D6.1 Smartphone sensors to support border identification 1

Document Due Date: 31.05.2020 (M09)
Document Submission Date: 29.05.2020

Work Package 6:
Alternative technologies to identifying people

Document Dissemination Level:
Public

D4FLY - **D**etecting **D**ocument frau**D** and i**D**entity on the fly
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833704

Abstract

The main objective of the tasks in WP6 is to explore alternative technologies for people identification. Task 6.1 – Using Smartphone Sensors for Identifying People, focusses on research and development of smartphone sensor-based solutions that can be used as an alternative biometric modality to be fused in the D4FLY on-the-move biometric verification system to complement the overall verification accuracy.

Smartphones have become an important part of people's daily life across the world. In particular, smartphones are carried by travellers for convenience, entertainment and communication, etc. Most recent smartphones are equipped with advanced sensors (such as accelerometer, gyroscope, magnetometer, GPS, Wi-Fi, Bluetooth, etc.). Within Task 6.1, the potential for using biometric modalities enabled by smartphone sensors to be employed in a border control scenario is explored. The developed solution will be integrated into the D4FLY Highly Automated Border Post scenario. The results can be fed into the fusion module with other biometric results to produce a final score.

This deliverable reports the work and progress carried out during the first period (M1-M9) within Task 6.1 which is summarised as follows:

- A background study was carried out investigating smartphone sensors, software, datasets, methodologies using smartphone sensors, and the state-of-the-art research on continuous person authentication using smartphone motion sensors
- An Android app was developed using the Android SDK that can collect various sensor data on an Android mobile device
- Designed the concept and use-case of smartphone-based person authentication to be used in a border control scenario, and how the developed technology can be linked and integrated into the D4FLY system
- A continuous person authentication-based approach using neural networks was developed for the initial feasibility investigation and initial testing was performed using public datasets

The final version of the developed solution will be reported in the subsequent deliverable D6.6 – Smartphone sensor to support border identification 2.

Project Information

Project Name	Detecting Document frauD and iDentity on the fly
Project Acronym	D4FLY
Project Coordinator	Veridos GmbH
Project Funded by	European Commission
Under the Programme	Horizon 2020 Secure Societies
Call	H2020-SU-SEC-2018
Topic	SU-BES02-2018-2019-2020 Technologies to enhance border and external security
Funding Instrument	Research and Innovation Action
Grant Agreement No.	833704

Document Information

Document reference	**D6.1**
Document Title	**Smartphone sensors to support border identification 1**
Work Package reference	WP6
Delivery due date	31.05.2020
Actual submission date	29.05.2020
Dissemination Level	Public
Lead Partner	UoR
Author(s)	Lulu Chen
Reviewer(s)	James Ferryman (UoR) Martin George (OVDK) Dimitris Kyriazanos (NCSRD)

Document Version History

Version	Date created	Beneficiary	Comments
0.1	01.04.2020	UoR	Initial draft – document structure
0.2	20.04.2020	UoR	Structure changes; Added content to various sections
0.3	28.04.2020	UoR	Added content to various sections
0.4	06.05.2020	UoR	Added Abstract, added content to various sections
0.5	11.05.2020	UoR	Finalised for first technical/internal review
0.6	14.05.2020	UoR	Made modifications after the internal review
0.7	17.05.2020	UoR	Made updates after 2nd round internal review and ready for external review
0.8	20.05.2020	UoR	Updates after external review
0.9	27.05.2020	UoR	Updates after security review
1.0	29.05.2020	VD	Final edits

List of Acronyms and Abbreviations

ACRONYM	EXPLANATION
EC	European Commission
EU	European Union
D4FLY	Detecting Document frauD and iDentity on the fly
BFM	Biometric Fusion Module
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
CNN	Convolution Neural Network
EER	Equal Error Rate
SVM	Support Vector Machine
UoR	University of Reading
VD	Veridos
DPIA	Data Protection Impact Assessment

Table of Contents

1 INTRODUCTION

The main objective of the tasks in D4FLY Work Package 6 – Alternative technologies to identifying people, is to explore alternative solutions for people identification. While Work Package 5 – Biometric technologies for identifying people on-the-move addresses contactless biometrics (for on-the-move identification), alternative solutions using innovative technologies will be developed within this work package. This deliverable reports activities within Task 6.1 – Using Smartphone Sensors for Identifying People, which focuses on on-the-move biometric identification using travellers' smartphone sensors.

In Task 6.1, the potential for a traveller's smartphone to perform biometric identification will be researched and investigated. A feasibility study of using such technologies in the D4FLY scenario will be carried out. The development and implementation of the solutions will be made. Task 6.1 is implemented in two phases.

In the first phase, research will focus on the development of a novel machine learning-based classification framework based on neural networks utilising sensory data from smartphones. The research will focus on motion sensors (i.e. accelerometer, gyroscope) that provide motion patterns of the travellers that can be used for identification. The second phase will focus on implementation and realisation of the developed solutions to enhance identification accuracy and efficiency. Research will also examine the potential for fusing the result from location-based tracking sensors (such as, GPS, Wi-Fi, Bluetooth, etc.) with biometric acquisition and recognition on the smartphone for future concepts and increased identification accuracy.

The outcome from the task can be considered as a biometric trait and integrated into the biometric identification system. The results from the identification can be fed into the fusion module (which will be developed in Task 5.6 Biometric Fusion starting in M17 - January 2021) with other biometric results to produce a final score.

The task will involve evaluating the approach against appropriately selected benchmark data and to assess the performance of the approach to spoofing.

1.1 Background

Task 6.1 starts in M1 (September 2019) and ends in M24 (August 2021), and the sole contributor of the task is UoR. There are two deliverables from the task:

TABLE 1 DELIVERABLES OF TASK 6.1

Deliverable number	Deliverable title	Type	Dissemination level	Due date
D6.1	Smartphone sensors to support border identification 1	Report	Public	M9 – September 2019
D6.6	Smartphone sensors to support border identification 2	Demonstrator	Public	M24 – August 2021

1.2 Aim of this document

This document introduces the first phase of the development for Task 6.1 and describes the activities and development progress within the task.

The main activities and progress carried out during the first period (M1-M9) to be reported in this document:

- A background study was carried out investigating smartphone sensors, software, datasets, methodologies using smartphone sensors, and the state-of-the-art research into continuous person authentication using smartphone motion sensors
- An Android app was developed using the Android SDK that can collect various sensor data on an Android mobile device
- Designed the concept and use-case of smartphone-based person authentication to be used in a border control scenario, and how the developed technology can be linked and integrated into the D4FLY system
- A continuous person authentication-based approach using neural networks was developed for the initial feasibility investigation and initial testing was performed using public datasets

2 SMARTPHONE SENSORS

As introduced in Section 1, Task 6.1 will develop an alternative solution for person identification based on smartphone sensory data. This section provides an overview of the smartphone sensors, especially on the motion sensors that are relevant to the task.

2.1 Smartphone inertial sensors

Most current smartphone devices are equipped with various built-in sensors that can be used for different application areas, such health care and fitness tracking, location tracking, environmental condition detection, security measures, gaming, etc.

The common sensors that included in smartphones nowadays are generally divided into four broad types: position sensors, motion sensors, environment sensors and biometric sensors:

- Position sensors: GPS, barometer, magnetometer
- Motion sensors: Accelerometer, gyroscope
- Environment sensors: Microphones, ambient light, infrared and proximity sensor
- Biometric sensors: fingerprint scanner, iris scanner and face camera

Most new phones claim to have advanced built-in sensors that can provide raw sensor data with high precision and accuracy. Current smartphone operating systems, e.g. Android and iOS, provide SDKs for the developers to access the raw data, e.g. three-dimensional device movement or positioning. Although there are many types of sensors equipped on a smartphone, the work in T6.1 during the first phase focussed on the following three types of sensors that will be used for person identification. As mentioned in Section 1.1, extension of the work on involving location based sensors with tracking ability (e.g. GPS, Wi-Fi, Bluetooth, etc.) will be carried out during the second phase.

