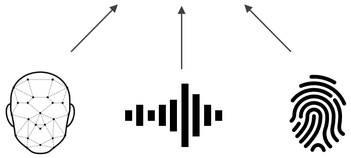
Differentially Private Federated Learning

- Adaptive Models
- Differential Privacy
- Local and Global Learning Models

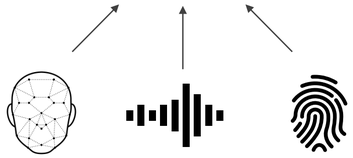
Differentially private federated learning for improving the models' accuracy and simultaneously keeping data private

Students' Biometric Data and Contextual Data

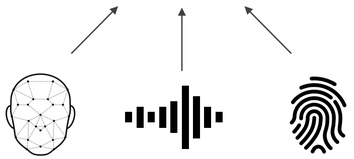
Physiological Data, Behavioral Data, Contextual Data



Student provides ground truth biometric data



Student verification during examination enrolment



Continuous student identification during examination

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Verifying the Authenticity of Users' Video Streams

- Benford's Law as an Efficient and Low-cost Solution for Verifying the Authenticity of Users' Video Streams in Learning Management Systems
- Authors: Argyris Constantinides, Christodoulos Constantinides, Marios Belk, Christos Fidas, Andreas Pitsillides
- The 20th IEEE/WIC/ACM International Joint Conference on Web Intelligenc Intelligent Agent Technology 14-17 December 2021, Melbourne, Australia

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Transition to Online Education Activities

- Issue: Single entry-point authentication mechanism
- Challenge: Efficient continuous verification through the webcam
- Threat: Impostors stream a pre-recorded video

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Current solutions

- Retina analysis
- Face, voice and body biometric analysis
- Behavioral analysis (e.g., keystroke dynamics, mouse patterns)

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Problems with current solutions

- Computationally heavy
- Expensive
- Increased network traffic

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Motivation

- Analyze input video stream
- Probability distribution of specific variables follows a pre-defined behavior in naturally generated data streams
- Benford's Law: Distribution of the first significant digit of quantized Discrete Cosine Transform coefficients – The leading digit is more likely to be small

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Research Questions

- RQ1. Can we build a prediction model for detecting authentic vs. pre-recorded videos from users' input streams by considering the distribution of the first digits of image DCT coefficients?
- RQ2. How well does the prediction model for detecting authentic vs. pre-recorded videos perform when a large number of users (e.g., 1000 users) are concurrently streaming videos?

