University of Sheffield

Continuous Authentication of Users to Robotic Technologies Using Behavioural Biometrics

Shurook S. Almohamade

A thesis submitted in partial fulfilment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in the

The University of Sheffield
Department of Computer Science

November 2022

Declaration

I Shurook S. Almohamade, confirm that the Thesis is my own work. I am aware of the University's Guidance on the Use of Unfair Means (www.sheffield.ac.uk/ssid/ unfair-means). This work has not been previously been presented for an award at this, or any other, university. Some parts of this thesis have been published by the author.

Shurook S. Almohamade

Acknowledgments

The work in this thesis would not even be accomplished without the support of many people. It gives me great pleasure to thank everyone who has helped me over the previous four years.

My PhD supervisors, Professor John A. Clark and Dr James Law deserve my heartfelt gratitude for their unending support, direction, encouragement, patience, and extensive expertise during my PhD studies.

No words can adequately describe my heartfelt thanks to my supportive and understanding husband, Mohammed, for his unwavering love, support, and understanding before and during my PhD studies. He has always been the one on whom I can rely at all times. Likewise, thank you to my beautiful daughter Yara, who is the light of my life. With her, I gained strength and became more productive during my PhD study.

I owe a debt of thankfulness to my parents for their compassion and love and steadfast trust in me, as well as to my brothers and sisters for their spiritual support during the writing of my thesis and in my life in general.

At last, I would want to express my heartfelt thanks to Taibah University (Saudi Arabia) for providing financial support for my studies.

Abstract

Collaborative robots and current human–robot interaction systems, such as exoskeletons and teleoperation, are key technologies with profiles that make them likely security targets. Without sufficient protection, these robotics technologies might become dangerous tools that are capable of causing damage to their environments, increasing defects in work pieces and harming human co-workers. As robotics is a critical component of the current automation drive in many advanced economies, there may be serious economic effects if robot security is not appropriately handled. The development of suitable security for robots, particularly in industrial contexts, is critical.

Collaborative robots, exoskeletons and teleoperation are all examples of robotics technologies that might need close collaboration with humans, and these interactions must be appropriately protected. There is a need to guard against both external hackers (as with many industrial systems) and insider malfeasance. Only authorised users should be able to access robots, and they should use only those services and capabilities they are qualified to access (e.g. those for which they are appropriately cleared and trained). Authentication is therefore a crucial enabling mechanism. Robot interaction will largely be ongoing, so continuous rather than one-time authentication is required.

In robot contexts, continuous biometrics can be used to provide effective and practical authentication of individuals to robots. In particular, the working behaviour of human co-workers as they interact with robots can be used as a means of biometric authentication.

This thesis demonstrates how continuous biometric authentication can be used in three different environments: a direct physical manipulation application, a sensor glove application and a remote access application. We show how information acquired from the collaborative robot's internal sensors, wearable sensors (similar to those found in an exoskeleton), and teleoperated robot control and programming can be harnessed to provide appropriate authentication. Thus, all authentication uses data that are collected or generated as part of the co-worker simply going about their work. No additional action is needed. For manufacturing environments, this lack of intrusiveness is an important feature.

The results presented in this thesis show that our approaches can discriminate appropriately between users. We believe that our machine learning-based approaches can provide reasonable and practical solutions for continually authenticating users to robots in many environments, particularly in manufacturing contexts.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

The use of robots in manufacturing processes is increasing. According to the World Robotics 2021 Industrial Robots report [71], the world now has a record 3 million industrial robots operating in factories, respresenting a 10% increase over the previous year. Despite the worldwide epidemic, new robot sales increased modestly by 0.5 percent, with 384,000 units sold globally in 2020.

Cybersecurity for robotics is becoming a critical issue as robots become more prevalent and connected, for instance, to external networks and wider infrastructure. Particular concerns arise in applications in which humans and robots operate in very close proximity, e.g. within shared spaces, or work alongside one another, where there are greater safety and personal data security risks. This occurs increasingly in industrial settings but could also occur in the home, office or public locations and in applications spanning manufacturing, healthcare, delivery & logistics, hospitality, education and entertainment.