Accelerometer

An accelerometer measures the acceleration of the specific device in the three-dimensional space. The speed and direction of the device’s motion and the device’s orientation can be estimated from the sensor reading. The sensor is made up of other sensors, including microscopic crystal structures that generate electric charge when they become stressed due to accelerative forces (piezoelectric effect). The accelerometer then interprets the voltage coming from the crystals (rate at which charge varies) to figure out how fast the phone is moving and in which direction.

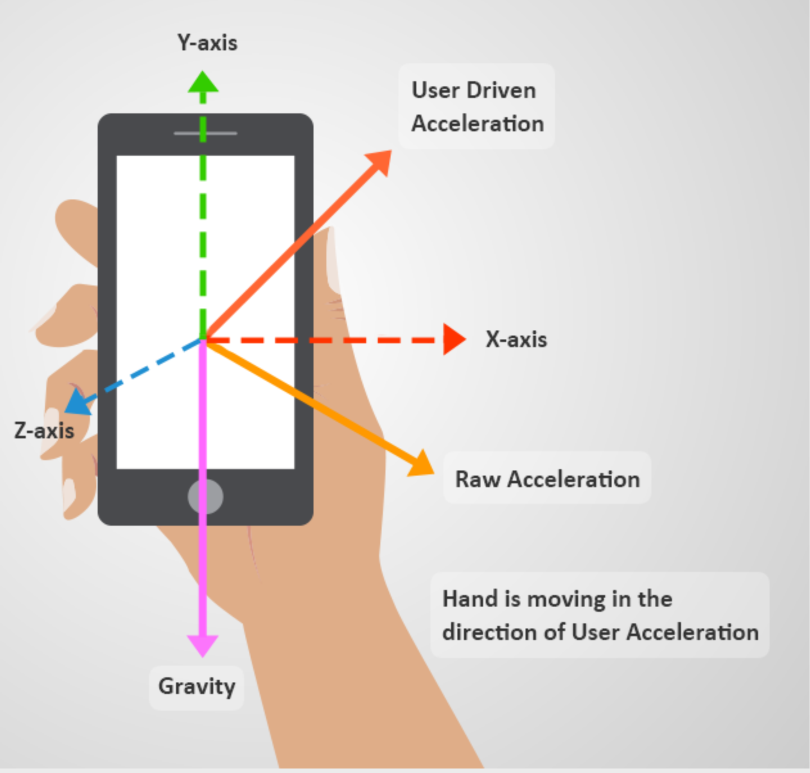

FIGURE 1 ACCELEROMETER ON A SMARTPHONE CAPTURES THE ACCELERATION OF THE DEVICE IN THREE AXES [30]

The accelerometer is the main and most important motion sensor in a phone. It can be used for motion related action/behavioural based verification. Accelerometers can be sensitive to orientation and positional variance.

Gyroscope

A gyroscope acts as a complementary sensor to the accelerometer that helps to estimate the general position and behaviour of the device. It specifically measures the degree of rotation around the three axes. It helps to calibrate the accelerometer in order to estimate which way the phone is orientated.

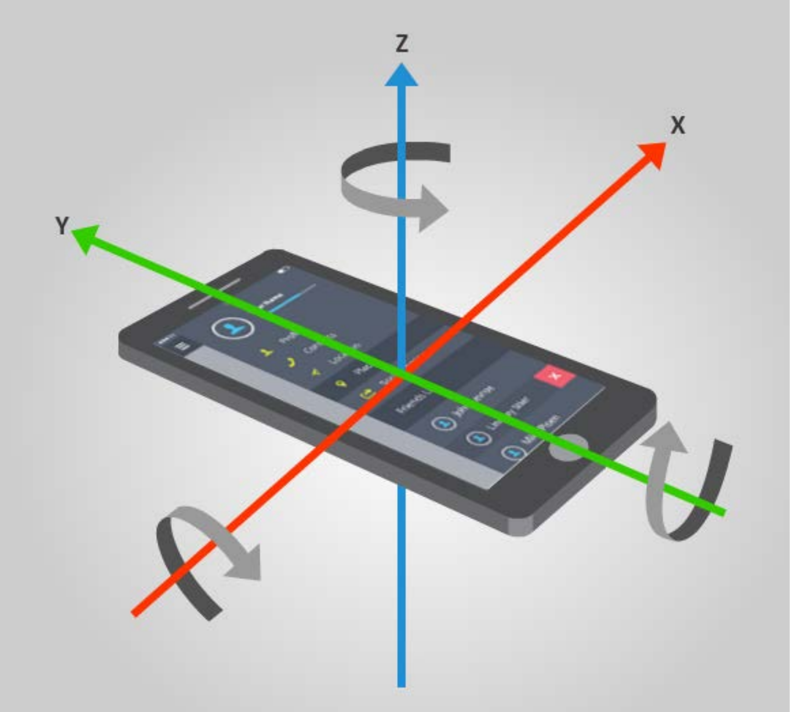

FIGURE 2 GYROSCOPE MEASURES THE ROTATIONAL SPEED OF THE DEVICE [30]

The gyroscopes inside smartphones are MEMS (Micro-Electro-Mechanical Systems) gyroscopes, embedded on an electronics board so it can fit inside a phone. These systems typically work by measuring the vibrations of a material across multiple axes.

Magnetometer

A magnetometer defines the position, orientation and direction of the device by measuring the local magnetic field to determine the direction of geomagnetic north. The sensor can be used to complement accelerometer as it is much less sensitive to orientation and position in comparison.

2.2 Smartphone sensor data capture

2.2.1 Developed smartphone app

For collecting data for training and evaluation, a dedicated app was developed. The app runs on Android operating system (OS). The app has two running modes: standalone and remote control. Figure 3 illustrates the user interface for each of the two modes.

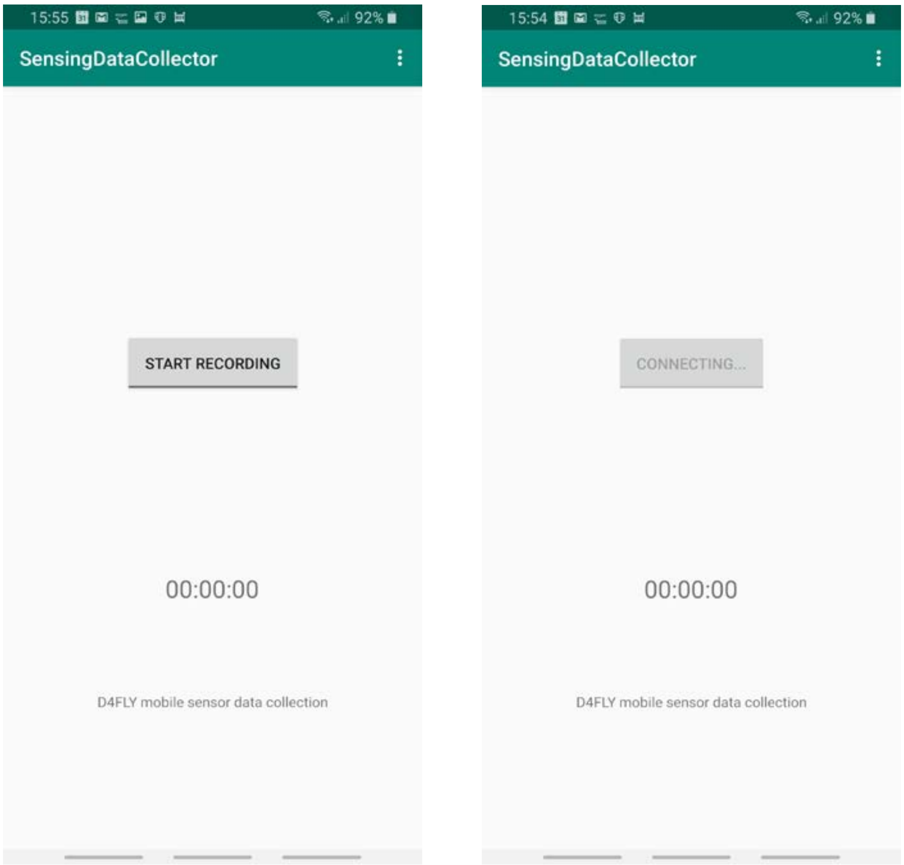

FIGURE 3 USER INTERFACE OF THE DEVELOPED ANDROID APP: LEFT - APP RUNS STANDALONE; RIGHT - APP RUNS BY REMOTE CONTROL OVER NETWORK

Standalone mode

The app can run as a standalone app. When the user presses “Start recording” button on the home screen, the app will start recording the readings from all the sensors, and the button changes to “End recording”. When the user presses “End recording” button, the app ends all data recordings. The records are saved as files on the phone’s internal non-volatile memory.