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

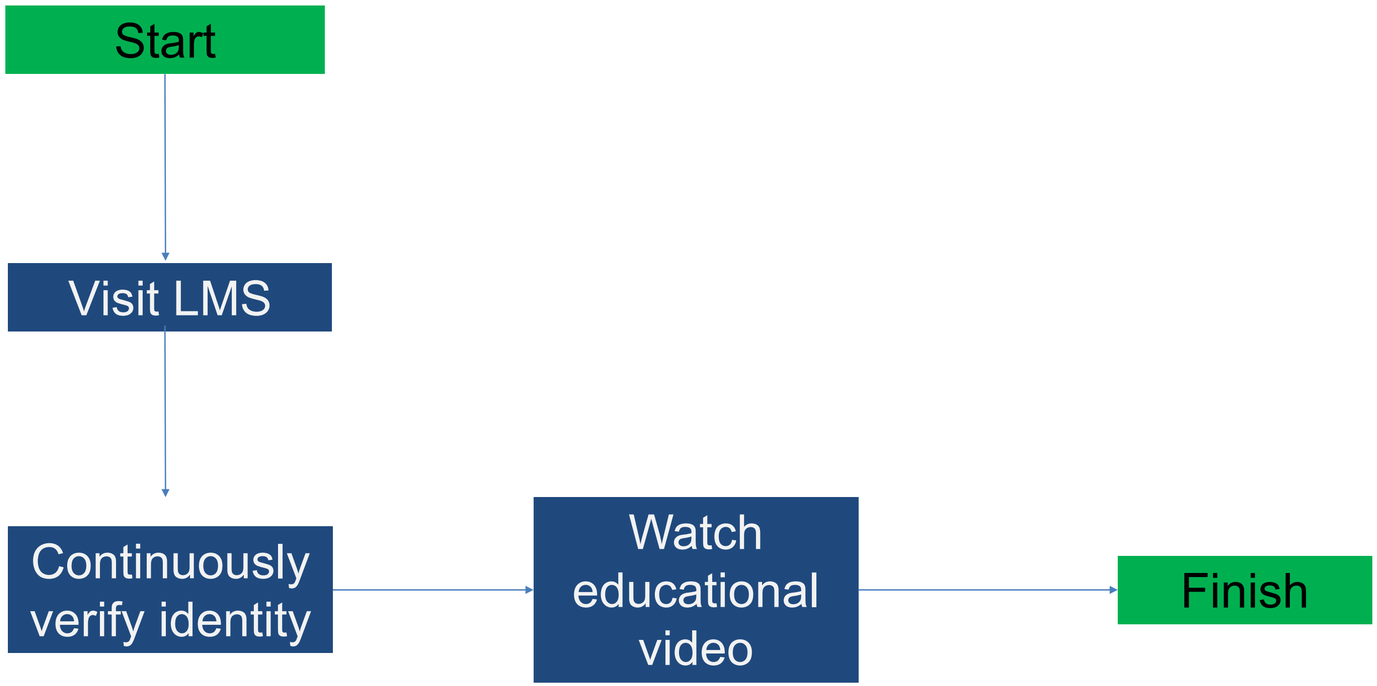
Remote User Study

- Between-subject design (N=18)
- Probability distributions of the first digits (ranging from 1 to 9) of the block DCT coefficients
- Divide each frame into distinct 8x8 blocks and the two-dimensional DCT is applied to each block

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Remote User Study



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

RQ1 – Detecting authentic vs. pre-recorded video streams

GI4E dataset

- 1339 authentic web camera images of 103 individuals
- Half of them uncompressed
- Other half were JPEG compressed with quality factors ranging between 80-99%

https://www.unavarra.es/gi4e/databases/gi4e

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Classification Results

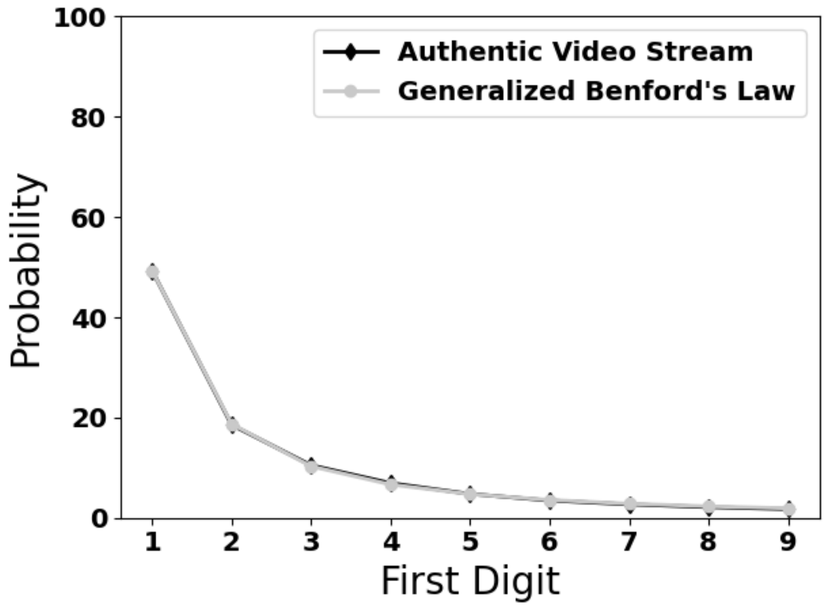
Classifier	Accuracy
Naïve Bayes	***81.9%***
Logistic Regression	78.7%
Support Vector Machines	79.1%