One of the main vulnerabilities in modern robots is inadequate user authentication protocols [39]. Authenticating users is key to ensuring that only permitted users have control over or access to the data handled by a particular device or access to the capabilities that a device can provide. In an industrial setting, this could be done to ensure that only trained users have the ability to change control parameters on a robot or access specific services and functionalities. In a healthcare scenario, the purpose is to ensure that patient data are shared only with authorised medical practitioners or that a patient is the intended recipient of a specific care regime.

Currently, authentication mechanisms in such user–robot collaborations, if there are any at all, are often one shot (e.g., pin codes, passwords or ID/access cards). Although one-shot approaches may give confidence that the user supplying the credentials is who they claim to be at the time of authentication, such confidence recedes as time elapses. We might, for example, believe that there is a significant risk of the authenticated user leaving their terminal or other devices unattended. This problem is often addressed by requiring the user to re-authenticate at intervals. However, in many industrial contexts, repeated authentication may be highly inconvenient and disruptive (e.g. if a user has to take off protective gloves in order to enter a password or if the user's collaborative task has reached a critical point).

In this regard, biometric systems and continuous authentication (CA) methods can play major roles. Biometrics is essentially about the ability of a person to be recognised. This recognition may then be used to provide access to systems [44]. Users' biometric features can be divided into physiological and behavioural traits. Physiological traits refer to users' physical attributes, including their fingerprints, facial features, iris patterns, retinal patterns, vascular patterns, palm prints, DNA, ear geometry and hand geometry. Behavioural traits refer to attributes such as typing habits, voice patterns, signatures, gait and behavioural profile. CA is an approach used to verify an individual's identity and thus facilitate cybersecurity protection on a continuous basis. CA checks users not only once but continuously throughout a session. It often uses machine learning (ML), and a number of components include behavioural patterns and biometrics to provide a smart, secure verification process without disrupting the workflow.

1.2 Research Hypothesis

The research hypothesis investigated in this thesis is as follows:

- Continuous biometrics can form the basis for the effective and practical authentication of users operating in close collaboration with robots.

1.3 Contributions of Our Research

This thesis examines the security issues associated with three different robotics technologies: collaborative robots, exoskeletons and teleoperation. More precisely, we are motivated by the necessity to develop useful and secure methods of user authentication for collaborative robots, as well as the potential for securing current human–robot interaction (HRI) systems, such as exoskeletons and teleoperation.

The following contributions are made by this thesis:

1. We propose a new approach that uses a robot arm's joint information (i.e. position, force and torque) as biometric authentication data during direct physical manipulation by the human operator. Our technique, which is based on ML and an established trust model, can provide a reasonable, practical solution for continually authenticating users who engage physically with a collaborative robot. Additionally, it uses data that the collaborative robot already maintains as part of its normal activity. Our research (see Chapter 3) is the first to make use of such data.

2. We propose a technique for continuous behavioural biometrics that rely on the data collected by wearable sensors (hand manipulations captured by a sensorised glove) while the user conducts a variety of industrial activities, such as loading and inserting screws.

The results indicate that the technique is capable of discriminating between users with a low equal error rate. This method, we believe, will also improve other applications in which wearables are used to operate robots, such as teleoperation or sophisticated exoskeletons.

3. We examine how continuous user behaviour monitoring may be used to provide unobtrusive continuous user authentication for remotely operated systems. To collect data, we run a simulation in which a group of users manually leads a robotic manipulator through a task (similar to teaching by demonstration or teleoperation), with some users masquerading as malicious agents. We then put our CA approach to the test against a common behavioural biometric threat known as a mimicry attack.

4. We generate two datasets for user interaction with collaborative robots in two different scenarios:

   (a) A collaborative robot dataset based on physical interaction (see Chapter 3). This dataset contains 30 users (with each user performing 15 tasks).

   (b) A collaborative robot simulation dataset (see Chapter 5). This dataset contains 32 users, each of whom is responsible for 15 tasks. Additionally, this dataset contains 384 attacks by 16 attackers and 48 video recordings of 16 victims.