Remote control mode

One issue with standalone mode is that when the user presses the “Start/end recording” button, the motions sensors will pick up even the slightest motions caused by the button pressing, which can cause a few seconds of inaccurate data. To eliminate this effect, a remote-control mode was developed. The app can be connected to a computer on the same Local Area Network that acts as a remote control for the app. When the user is ready for recording, the “start recording” and “end recording” actions can be triggered by the remote control app on the computer. In this way, no spurious data caused by the user attempting to trigger the app is generated.

The sensor data that the app currently collects include:

- Acceleration: including linear acceleration and gravitational acceleration

- Gyroscope
- Magnetometer
- Luminosity
- Barometer
- Other sensors can be easily added if needed

Additional sensors such as GPS, Wi-Fi, Bluetooth, etc. will be added for the D4FLY multimodal data collection event. The additional sensor types will be used for investigating the possibility and potential for fusion to increase overall person identification accuracy using the smartphone sensors.

2.2.2 Initial data collection for proof of concept

Some initial data was collected for testing the functionalities. A limited data collection was performed with only 2 users in order to test the app's functionality, capacity and stability. Each user was asked to perform a few walks along a corridor-like setup while holding the phone in one hand. Each walk took about 10 to 20 seconds. During each walk, the user held the phone in different positions, e.g. phone over the ear, phone in the front, phone in a trousers' pocket, etc. Sensors collected included: accelerometer, gyroscope, magnetometer, luminosity and barometer. Sensor data were recorded at a frequency of 50Hz and data were saved into a .txt file for each sensor type. The recording was performed using both standalone and remote-control modes so that the networking functionality was tested.

An internal data collection event with more users was originally planned for algorithm testing and evaluation, however due to the COVID-19 pandemic the event was unable to take place. Instead, some public datasets were used for experiments and initial algorithm evaluation (Section 4.4). The developed Android app is ready and will be used for collecting sensor data in the D4FLY multi-modal data collection event that relates to Task 5.1 Multimodal biometric datasets.

2.2.3 Data protection and ethical requirements

The data collection process using the developed Android apps will follow the data protection guidelines described in D4FLY deliverable D3.2 Privacy and Data Protection Impact Assessment [29]. The deliverable D3.2 provides detailed Data Protection Impact Assessment (DPIA) for each of the technologies/tools developed within D4FLY including the Android applications to be developed in this task.

Two separate Android applications will be developed within this task: the UoR sensor data collection app as described above in Section 2.2.1; and the UoR continuous person authentication app that will be integrated in the D4FLY scenarios (concept is introduced in Section 3).

In general, both apps follow these data protection and ethical requirements guidelines:

- The developed app will not share any collected data with any other applications installed on the phone
- Only sensor data stated on the consent form will be collected and no other personal data from the phone will be recorded
- Data collection, and the testing and demonstration of the apps will try to recruit people from a wide range of demographic background, including a variation in race,

gender, age, and health related issues. This is to ensure that the developed technology does not discriminate against segments of the population

Each app also follows additional guidelines specific to their use-case in order to maintain data protection in the two applications.

The UoR data collection app (Section 2.2.1) follows these additional guidelines:

- The collected dataset will be stored on GDPR compliant Microsoft SharePoint which is secure, and auto-backed up.
- Only authorised user accounts (currently only people who work on D4FLY project) can access the data and 2-factor authentication is required to login into the SharePoint.
- When required to share the dataset with project partners, access to the dataset will be granted only upon submitting a request form. 2-factor authentication will be required to login and access the data.

In standalone mode, the data will be encrypted and anonymised on the phone, i.e. the user will be assigned with a random ID number and if the phone is lost, no links to the real user can be found. The data will be transferred to the secure storage location via wired connection and deleted once the transfer is completed.

In remote-control mode, communication between the phone and the server will use a secure encrypted connection following current best practice. Data will be transferred over this secure channel. Data will be deleted automatically from the phone after successful transmission.

The UoR continuous person authentication app (Section 3) follows these additional guidelines:

- The mobile device will not store any recorded raw sensor data after the process
- Any recorded raw sensor data and generated data will be deleted from the device after the process
- The app can only be started by the D4FLY VD Android app (a different application installed on the same device) for either the Enrolment or Verification procedure (the two types of procedures for D4FLY scenario 2 are defined and described in detail in the D4FLY deliverable D4.2 System Architecture [28]); and the app will be terminated after the procedure finishes

In the enrolment phase, a biometric template will be generated by processing the raw sensor data. This template will be encrypted and sent through a secure network to the D4FLY database. Please refer to Task 6.3 Smartphones based enhanced traveller verification and Task 4.2 System architecture on how the communication and data transferring is designed and implemented.

In the verification phase, raw sensor data will be continuously read and processed to provide matching results. There will only be the matching results (matching scores/decision) sent to the biometric fusion module (Task 5.6).

3 Continuous person authentication based on smartphone sensors

Continuous person authentication is a relatively new research topic. It can be applied in areas that require higher security, such as mobile banking. The change in the motion patterns from the user can help identify unauthorized use of the mobile device. The topic has not really been explored in case of border control scenarios. Therefore, a background study and literature review has been conducted to answer the following questions:

- How can continuous person authentication fit into the whole D4FLY border crossing process?
- How can it be used to support different border crossings?
- What level of accuracy can it provide?
- What are the issues and mitigations concerning potential spoofing attacks?
- Can the continuous person authentication process be real-time, especially if relying on smartphone computing power alone?

This section and next section will try to answer most of these questions which will aid the design of the system.

3.1 One-time vs. continuous systems

The current common person verification methods are passwords, PINs, and biometric recognition (e.g. fingerprint, face, iris, voice recognition). These approaches are one-time verification methods in that the verification process is only performed once at the beginning of a session (e.g. to unlock the phone, log into mobile banking, etc.).

In contrast, a continuous person authentication process will enforce access control during the entire work session, constantly verifying the user's identity at a selected frequency based on the system requirements. This may be useful to manage the access rights during the work session, e.g. preventing an unauthorised user from gaining access to the system by temporarily taking possession of a device from an already authenticated user.

Centeno et al. [24] claims that continuous system can add a layer of security to the service provider and improve usability. When the system provides continued confidence in the identity of the user, the service provider may decide to skip further security queries, i.e. not requiring an extra verification step. Alternatively, continuous approaches could be used as the primary authentication method.

3.2 Person authentication based on behavioural biometrics

Current related research based on smartphone sensor data have mostly focussed on person authentication for gaining access to their smartphones. There are two categories of biometrics: physiological and behavioural biometrics. Physiological biometrics detects persons' physiological features, such as facial features, fingerprint, iris pattern, etc. Behavioural biometrics are based on a user's behaviour and includes analysis of information like the shape and flow of one's handwriting, timing of keystrokes, unique patterns inherent in one's gait, speech and usage of styluses, and other features of one's general behaviour [25].

Activity recognition based on mobile sensors is not a new research topic, especially regarding accelerometer data. However, research on user identification/authentication based on smartphone sensors is relatively new. In a review by Alzubaidi and Kalita [2] on behavioural biometric user authentication methods for smartphones, the authors introduce that the main methods are to use the data that originates from the continuous interaction of the user with their mobile device to generate a number of features that uniquely model the user's interaction, and discriminate that person from others. Seven different behavioural biometrics were identified in the work for user authentication, including gait, touchscreen interaction, hand waving, keystroke pattern, voice, signature and behavioural profiling. Most of these behavioural biometrics would require active interaction/input from the user (e.g. typing, swiping, touching and the phone screen), which is not practical in border crossing applications.

Gait based:

Gait recognition using smartphone sensors may be applicable to this task [10][32][33]. However, as many previous studies have pointed out, it is limited and less reliable than other biometrics (e.g. face, fingerprint, etc.) due to its fundamental lack of discrimination power compared to other biometric modalities, and a person's walking style can be influenced by and vary due to many external factors (such as mood, speed, environment, etc.). Additionally, the data collected can be very sensitive to where the sensors are attached.