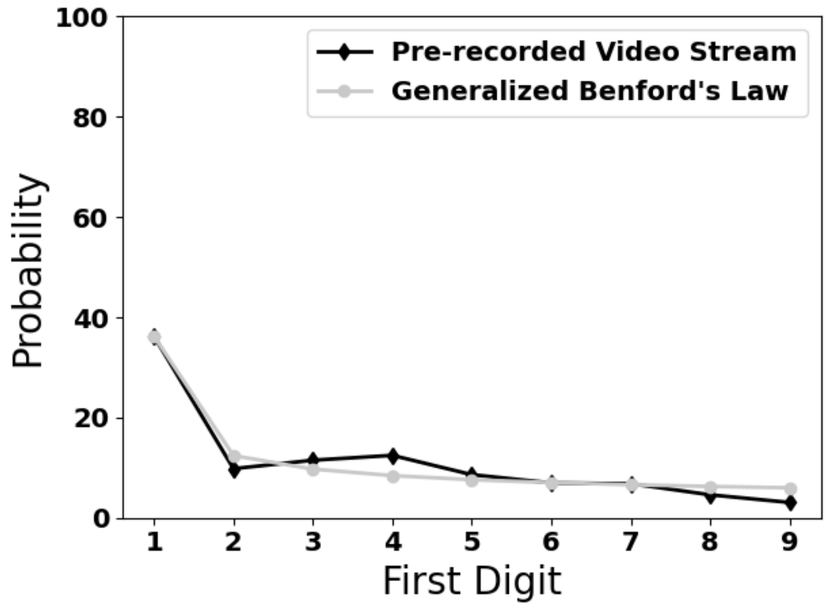
This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Distribution of first DCT coefficients

- Authentic input video stream follows the Benford's law perfectly
- Pre-recorded input video stream violates the Benford's law





This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

RQ2 – Performance testing

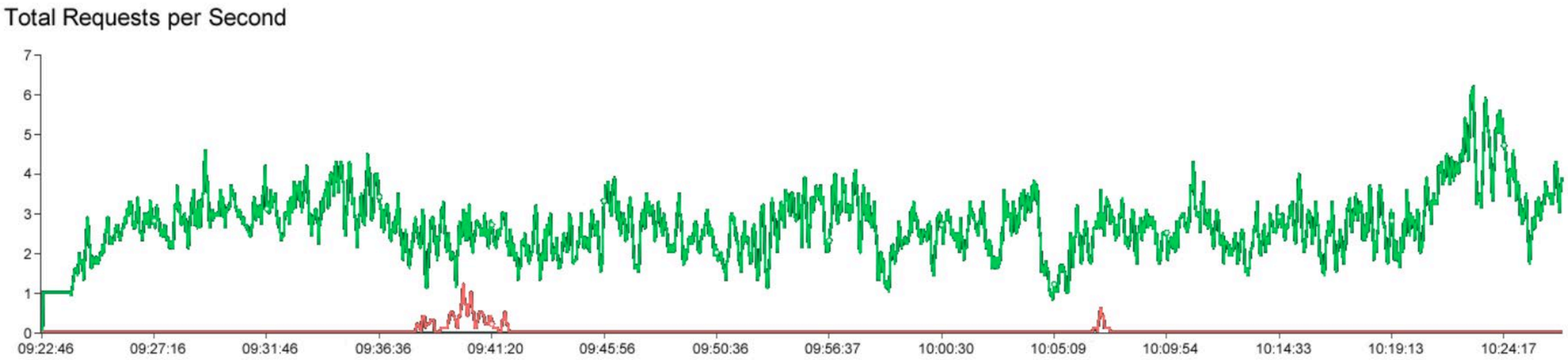
Simulated system through Locust:

- Students login to a proctoring platform
- 1000 concurrent students
- Frame from camera is captured periodically