1.4 Publications

The work reported in this thesis has given rise to the following publications:

1. Almohamade, Shurook S., John A. Clark, and James Law. "Behaviour-Based Biometrics for Continuous User Authentication to Industrial Collaborative Robots." International Conference on Information Technology and Communications Security. Springer, Cham, 2020. This work is reported in chapter 3. The URL for the electronic version of this publication is: `https://link.springer.com/chapter/10.1007/978-3-030-69255-1_12`

2. Almohamade, Shurook, John Clark, and James Law. "Continuous User Authentication for Human-Robot Collaboration."The 16th International Conference on Availability, Reliability and Security". 2021. Association for Computing Machinery, New York, NY, USA, Article 115, 1–9. DOI:https://doi.org/10.1145/3465481.3470025. This work is reported in chapter 4. The URL for the electronic version of this publication is:`https://dl.acm.org/doi/abs/10.1145/3465481.3470025`

3. Almohamade, Shurook S., John A. Clark, and James Law. "Mimicry Attacks Against Behavioural-Based User Authentication for Human-Robot Interaction."The 4th International International Workshop on Emerging Technologies for Authorization and Authentication". Springer, Cham, 2021. This work is reported in chapter 5. The URL

for the electronic version of this publication is:https://link.springer.com/chapter/10.1007/978-3-030-93747-8_8

In addition, most of the data, codes and videos used in this thesis were released publicly and can be found at https://github.com/SSAlmohamade

1.5 Ethical Considerations

We obtained approval from the University of Sheffield Research Ethics Committee, as is required for any experiments involving human volunteers. Under reference number 024354, approval has been given.

1.6 Thesis Outline

This thesis is structured as follows:

In **Chapter 2**, we present a systematic literature review that addresses relevant research topics in the literature, including the security of robotics, authentication, biometric authentication and CA.

In **Chapter 3**, we investigate CA methods in the use of collaborative robot manipulators.

In **Chapter 4**, we investigate the implementation of continuous behavioural biometric authentication using wearable sensors similar to those found in an exoskeleton or teleoperation system.

In **Chapter 5**, we investigate CA using behavioural biometrics in the context of industrial and teleoperated robot control. We consider a scenario in which attackers are informed about their victims' behavioural tendencies and make conscious attempts to imitate them.

Chapter 6 summarises this study's major findings, emphasising both its accomplishments and limitations. The chapter also discusses future research.

Chapter 2

Background and Literature Review

2.1 Security of Robotics: Vulnerabilities, Threats and Risks

Robotics is a large area of research and development with applications in many fields, such as medicine, manufacturing, security, aeronautics, military, transportation and entertainment. Robots can serve, assist and enhance human life [143]. However, many accidents have occurred, resulting in severe injuries and tragic consequences, such as the avoidable loss of human life [211]. Accidents will always occur, but malicious attacks provide a unique set of challenges. They involve significant economic and financial damages by maliciously hijacking and manipulating robots [159][211].

The purpose of this section is to highlight the robotic domain's vulnerability to the number of security and safety risks that may result in hazardous attacks.

2.1.1 Security Vulnerabilities

Many robotic vulnerabilities may be used to attack robotic systems and applications [39]. This section presents several security issues that are challenging:

- Insecure networking makes communication between robots and humans vulnerable [214].
- Inadequate authentication leads to unauthorised access through common usernames and passwords, which a determined attacker may easily compromise. [27],[39],[128].
- Lack of authorisation (physical access to robotics laboratories, factories and industries) results in unprotected robot functionality, including critical functions, such as application installation and operating system software updates. This allows an attacker to install software on robots without permission and to gain complete control over them [39].
- Lack of confidentially is caused by the implementation of insecure encryption methods that expose sensitive robotics data [39].

Table 2.1: Attacks against robots (Maggi et al. [128])

Attack Class	Concrete Effect
Altering Control-Loop Parameters	Defective or Modified Products
Tampering with Calibration Parameters	Damage to Robots
Tampering with the Production Logic	Defective or Modified Products
Altering the User-Perceived Robot State	Injuries to Operators
Altering the Robot State	Injuries to Operators

2.1.2 Security Threats

Threats may come from two main sources: physical attacker and network attacker [128]. The robot operator (insider), who utilises the robot's manual interface on a regular basis to pilot and program it, is the simplest and most typical profile of a physical attacker [128]. Robotic systems may potentially be physically damaged and destroyed by insiders. In this case, the attacker can physically access the robot's manual interface. Then, the attacker reprogrammes the robot or evens steals its data [107]. Network attackers target the network connection [159] [128] to get access to information for malicious reasons, cause system malfunction or interrupt services by injecting false or malicious data [211].