Tap/swipe screen touch event based:

Another group of works identify users based on smartphone sensors analysing the features when the user taps or swipes on the screen [9][11][12][15][16]. The main limitation of this approach is that active user interaction is required. As reported in the experiments by Sitová et al. [9], the best EER was achieved by a combination with tap while walking using the motion features they proposed.

Single movement based:

There are also works using a specific motion/movement to identify the user, for instance, hand waving. This has similar drawbacks as gait recognition, in that the motion can change significantly due to the person's mood, environment, etc.

A few previous works also combined different behaviours [9][13][14], such as combining touch events with movement. One common limitation of some of these works is that, as with normal phone authentication methods (passcode, pattern, iris, face and fingerprint recognition), they are normally used as a one-time authentication method. In a border crossing scenario a more continuous authentication process is desired. Although these works are not directly relevant to the tasks, the methods described and features extracted from sensor data can be useful.

More recently, several works have focussed on continuously identifying the user by recognising pre-defined actions, such as walking, sitting, standing, going upstairs/downstairs, drinking, etc.[1] Muhammad et al. [5] presented a multi-class smartphone user authentication framework (IntelliAuth) using physical activity recognition which recognises behavioural patterns from a series of activities performed by the user, and micro-environment sensing based on recognising elements within proximity of the surrounding area of the mobile phone. Six types of activities were considered in the research: walking, sitting, standing, running, walking upstairs and downstairs. Three mobile sensors were used for collecting data: accelerometer, gyroscope and magnetometer. Yoneda and Weiss [22] defined eighteen daily activities. Only accelerometer and gyroscope are used [20][22]. 51 users were used in the evaluation. Mario et al. [23] presented a continuous authentication system based on an autoencoder - a deep learning technique to extract features relying on user-specific activities.

To achieve real-time authentication in real-world scenarios, they developed the system hosted on a cloud platform to overcome the performance limitations from smartphones. The only sensor data used is the accelerometer in order to reduce the computational time. Different from the works above, the stage for activity recognition is ignored by assuming that people are doing the same activity.

The main idea is to address the challenge of user authentication on smartphone in a passive, non-intrusive way, and to utilise the sensor data where features can be extracted to recognise different actions to identify the user continuously and in real-time. This would normally require a two-stage processing: 1) action recognition that firstly recognises the action that is being performed, 2) and user verification based on the recognised action. One of the issues of this approach can be that users' activities will be continuously learnt which can seriously expose the user's privacy.

There have been a few works more recently that perform person authentication without activity recognition. Centeno et al. [26] proposed a Siamese Convolutional Neural Network (CNN) to learn the deep features that achieved an accuracy up to 97.8% by testing on the H-MOG dataset [9]. Neverova et al. [4] presented a continuous motion recognition system based on accelerometer and gyroscope data. Their method firstly transformed the observations into a new set of features based a customised Recurrent Neural Network (RNN) and estimated a general distribution using a Gaussian mixture model. The authors obtained an EER of 18.2% using a large self-collected dataset from 1500 volunteers. Sitová et al. [9] proposed an approach using accelerometer, gyroscope and touch-screen sensor data. A one-class SVM was used for classification. They created a dataset (H-MOG) from 100 users collected in a controlled environment where users were asked to perform three types of touchscreen activities while sitting and walking. They obtained an EER of 7.16% when the user was walking and 10.05% when the user was sitting. This dataset is currently one of very few publicly available datasets related to the research topic. More recently, Volaka et al. [34] applied an approach using a 3-dense layer neural network on extracted features from the raw sensor data. They analysed the performance of the approach using the H-MOG dataset. They split the data into different data modalities: only using touch-screen data, only using data from motion sensors and their combinations. They achieved an average accuracy of 88% with an EER of 15% when different modalities are combined, and the combination of touch (scroll) and gyroscope features gave a slightly better performance than other combinations of the data.

As part of the literature review, a few works have been found on continuous person authentication based on wrist-worn smartwatches. Very similar to the ideas presented based on smartphones, existing methods are based on gesture recognition [19], gait recognition [17][18][21], and activity recognition [17]. Most works only used the built-in accelerometer sensor in the smartwatch, but some also used the gyroscope [20]. One of the main challenges compared to smartphone is that the computation cannot be directly processed on the watch as the processing capability on a smartwatch is limited, but probably can be done on the connected phone instead. Also, in most of the previous work, the smartwatch needed to be worn on the dominant hand.

3.3 Discussion

This section discusses the advantages and challenges of smartphone sensor-based continuous person authentication methods.

Main advantages:

1. Passive - no particular user interaction/input required such as tapping/swiping on the screen
2. Continuous recognition, instead of one-time only recognition
3. Spoofing-resistant: human motion or activities are very difficult to be copied due to so many degrees of freedom, differences in body flexibility/weight/height/etc., and mood (even the same person is not able to perform the same motion exactly the same). Even professional actors cannot mimic another person's motion in the exact same way. Therefore, motion sensor-based person authentication could be considered as naturally spoofing-resistant.

Challenges and limitations:

1. There are currently very limited public datasets for training and validation of the developed approach. Neverova et al. [4] claims that issues have been found from previous research with data collection procedures due to inadequate amount and diversity of data, poor representation and description of real-world events, and crucially self-consciousness of the members participating for performing different activities
2. Alzubaidi and Kalita [3] mentioned that it is a challenge to collect mobile sensor data from a practical and legal standpoint. This means that privacy, ethical and legal requirements could be an issue for data collection and even use of this technology. This creates a research opportunity within this task to implement privacy and ethics "by-design" in the technology (smartphone apps) to be developed
3. Orientation and position sensitivity of smartphone inertial sensors, i.e. accelerometer and gyroscope, which means that results can be affected by the position and direction of phone on the user's body. Thus, data collection and training need to take this into account
4. Sensor data can be noisy, and affects learning the motion patterns
5. Incorporating real-time sensor data into a biometric authentication setup on a smartphone, which is limited in terms of memory and processing power on the phone
6. Although continuous authentication based on smartphone sensors may be naturally spoofing-resistant, it's also difficult to create spoofing data for testing
7. There are limited types of actions to define that can be used practically for enrolment and training, however, in a border crossing scenario this could be easy to solve as the most common action is walking

3.4 Resources

3.4.1 Datasets

There are very limited publicly available smartphone sensor datasets. Most of the datasets (listed in the table below) focus on readings on tapping/swiping on touchscreen while asking the users to perform activities such as text typing, i.e. there are no available datasets currently that exactly suit the purpose of border crossing scenarios.

TABLE 2 LIST OF PUBLIC SMARTPHONE SENSOR DATASETS

Dataset	No. of users	Action types	Data type	License agreement
H-MOG Dataset [9]	100	Tapping on screen events while sitting and walking	Sensor data: Accelerometer, gyroscope, and magnetometer	Online license agreement
BrainRun dataset [2]	2218	Screen tapping, and swiping	Sensor data: Accelerometer, gyroscope, magnetometer, device motion sensor Gesture data: while paying the game: taps, swipes Collected by a brain-training game ‘BrainRun’	Open Access
Yoneda [22]	51	18 actions	Sensor data: Accelerometer, gyroscope	Currently not accessible
CrowdSignals .io	30	Crowdsourced dataset, Recorded in 30 days All types of data from using smartphones	Labelled data: e.g. location, activity, etc.	Currently not accessible

3.4.2 Software

Both Android SDK and Apple iOS SDK provide tools to access the phone’s raw sensor data. There is also other third-party software that provides the ability for record sensor data. Tables below lists a few publicly available software/libraries that can be used for mobile development, accessing sensors collecting sensor data in real-time on the mobile phone, etc.