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

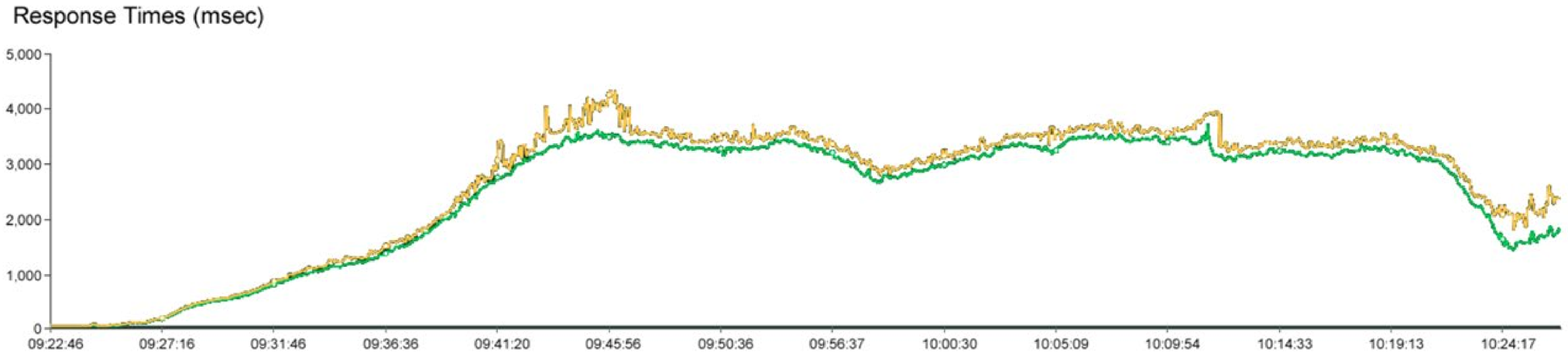
Performance testing results



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

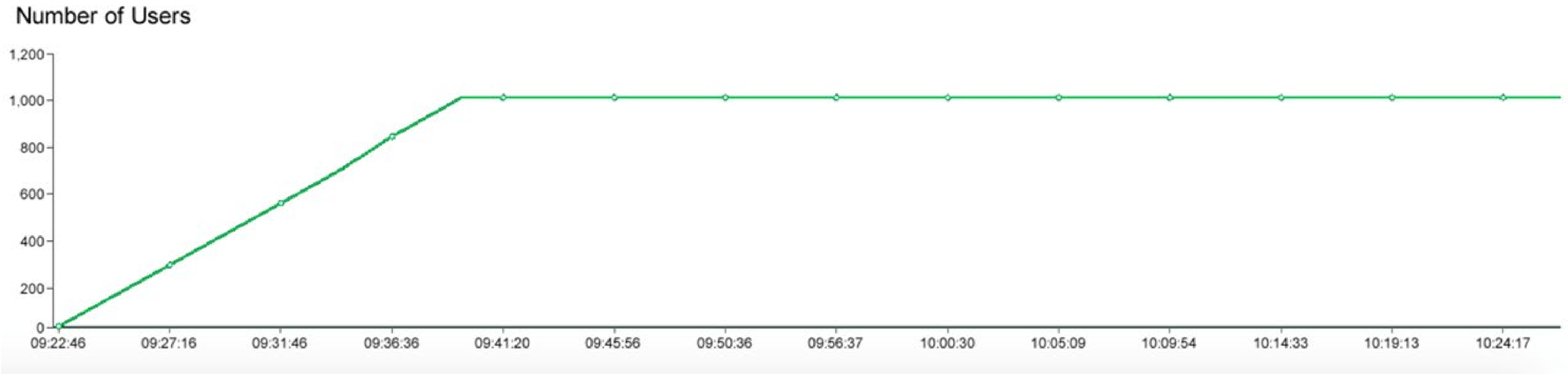
Performance testing results



This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Performance testing results



Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Takeaways

- Apply Benford's law for predicting the authenticity of input video stream within LMS
- No need for complex ML algorithms for continuous student verification
- Low-cost and scalable solution

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

CONTENT 9

Sources

- Erasmus+ TRUSTID Project – https://trustid-project.eu
- Face-based Identification by Institute of Systems and Robotics, University of Coimbra

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Thank you.

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423