2.1.3 Security Risks

Robots are data-driven technologies, and a cyberattack may endanger their functionality and the safety of their users. For example, shutting down a robot surgeon in the middle of a surgery might endanger the procedure's success [5]. Security flaws may disrupt the regular processing and functioning of industrial robots and could interrupt production and industrial operations, resulting in financial losses. More specifically, they may result in system obstruction, data theft and physical harm [159]. Physical theft, hijacking and control of robotic equipment are also possible. One example is the de-authentication procedure, which enables malicious users to disconnect legal owners and re-control devices (i.e. robots and drones) [210]. In the paper by Trend Micro, Maggi et al. [128] identified five types of robot-specific attacks (see Table 2.1) that may have impacts on both operational and functional safety and security processes, putting the lives of their human operators in danger and resulting in defects to products and damage to robots.

2.2 Human–Robot Interaction (HRI)

HRI is an area of research devoted to understanding, developing and evaluating the robotic systems used by or in collaboration with humans.

The interactions between a human and a robot may take many forms but are significantly affected by proximity. As a result, interaction may be divided into two broad categories [81]:

1. **Proximate interaction** – In this scenario, humans and robots are co-located; robots

would be in the same room as humans are. Proximate interaction can include physical interaction, but this is not essential.

2. **Remote interaction** – Humans and robots are physically or even temporally apart. Teleoperation or supervisory control is often used to refer to remote interaction, but with a physical interface.

Several robotics technologies require closely coupled, proximal/physical interaction, such as collaborative robots, robotic exoskeletons and robotic teleoperation.

2.2.1 Collaborative Robots

Collaborative robots are designed to assist human workers in a variety of work tasks by interacting with them in a cooperative manner [46]. They can be defined as a type of robot that collaborates with humans as assistants or guides in a specific task, especially when the task can utilise both human and robotic benefits. These robots are designed with a number of technical features to ensure that they do not cause damage, either deliberately or inadvertently, when a worker comes into direct contact with them [56].

A key difference between collaborative robots and traditional (non-collaborative) ones is that traditional robots work are required to be segregated from human users (e.g. by safety barriers or fences). However, collaborative robots are designed to work with humans in the same work area and can respond to human behaviours or actions. Collaborative robots have many benefits compared with traditional robots [85] [106] [56] [155] [166] [205] [93], which are as follows:

1. **Productive and convenient robots.** Collaborative robots are considered productive robots. At the same time, they are convenient because they combine a computer's precision and a human worker's skill and experience.

2. **Safe interaction with humans.** Industrial robots follow a programme without regard for the humans working nearby. Special fences and barriers are installed in the workplace to avoid accidents. Recently, the expectations of making humans safely work with collaborative robots in direct contact without needing additional safety measures have grown. No protective barriers are needed while utilising them.

3. **Reduced risk in the performance of hazardous tasks.** Collaborative robots carry out tasks that are potentially dangerous to humans. These risks include interfacing with dangerous machinery and/or manipulating dangerous materials and tooling.

4. **Learning and flexibility.** Industrial robot control needs specialised programming abilities. Collaborative robot programming has become simpler. Collaborative robots are easy to train and programme, flexible and capable of assisting in repetitive, boring and complex tasks.

5. **Wide application and fast adjustment.** Collaborative robots are simple to transfer and utilise at different locations in the manufacturing chain. Different types of robots may need to be installed on any surface horizontally or vertically.

6. **Affordable solution.** Some tasks may be too difficult or costly to completely automate by robots. The most flexible and cost-effective option is for a human worker to help and share such tasks with robots.

7. Collaborative robots also **provide an economically feasible starting point** for robotic automation. For example, collaborative robots can provide opportunities for productivity and quality improvements (e.g. in small to medium-sized manufacturers). They can also provide support to workers in the completion of final assembly tasks (e.g. in automotive manufacturing).