TABLE 3 LIST OF AVAILABLE OPEN SOURCE SOFTWARE THAT CAN BE USED FOR ACCESSING SMARTPHONE RAW SENSOR DATA

Library	Description	License	Platform	Features
SensingKit framework [7]	Framework for accessing sensor data	Open source	iOS, Andriod	Accelerometer, Gravity, Linear Acceleration, Gyroscope, Rotation, Magnetometer, Ambient Temperature, Step Detector, Step Counter, Light, Location, Activity, Battery, Screen Status, Audio Recorder, Audio Level, Bluetooth
Expo Sensors	APIs from open-source SDK Expo	Open source	iOS, Android	Accelerometer, Barometer, Gyroscope, Magnetometer, Pedometer
Pan Responder	Library for React Native framework	Open source	iOS, Android	Recognise multi-touch gestures, swipe, and other touch events on the mobile touchscreen

4 Scenario concept and machine learning-based approach

After the background study and state-of-the-art review, a scenario concept based on continuous person authentication for border control has been proposed. This section presents the designed scenario concept and proposes an approach based on neural networks.

4.1 Smartphone person authentication app

A smartphone app will be developed that can be installed in travellers' phones. The app will be triggered when the person enters the "biometric verification corridor" and starts the authentication process. The app will continuously read the sensor data from the mobile device and provides an authentication result for every given time window (e.g. every few seconds).

The app will only be started by the D4FLY border app, i.e. it cannot start as a standalone application. The app will not store or transmit any raw sensor data. Only scores/a decision will be output and sent to the D4FLY border app which will be used in the biometric fusion.

4.2 Continuous person authentication in D4FLY scenarios

In D4FLY deliverable D4.2 – System Architecture [28], four D4FLY scenarios are described:

- Scenario 1 - Enhanced document verification
- Scenario 2 - Highly automated border post
- Scenario 3 - Land border scenario
- Scenario 4 - Coach scenario

Among all four scenarios, Scenario 2 aims at proposing a border contol process that uses automated technology and enables travellers a smooth and on-the-move checking experience, including on-the-move biometric verification. As introduced above in Section 3, continuous person authentication based on smartphone sensors is a type of behavioural biometric, hence can be applied as a biometric trait. Therefore, the outcome from this task can contribute and be integrated to D4FLY scenario 2.

D4FLY scenario 2 contains two phases: enrolment and verication phases [28]. The detailed system architecture – the workflow and how different components are connnected in the whole system, is introduced in D4FLY deliverable D4.2 System architecture.

Figure 4 and Figure 5 illustrate the system architectures of the Enrolment and Verification phases, respectively, for scenario 2 introduced in D4FLY deliverable D4.2. A link is added in both diagrams to indicate the link with the continuous person authentication module - the UoR sensor controller. The UoR Android app will be installed on the same phone where the D4FLY VD Android app is installed.

During the enrolment phase:

- The traveller approaches the enrolment kiosk which is a supervised environment (please refer to D4FLY Deliverable 4.2 System Architecture [28] on the detailed description on the step-by-step enrolment procedure for Scenario 2)

- The UoR Android app will start running in enrolment mode by selecting the enrolment option on the D4FLY VD Android app
- The app will present on-screen instructions to the user: how to perform the enrolment process. The users will be asked to walk along the corridor for a few times while holding the phone or putting the phone in a pocket. Sensor data will be recorded while the person is walking.
- Once data are collected, the app will build a biometric template of the enrolled user on the background
- Once the whole enrolment process is completed, the enrolled biometric template will be sent via the communication route designed in Task 4.2 System architecture to the secure D4FLY storage server - please refer to D4.2 [28] and D4.6 (due in May 2022) for detailed communication strategy
- The UoR Android app will terminate on completion of all processes

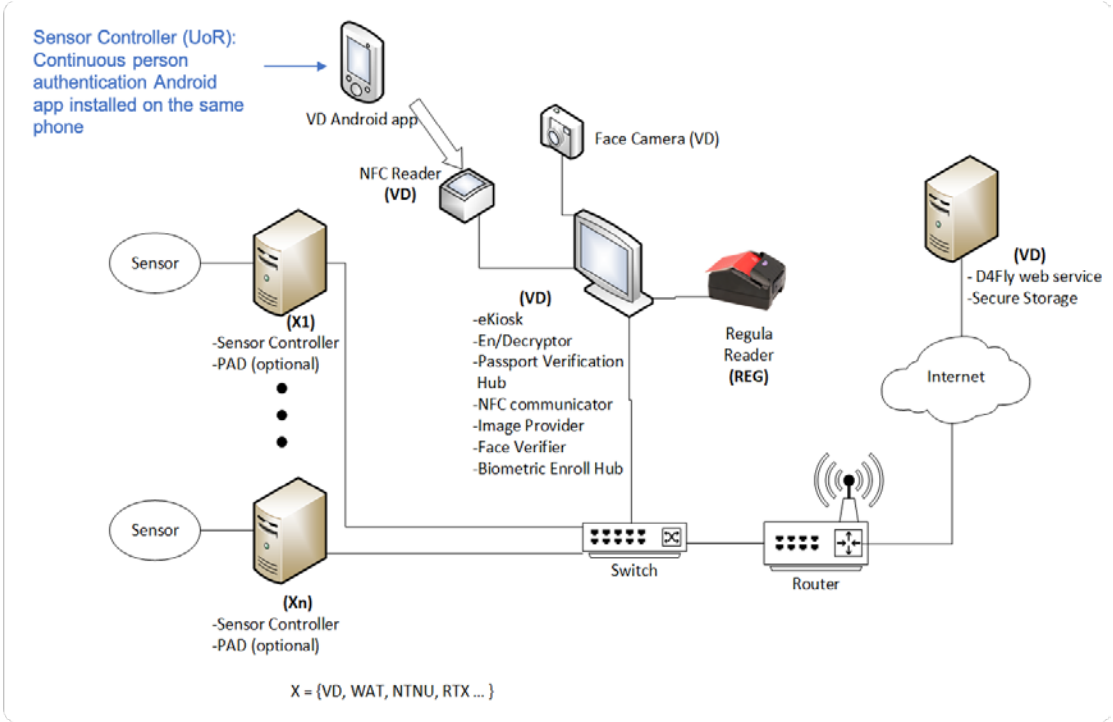

FIGURE 4 SYSTEM CONFIGURATION FOR ENROLMENT IN SCENARIO 2 [28] WITH ADDED LINK TO THE UOR CONTINUOUS PERSON AUTHENTICATION MODULE

During the verification phase:

- When the traveller enters the “biometric verification corridor”, the traveller will start the D4FLY VD Android app which will trigger the UoR continuous person authentication app (please refer to D4FLY Deliverable 4.2 System Architecture [28] on the detailed description of the step-by-step procedure for this phase in Scenario 2)
- The UoR app will start running in verification mode: sensor data (accelerometer, gyroscope, magnetometer, etc.) will be continuously read from the app; the app will calculate matching scores for every short (a few seconds) time window, i.e. the traveller will be continuously verified while walking along the corridor.

- Figure 6 provides a simple illustration of the traveller walking along the corridor while holding the phone
- A combined matching score/decision will be calculated based on all the output and sent via the communication route designed in Task 4.2 System architecture to the Biometric Fusion Module (BFM) for an overall decision – please refer to D4.2 [28] and D4.6 (due in May 2022) for detailed communication strategy
- The UoR Android app will terminate on completion of all processes