Types of Collaboration with Industrial Robots

The term 'human–robot collaboration' refers to the use of robots without protection fencing, i.e. cage-free robots. The interaction types in the shared work space can be categorised into five cases according to the task specified in the application [20]. The five types of interactions between human workers and robots are cell, coexistence, synchronised, cooperation and collaboration [20]. The type **cell** is not a real situation of collaboration because the robot is operated in a conventional cage. In **coexistence**, the human and cage-free robot work side by side but do not share a workspace. In **synchronised** interaction, the workflow architecture features synchronised robot and human interaction in a single workspace, but only one of the participants is physically present in the workspace at any given time. In **cooperation** interaction, the two contact partners may do activities concurrently in the (shared) workspace but do not operate on the same product simultaneously. In **collaboration** interaction, the human worker and robot work together on the same product at the same time.

Collaborative robots come in a variety of sizes, payload capacities, maximum ranges and operational speeds. Many are compact enough to be placed on a workbench or a robust cart. Larger examples may be placed on the floor, roof or wall. The payload limitations are usually between 3 and 16 kg. Six-axis motion is still utilised by many collaborative robots, enabling sophisticated travel through and between other devices. Table 2.2 presents a summary of some commercial collaborative robots with their key specifications.

Applications of Collaborative Robots

While modern ways of automation do not alter the essence of employment, they have provided significant economic opportunities to the manufacturing sector. Collaborative robots have the potential to produce enormous profits for manufacturers. One reason is that these robots are designed to work around the clock and assist production firms in their efficiency, output and sales targets. Collaborative robotics are of key significance in production in the following respects:

1. **Picking and packing:** Doing these procedures manually may be tedious and is often time consuming. Picking and packing may be easily automated with the use of collaborative robots, considerably increasing the line's productivity and efficiency, as well as packaging quality [183].

2. **Welding:** Welding is one of the most cumbersome and dangerous activities in assembly plants. Collaborative robots may be used alongside humans, shielding human workers from events such as fatalities and injuries.

3. **Assembling items:** Assembling is a process that involves screwing and assembling/installing components. Using a collaborative robot, this process may be readily automated, increasing efficiency and quality on the assembly line [207] and preventing workers from doing tedious tasks [205]. Simultaneously, worker safety is addressed, particularly in instances in which assembly can be dangerous.

4. **Handling materials:** Collaborative robot materials handling can automate the most physically difficult, dangerous, repetitive and tedious activities on the manufacturing line [205].

5. **Inspecting products for quality:** Various forms of collaborative robots are widely used in quality control applications to identify and correct faults or anomalies in an assembly or system [207].

6. **Machine tending:** Machine tending refers to the process of loading and unloading components and materials into a machine. The most prevalent uses of machine tending would be in machine shops, where robots load raw materials, run their programmes and then remove completed products. This procedure may be repeated indefinitely as long as the robot continuously receives raw materials and the machine consistently produces quality parts.

7. **Palletising:** Palletising is a demanding process that involves stacking boxes, bottles and cartons onto pallets as the last stage before they are loaded into a transport vehicle.

Table 2.2: Examples of commercial collaborative robots with their main specifications (Extended from [87, 204]).

Robot	**Specifications**	**Robot**	**Specifications**
ABB: YUMI IRB 14000, Switzerland	Payload: 0.5 kg Reach: 559 mm Repeatability: 0.02 mm # of axis: 7 (each arm) Weight: 38 kg Sensors : Camera, force sensor in joints Application areas: Electronics and small parts assembly lines Features: Dual-arm, soft padded plastic casing, magnesium skeleton, control through programming	KUKA : LBR IIWA 7/ LBR IIWA 14, Germany	Payload:7 kg / 14 kg Reach: 800 mm/ 820 mm Repeatability: +/- 0.1 mm # of axis: 7 Weight: 22.3 kg / 29.9 kg Sensors: Force sensor in joints, torque sensors in all axes Application areas: Machine tending, palletising, handling Features: Three operating modes (Position Controller, Gravity Compensation, Compliance Controller)
Rethink Robotics : BAXTER, USA	Payload:2.2 kg per arm Reach:1210 mm per arm Repeatability—±0.1 mm # of axis: 7 per arm Weight: 165 lbs (75kg), 306 lbs with pedestal Sensors: Force sensing (each joint), camera (each arm) Application areas: Machine tending, circuit board testing, material handling, packaging, kitting, etc. Features: Power and force limiting sensors, Intera operating software	COMAU | RACER 3 5, Italy	Payload: 3 kg| 5 kg Reach: 630 mm| 809mm Repeatability: +/- 0.02 mm | +/- 0.03 mm # of axis: 6 Weight: 30 kg | 32 kg Sensors : N/A Application areas: Assembly, handling, machine tending, dispensing, fast pick & place Features: Lightweight materials, stiffness, speed
DENSO: COBOTTA, Japan	payload: 500g reach: 310mm Repeatability: ±0.05mm # of axis: 6 weight: 3.8 kg Sensors: Speed and torque sensors in each axis Application areas: Portable dispensing system, three-colour pen factory, mini car assembly, labelling, recommendation application Features: Portable body, easy to use, open platform and safe design	Productive Robotics: OB7, USA	Payload: 5 kg Reach: 1000 mm Repeatability: +/- 0.1 mm, # of axis: 7 Weight: 24 kg Sensors: N/A Application areas: Testing, packaging, machine tending, injection moulding, laser cutting, work assistant Features: No programming, learn by demonstration
AUTOMATA: EVA ,UK	payload: 1.25kg Reach:600mm Repeatability: ±0.5mm # of axis: 6 weight: 9.5kg Sensors : N/A Application areas: Product testing, machine tending, inspection sorting, lab automation Features: Made from 3D printed plastic; a lightweight desk robot	Rethink Robotics: Sawyer USA	Payload: 4 kg Reach: 1260 mm Repeatability: 0.1 mm # of axis: 7 Weight: 19 kg Sensors : Force sensing ,camera Application areas: Metal fabrication, moulding operations, packaging, line loading and unloading, test and inspection Features: Power and force limiting sensors, Intera operating software
NEXTAGE, JAPAN	payload: 2.5kg ((one arm) Reach:600mm Repeatability: ±0.03mm # of axis: 15 (6 for each arm, 2 for neck, 1 for waist) weight: 36kg Sensors: A head camera and two hand cameras Application area: N/A Features: Moves easily, image recognition system, designed with human-like qualities	AUBO: OUR-1, China	Payload: 5 kg Reach: 850 mm Repeatability:±0.05mm # of axis:6 Weight:15 kg Sensors: Gigabit ethernet camera Application areas: Pick & Place, machine tending, quality testing, palletising Feature: Touchscreen programming
Universal Robots: UR3, UR5, UR10, Denmark	Payload: 3 kg / 5 kg / 10 kg Reach: 500 mm/ 850 mm / 1300 mm Repeatability: 0.1 mm to 0.0039 # of axis: 6 Weight: 11 kg / 18.4 kg / 28.9 kg Sensors: Force sensors embedded in joints Application areas: Packaging, palletising, assembly, pick and place. Feature: 12 in touchscreen programming	FANUC: CR-35IA, Japan	Payload: 35 kg Reach: 1813 mm Repeatability: 0.08 mm # of axis:6 Weight: 990 kg Sensors: camera (iRVision), safety sensor Application areas: Pick & place, machine tending, quality testing, palletising, laser cutting, painting, welding Feature: Safety sensor located separately

Collaborative Robotics Market

From 2022 to 2030, the global collaborative robotics market is projected to rise at a compound annual growth rate (CAGR) of 31.5% [50]. The number of collaborative robots has been forecasted to increase from 8,950 in 2016 to 434,404 by 2025 [143], and the market is anticipated to reach $5.6 billion worldwide by 2027 (representing 30 percent of the global robot market) [45]. According to NIST, advanced robotics will save U.S. manufacturers $40.3 billion annually (or 5.3%) [9], while in the UK the use of automation and robotics is estimated to have a £183.6 billion 10-year Value at Stake for the economy [130].

The market research companies publish reports and analyses regarding the global adoption of robotics based on the available market data. According to these reports, there appears to be disagreement over which region has the largest market for collaborative robots. For example, MarketsandMarkets [47] state that Asia-Pacific held the largest market share in 2021 as a result of low production costs, the availability of inexpensive labor, and the government's efforts to attract foreign direct investments (FDIs), allowing Asia-Pacific to maintain a dominant market position in the collaborative robot market. Also, Coherent Market Insights [49] gives Asia-Pacific as the largest market share in 2020, followed by Europe. However, Grand View Research [50] identifies Europe as having the largest revenue share in 2021 at 30%, but predicts that Asia-Pacific will outpace it by 2030. This is primarily attributable to the extensive use of collaborative robots in numerous industries, including logistics, electronics, and numerous area. Furthermore, the development base of collaborative robots is a European strength, e.g. Universal Robots has about 52% share of the market and is based in Denmark [48].