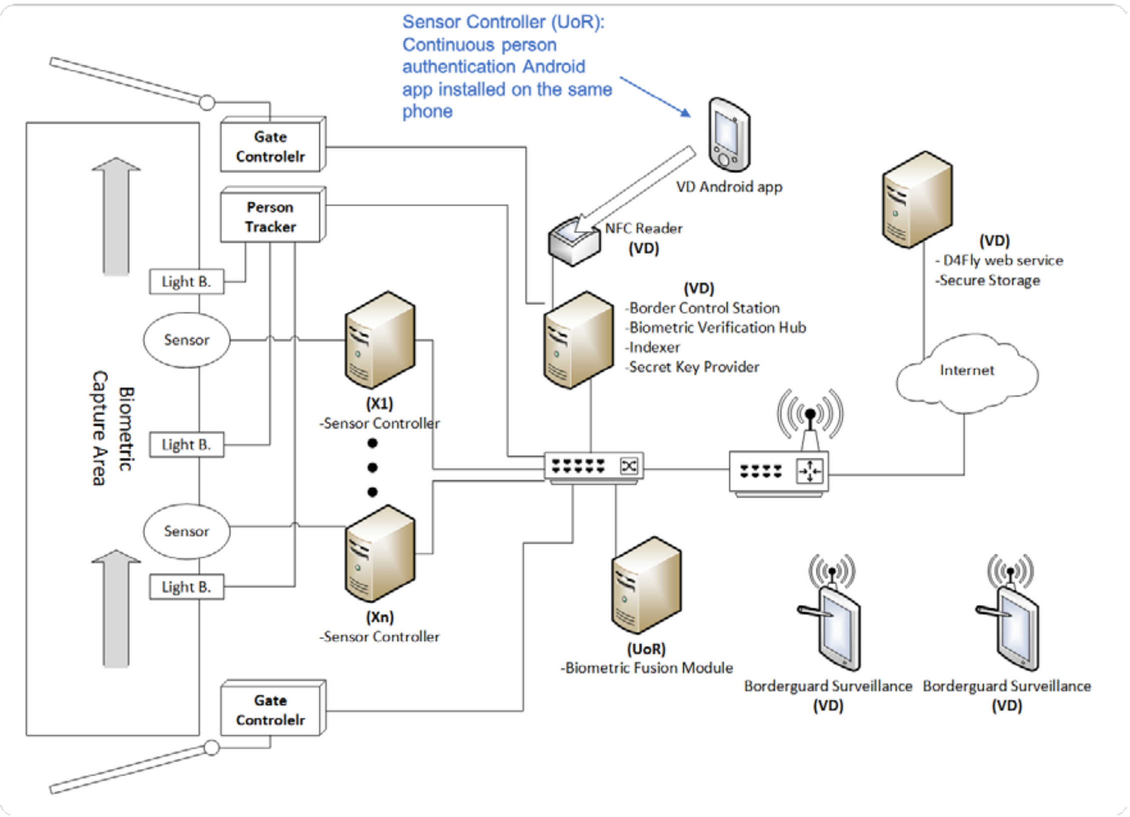

FIGURE 5 SYSTEM CONFIGURATION FOR VERIFICATION IN SCENARIO 2 [28] WITH ADDED LINK TO THE UOR CONTINUOUS PERSON AUTHENTICATION MODULE

Target timings

One of the main challenges of smartphone sensor-based person authentication is the need for a rapid decision. The overall system must have produced a decision by the time the user arrives at the end of the biometric verification corridor. The current length of the corridor is not yet specified, but it is reasonable to expect that most users would only spend around 10 to 20 seconds traversing the corridor (it is further reasonable to expect that a minority of users will spend even less time in the corridor if they are, for example, rushing to make a connection elsewhere in a transit area, so practically the system needs to make a decision as quickly as possible).

Current experimental results indicate that these timing constraints are achievable using offline processing. The next phase of this task includes as a main focus developing a dedicated smartphone app to read sensor data continuously whilst also performing person authentication. As smartphones have limited computing power available, one of the challenges of this future work will be to ensure that the timing constraints can be met with online processing.

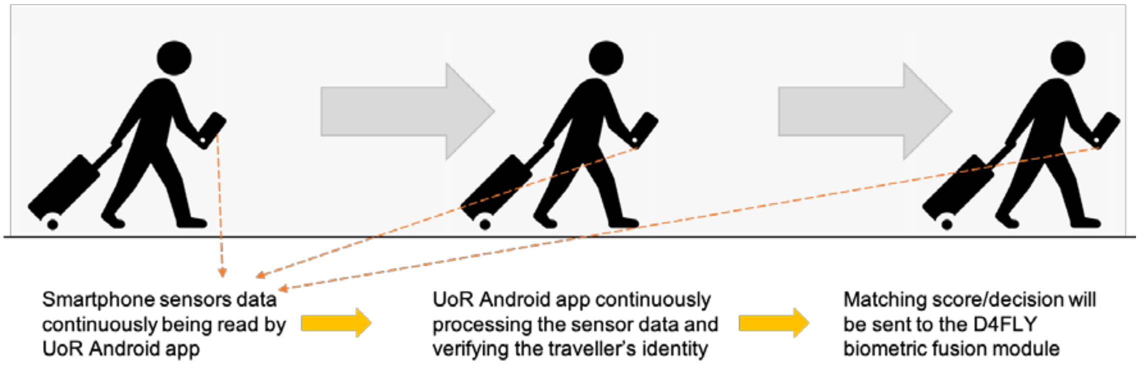
Smartphone sensors data continuously being read by UoR Android app
UoR Android app continuously processing the sensor data and verifying the traveller's identity
Matching score/decision will be sent to the D4FLY biometric fusion module

FIGURE 6 ILLUSTRATION OF THE CONCEPT OF SMARTPHONE BASED CONTINUOUS TRAVELLER AUTHENTICATION IN THE BIOMETRIC VERIFICATION CORRIDOR

4.3 Neural network-based approach

Pre-processing and windowing

Raw sensor data is inherently noisy due to limitations in the accuracy and response time of the underlying hardware. This was especially true for the H-MOG dataset as the sample frequency was not constant throughout a session varying between 2ms to over 5 seconds in some extreme cases (though practically the median sampling frequency was 100Hz). In their original work of H-MOG by Sitova et al. [9], 20 users were removed from their experiments due to the quality of the dataset [34].

As this experiment was to investigate the feasibility of the methodology, investigate multiple potentially useful datasets (HCI-HAR and H-MOG) and to develop an architecture toolchain for rapid prototyping and training of different network architectures, only minimal data cleaning techniques were applied to the H-MOG dataset (HCI-HAR had already been pre-processed). The dataset was first resampled to a consistent 50Hz using linear interpolation. Noise reduction was then implemented using a median filter and a 3rd order low-pass Butterworth filter with a corner frequency of 20Hz [27]. No users were excluded from the experiments. The sensor data was divided into a series of windows of fixed width (currently 2.56 seconds) to be used as input to the neural network. Successive windows overlap by 50%.

CNN LSTM network

A Recurrent Neural Network (RNN) is a type of artificial neural network that is designed to learn and recognise patterns in sequential data. They have been applied successfully for processing sequential data in various fields, e.g. text recognition, speech recognition, human action recognition, sensor data analysis, stock prediction, etc. The dynamic nature of recurrent models allows for modelling richer temporal structures and better discrimination among users acting under different conditions [4].

Considering the nature of the smartphone sensor data, which are multi-axis time-series data, an RNN network seems to be a good choice to learn the patterns presented by each user when they are using the phone. A Long Short-Term Memory (LSTM) network is a variant of an RNN network designed to be able to learn and remember over long sequences of input data whilst still being responsive to short-term changes in the sequence, and can support multiple parallel sequences of input data, such as three-axis data of the accelerometer and gyroscope. They have, so far, been one of the best performing models for learning long-term temporal dependencies. Figure 7 illustrates the architecture of a single LSTM cell. The LSTM cell reads input from a data stream, and provides output, but it also makes available the cell's internal state to the next iteration (hence "memory"). The LSTM cell uses a mechanism called "gates" to control what information is relevant from the past and can therefore adapt the relevant weighting of long-term and short-term trends (hence "long short-term") based on its inputs.

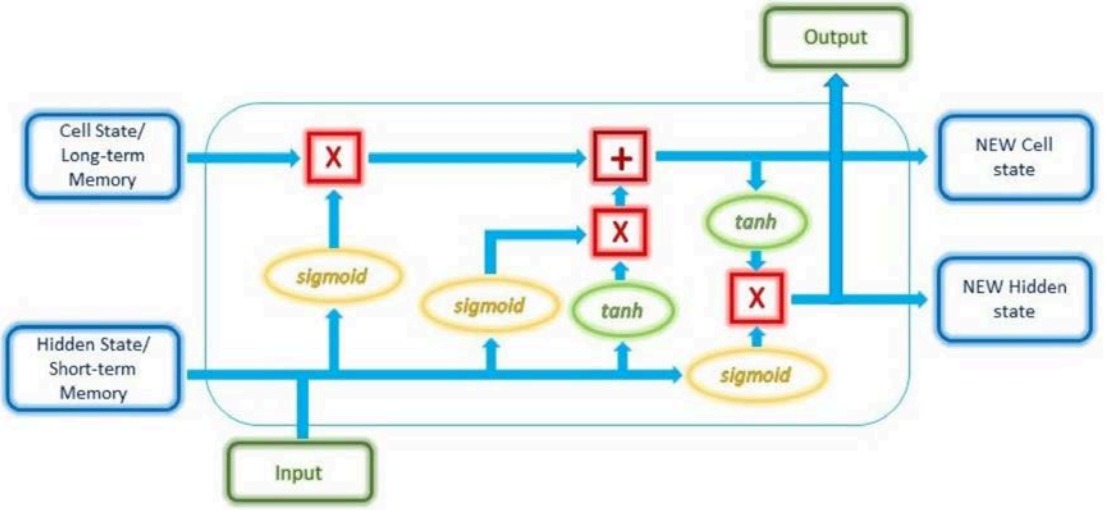

FIGURE 7 ARCHITECTURE OF A SINGLE LSTM CELL

Sainath et al. [31] claims that one challenge with LSTMs is that the temporal modelling is done on the input feature. Higher-level modelling can help to disentangle underlying factors of variation within the input, which should then make it easier to learn temporal structure between successive time steps. They presented the power of combining convolutional neural networks (CNN) and LSTM networks into a unified architecture.