2.2.2 Robotic Exoskeletons

The term 'exoskeleton' refers to active and powered wearable robotic equipment. Scholarly publication, development and testing, and commercialisation have resulted from the academic and industrial sectors' interest in this field since the first robotic exoskeleton was developed in 1960 [18]. Exoskeleton or wearable robotic systems have been substantially developed for application in robotic rehabilitation, human power assistance and haptic interface in virtual reality (VR) [83]. Exoskeleton robots are HRI systems that enhance the wearer's skills in a range of situations, while the human operator controls the robot's position control, contextual sensing and motion signal generation [122].

According to the level of support provided by exoskeletons to various areas of human anatomy, there are four main categories of exoskeletons: lower limb exoskeletons, upper limb exoskeletons, full body exoskeletons and particular joint support exoskeletons. Table 2.3 presents some examples of available commercial exoskeletons.

Application Areas of Exoskeletons

Exoskeletons are now being used in a variety of domains, including medical [163], military [115] and industrial [208]. Additionally, robotic exoskeletons have been developed by integrating many fields, such as mechanics, sensing, control, data science and mobile computing [17].

- **Medical:** Exoskeletons are widely used in the field of rehabilitation and physiotherapy of stroke or spinal cord-damaged patients. People with muscular disorders and other neuromuscular disabilities use exoskeletons to enhance their muscle power. Exoskeletons for medicinal use are classified into six groups: stationary lower body exoskeletons, stationary upper body exoskeletons for rehabilitation of the arm and wrist, stationary upper body hand exoskeletons for rehabilitation, mobile upper body exoskeletons for rehabilitation & augmentation, mobile lower body exoskeletons for rehabilitation and mobile lower body exoskeletons for augmentation.

- **Military:** The primary application of exoskeletons is to reduce tiredness and enhance soldiers' abilities to run, climb stairs and travel long distances. They are also used carrying payloads (general equipment and/or casualties). Military exoskeletons are classified into five categories: full body, lower body propelled, passive, energy scavenging and stationary.

- **Industry:** Industrial exoskeletons are used in the workplace. Their goal is to amplify, increase or strengthen the performance of a worker's current bodily components, particularly the lower back and upper extremities (arms and shoulders). Industrial exoskeletons are classified into six categories: tool-carrying exoskeletons, chairless chairs, back support, powered gloves, full-body power suits and robotic arms with supernumeracy.

Table 2.3: Examples of commercial exoskeletons.

ShoulderX by suitX [188]	Chairless chair by Noonee [147]
EVO by Ekso Bionics [63]	Fraco by Mawashi [137]

2.2.3 Robotic Teleoperation

A teleoperation system is a device that is remotely operated. Numerous teleoperation systems have been developed and used in recent decades to assist individuals in remotely executing tasks, particularly in hazardous areas. These activities include working in a dangerous or poisonous environment, performing distant operations, such as telesurgery and space operations, and conducting high-precision tasks, such as operating chemical and nuclear energy plants. Teleoperation systems, in general, comprise a human operator, a master manipulator and slave manipulators that are connected via a network connection and the environment. Teleoperation systems enable operators to exchange location, velocity and/or force information over a distance in order to conduct required motions, sensing and physical manipulation.

Teleoperation systems are classified into two broad categories [92]: unilateral and bilateral. When motion is transmitted from master to slave, it is referred to as a unilateral teleoperation system. A bilateral teleoperation system (BTS), on the other hand, comprises transmissions between master and slave in both forward and backward directions. In general, researchers are more interested in BTSs because they are used in environments that are inaccessible to humans, such as underwater vehicles and space exploration [92].

In teleoperation systems, the operator controls the robot via direct, shared or supervisory control [124]. The remote robot requires no intelligence when it is under direct control. The operator performs the motion planning, and the remote system receives the joint angles immediately [124].