1-dimensional convolutional networks have been used for modelling temporal structure in tasks like speech recognition. In this task, a network combining a multi-scale 1D CNNs with a LSTM network is applied to learn the patterns from the sensor data. Figure 8 presents the overview of the proposed approach for continuous person authentication based on smartphone sensors.

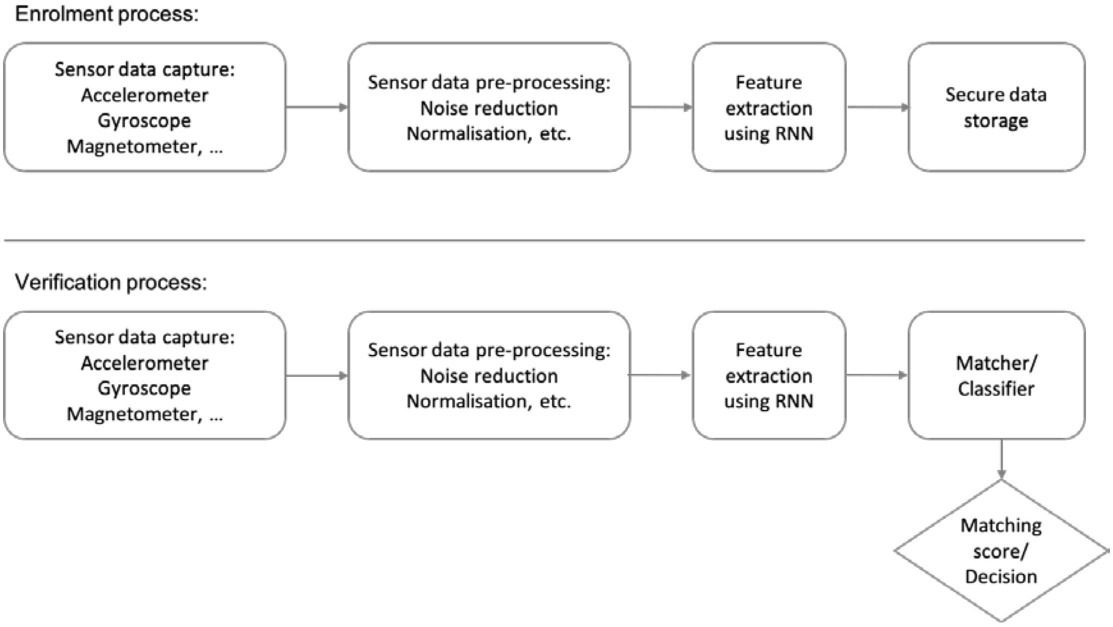
Enrolment process:
Sensor data capture: Accelerometer Gyroscope Magnetometer, ...
Sensor data pre-processing: Noise reduction Normalisation, etc.
Feature extraction using RNN
Secure data storage
Verification process:
Sensor data capture: Accelerometer Gyroscope Magnetometer, ...
Sensor data pre-processing: Noise reduction Normalisation, etc.
Feature extraction using RNN
Matcher/ Classifier
Matching score/ Decision

FIGURE 8 ARCHITECTURE OF THE PROPOSED APPROACH: TOP - ENROLMENT PROCESS; BOTTOM – VERIFICATION PROCESS

4.4 Experiments and evaluation

4.4.1 Datasets

Two public datasets were used for the initial experiments and evaluation of the approach: HCI-HAR [27] and H-MOG [9].

The HCI-HAR dataset was generated for the purposes of human action recognition using smartphones. It is a relatively small dataset consisting of 30 users. As the dataset was developed for training action types, and not for discriminating between different users, there was not sufficient depth to the data for the per-user scenario (e.g. not every user performed every action, which means that the network cannot learn the difference between users for that action). However, this dataset was sufficient for initial experiments and testing with the limited usable datasets publicly available. The dataset contains 6 types of actions performed by the volunteers: walking, walking upstairs, walking downstairs, sitting, standing and lying. Two types of sensors (accelerometer and gyroscope) were recorded. The accelerometer data were pre-processed and split into acceleration due to gravity and acceleration due to the motion of the device.

The H-MOG dataset consists of 100 users and was created for smartphone user authentication when the user is directly interacting with the phone. Real-time touch, sensor, and keypresses were recorded while the user performed one of the three types of actions: 1) document reading, 2) text typing, and 3) navigation on a map. These actions were further recorded in two posture scenarios: sitting and walking. The dataset consists of 3 motion sensors (accelerometer, gyroscope, magnetometer), as well as various touchscreen events (touch, tap, scale, scroll, fling, and keypress). The sensor data were presented raw, with no pre-processing and appear to be recorded isochronously, and the time between subsequent samples can vary significantly. Thus, pre-processing was necessary for this dataset. As the dataset were created under two scenarios: walking and sitting, the data were developed into three sets: walking, sitting and combined.

4.4.2 Results and discussion

Only the accelerometer and gyroscope data were used from either dataset during the experiments as the HCI-HAR dataset only provides these two sensors. In future work, evaluation will be performed where more sensors are included. Data were split into training set and test set: 70% of the data formed the training set and 30% of the data formed the test set. Table 4 below presents the results from the initial experiments using the two datasets. The results are reported in classification accuracy: the percentage of all correctly classified samples from the test set in terms of the person IDs present in the training data against the total number of samples in the test set.

Between the two datasets, the overall classification accuracy is higher for the HCI-HAR dataset than for the combined H-MOG dataset. This is probably due to the HAR data being collected in a lab-controlled environment using a waist-worn belt. However, due to limited number of training samples for person-wise training in HCI-HAR dataset, the overall classification accuracy is not very high. The high accuracy from the H-MOG walking scenario is probably due to the larger volume of data available for training.

Within the H-MOG dataset, the walking scenario achieved the highest accuracy. This is probably due to the richer motion cues available from walking; conversely the low accuracy of the sitting scenario is likely due to the accelerometer and gyroscope data being less discriminative sensors when the user is not moving significantly (magnetometer and touchscreen events were not used for these experiments).

These experiments attempted to investigate the feasibility of applying continuous person authentication in a border control scenario. The developed network would form the basis of the full authentication solution, and whilst the objective is to achieve as high an accuracy as possible, it should be considered that the network is being trained primarily to identify ways of generating discriminating features for identifying people.

TABLE 4 EXPERIMENT RESULTS USING HCI-HAR AND H-MOG DATASETS

Dataset	Number of users	Accuracy
HCI-HAR dataset	30	~83%
H-MOG dataset (sitting scenario)	100	~74%
H-MOG dataset (walking scenario)	100	~88%
H-MOG dataset (combined)	100	~78%

The results shown above (Table 4) are promising considering the constraints of the feasibility study. This illustrates the potential of the continuous authentication approach for integration into the D4FLY biometric verification control scenario and will hopefully increase biometric verification confidence and complement the overall accuracy. From current experiments, 10s walking along the corridor should provide enough time for producing a reliable authentication result in terms of the D4FLY biometric verification corridor use case, though these results are for offline processing. Future work will involve more experiments and evaluation to improve the accuracy and overall performance and focus on the practicality of real-time operation for demonstrators.

5 Conclusions and next steps

In this deliverable, the objectives of Task 6.1 have been introduced. The current status and progress of the work carried out during the first period has been reported. A background study and literature review were completed for the topic on continuous person authentication based on smartphone sensors. Based on the outcome, a scenario concept was designed and proposed to include smartphone person authentication as an alternative biometric modality in the D4FLY biometric corridor scenario. An Android app was developed and is fully functional for collecting smartphone sensor data in two modes: standalone and remote control. An RNN-based approach was proposed, implemented, and tested on a public dataset; achieving promising results.

As mentioned above, continuous person authentication based on smartphone sensors has been a relatively new research area, especially in its application for border control. Thus, there are still many things to explore and investigate. The next steps are to focus on improving the authentication accuracy, and practical solutions for implementation of the technology into the demonstrators:

- To use the developed smartphone app to build a dataset specific to the D4FLY scenario for algorithm testing
- To improve the current RNN based algorithm for continuous person authentication and the overall accuracy
- To develop the UoR smartphone app for continuous person authentication
- To investigate the practicality of running the verification process on the smartphone phone alone – can real-time verification be achieved with the available computing resources on the smartphone, and to identify alternative solutions if not. This means that by the time the user gets to the end of the biometric verification corridor, a result should have been produced based on the sensor data and any computation required
- As mentioned above in Section 3.3, continuous person authentication may be naturally spoofing resistant; but further effort will be spent investigating this topic in depth
- To focus on integrating the developed technology into the D4FLY scenarios, field tests and demonstrators
- To fully evaluate the performance of the final solution

REFERENCES

[1] B. Chakraborty, K. Nakano, Y. Tokoi and T. Hashimoto, "An Approach for Designing Low Cost Deep Neural Network based Biometric Authentication Model for Smartphone User," TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 772-777

[2] Papamichail, M.D.; Chatzidimitriou, K.C.; Karanikiotis, T.; Oikonomou, N.-C.I.; Symeonidis, A.L.; Saripalle, S.K. BrainRun: A Behavioral Biometrics Dataset towards Continuous Implicit Authentication. Data 2019, 4, 60.

[3] A. Alzubaidi and J. Kalita, "Authentication of Smartphone Users Using Behavioral Biometrics," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1998-2026, thirdquarter 2016.

[4] N. Neverova et al., "Learning Human Identity From Motion Patterns," in IEEE Access, vol. 4, pp. 1810-1820, 2016.

[5] Ehatisham-ul-Haq, Muhammad, Muhammad Awais Azam, Jonathan Loo, Kai Shuang, Syed Islam, Usman Naeem, and Yasar Amin. 'Authentication of Smartphone Users Based on Activity Recognition and Mobile Sensing'. Sensors 17, no. 9 (6 September 2017): 2043. https://doi.org/10.3390/s17092043.

[6] CrowdSense, https://www.sensingkit.org/projects.html

[7] DataCollector App, https://github.com/seemoo-lab/seemoo-mobile-sensing

[8] SensingKit framework, https://github.com/SensingKit/SensingKit-Android/blob/master/README.md

[9] Sitová, Zdeňka, Jaroslav Šeděnka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, and Kiran S. Balagani. 'HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users'. *IEEE Transactions on Information Forensics and Security* 11, no. 5 (May 2016): 877–92.

[10] Derawi, Mohammad Omar, Claudia Nickel, Patrick Bours, and Christoph Busch. 'Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition'. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 306–11. Darmstadt, Germany: IEEE, 2010.

[11] Frank, Mario, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 'Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication'. *IEEE Transactions on Information Forensics and Security* 8, no. 1 (January 2013): 136–48.

[12] Serwadda, Abdul, Vir V. Phoha, and Zibo Wang. 'Which Verifiers Work?: A Benchmark Evaluation of Touch-Based Authentication Algorithms'. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 1–8, 2013.

[13] Bo, Cheng, Lan Zhang, and Xiang-Yang Li. 'SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics', 31 August 2013.

[14] Shi, Weidong, Jun Yang, Yifei Jiang, Feng Yang, and Yingen Xiong. 'SenGuard: Passive User Identification on Smartphones Using Multiple Sensors'. In *2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 141–48, 2011.

[15] Zheng, Nan, Kun Bai, Hai Huang, and Haining Wang. 'You Are How You Touch: User Verification on Smartphones via Tapping Behaviors'. In *2014 IEEE 22nd International Conference on Network Protocols*, 221–32, 2014.

[16] Gascon, Hugo, Sebastian Uellenbeck, Christopher Wolf and Konrad Rieck. “Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior.” Sicherheit (2014).

[17] M. Ahmad *et al.*, ‘Smartwatch-Based Legitimate User Identification for Cloud-Based Secure Services’, *Mobile Information Systems*, 2018.

[18] Davidson, Scott, Derrick Smith, Chen Yang and Siew Cheong Cheah. “Smartwatch User Identification as a Means of Authentication.” (2016).

[19] Yang, Junshuang, Yanyan Li, and Mengjun Xie. 2015. ‘MotionAuth: Motion-Based Authentication for Wrist Worn Smart Devices’. In *2015 IEEE International Conference on* Pervasive Computing and Communication Workshops (PerCom Workshops), 550–55.

[20] G. M. Weiss, K. Yoneda and T. Hayajneh, "Smartphone and Smartwatch-Based Biometrics Using Activities of Daily Living," in IEEE Access, vol. 7, pp. 133190-133202, 2019.

[21] A. H. Johnston and G. M. Weiss, "Smartwatch-based biometric gait recognition," 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), Arlington, VA, 2015, pp. 1-6.

[22] K. Yoneda and G. M. Weiss, "Mobile sensor-based biometrics using common daily activities," 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), New York, NY, 2017, pp. 584-590.

[23] Yang, Qing, Ge Peng, David T. Nguyen, Xin Qi, Gang Zhou, Zdenka Sitova, Paolo Gasti and Kiran S. Balagani. “A multimodal data set for evaluating continuous authentication performance in smartphones.” SenSys (2014).

[24] M. P. Centeno, A. v. Moorsel and S. Castruccio, "Smartphone Continuous Authentication Using Deep Learning Autoencoders," 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, 2017, pp. 147-1478.

[25] S. P. Banerjee and D. L. Woodard, “Biometric authentication and identification using keystroke dynamics: A survey,” Journal of Pattern Recognition Research, vol. 7, no. 1, pp. 116–139, 2012.

[26] Mario Parreño Centeno, Yu Guan, and Aad van Moorsel. 2018. Mobile Based Continuous Authentication Using Deep Features. In Proceedings of the 2nd International Workshop on Embedded and Mobile Deep Learning (EMDL’18). Association for Computing Machinery, New York, NY, USA, 19–24.

[27] Davide Anguita, Alessandro Ghio, Luca Oneto, Xavier Parra and Jorge L. Reyes-Ortiz. A Public Domain Dataset for Human Activity Recognition Using Smartphones. 21th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, ESANN 2013. Bruges, Belgium 24-26 April 2013.

[28] D4FLY deliverable: D4.2 System architecture

[29] D4FLY deliverable: D3.2 Privacy and Data Protection Impact Assessment, submitted in April 2020

[30] Image obtained on Stride website on 16th May 2020, https://doc.xenko.com/latest/en/manual/input/sensors.html

[31] T. N. Sainath, O. Vinyals, A. Senior and H. Sak, "Convolutional, Long Short-Term Memory, fully connected Deep Neural Networks," 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brisbane, QLD, 2015, pp. 4580-4584

[32] H. Li, J. Yu and Q. Cao, "Intelligent Walk Authentication: Implicit Authentication When You Walk with Smartphone," 2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Madrid, Spain, 2018, pp. 1113-1116

[33] B. Chakraborty, "Gait Related Activity Based Person Authentication with Smartphone Sensors," 2018 12th International Conference on Sensing Technology (ICST), Limerick, 2018, pp. 208-212

[34] Hasan Can Volaka, Gulfem Alptekin, Okan Engin Basar, Mustafa Isbilen, Ozlem Durmaz Incel, Towards Continuous Authentication on Mobile Phones using Deep Learning Models, Procedia Computer Science, Volume 155, 2019, Pages 177-184, ISSN 1877-0509

LIST OF FIGURES

LIST OF TABLES