Application Areas of Teleoperation

Teleoperation is now used in a wide range of fields, including space [126], medical [41], military [116], mining [152] and industry [10].

- **Space exploration:** Teleoperation has been widely used in space applications. Because the physical presence of humans in space is prohibitively expensive (planet exploration), deploying teleoperated vehicles is more efficient. The teleoperation system has two roles as a space robot's control equipment: to sense and feedback the space robot's condition and to turn the operator's operational intent or action into instructions.

- **Medical application:** Teleoperated medical robotic systems enable procedures, such as surgeries, treatments and diagnoses (e.g. diagnostic scans), to be performed over short or long distances using wired and/or wireless communication networks [14]. There are a number of teleoperation systems in the medical area, including telesurgery and telemedicine systems. Telesurgery allows patients who are unable to travel vast distances to receive surgical operations [42]. Telesurgery also allows doctors to work at very different scales than they would manually. Telemedicine refers to the use of information technologies and online communication to provide services to patients, such as diagnosis, examination and medical assessment [52].

- **Military application:** Teleoperation in military contexts has the potential to significantly reduce the risk of injury or death to soldiers; replacing them with machines (remotely operated mobile robots) is especially beneficial, at least in the most dangerous tasks. I believe there are *scout* applications as well - robots are thrown into buildings/potentially dangerous areas and remotely controlled to scout out the area before humans enter.

- **Mining:** Because mining and forestry are risky by nature, a variety of teleoperation vehicles are utilised in these areas.

- **Industrial application:** Teleoperation in an industrial environment enables human workers to execute their duties without physically being present in the manufacturing line.

2.3 Robotics and the Need for User Authentication

User authentication is a long-standing and critical element of the security of modern systems. It also plays an essential role in the environments of robots [118]; this is addressed in the remainder of this section.

Cerrudo et al. [39] identified nearly 50 cybersecurity vulnerabilities in robot environments. They stressed the importance of identifying users authorised to access or work with robots and considered the lack of identification and authentication to be the most critical vulnerability. Similarly, in a highly influential report, Maggi et al. [128] not only documented the significant scale of the vulnerability of industrial robots on the internet but also identified vulnerabilities in a particular industrial robot (ABB IRB 140). They found that weak authentication protocols are major sources of vulnerability. There were flaws in the implementation that could weaken the robot's user authentication system, such as the possibility of disabling authentication during a system boot. Another problem was the use of a username without a password. These flaws could enable an attacker to bypass the user authentication system and consequently damage the larger system significantly. Bonaci et al. [27] highlighted the lack of authentication and encryption in the communication channels of surgical robots, rendering the robots vulnerable to man-in-the-middle attacks and enabling an attacker to seize control of them.

However, few attempts have been made to build systems that incorporate human user authentication into robotic environments. Haas et al. [89] suggested a form of two-factor authentication (2FA) using a smart card and fingerprint recognition to avoid the disadvantages of traditional passwords. Kim et al.[112] proposed a system of authentication for smart service robots. The system combines biometrics with semi-biometric measurements, which refer to a set of non-unique biometric features, such as body height. The system aims to identify users who move freely around smart service robots and to whom the robots need to provide appropriate services. A camera is used as a device to identify biometric characteristics, and the system does not require cooperative contact from users, unlike, for example, fingerprinting recognition systems. Kumari and Vaish [118] proposed a user authentication system in the robotic environment. Their system is based on the recognition of a user via the user's brainwaves during the performance of cognitive tasks. The researchers measured brainwaves, which are electrical signals that occur because of brain activity, using a tool called an electroencephalogram (EEG). The distinguishing nature of this system is that stealing a password is difficult because this EEG-based authentication system depends on the interaction between a human and a robot.

Recently, scholars [96] developed a motion-controlled robotic arm system that inherits the majority of its user's behavioural data. They used these behavioural data to provide a mechanism for the robotic arm's user authentication. They captured the angles of the robotic arm's joints to replicate its 3D movement track in their work. They recruited 10 individuals to evaluate their authentication technique. According to their tests, their system properly validates users 95% of the time while preventing impersonation efforts. However, it is notable that their system does not utilise continuous-based authentication.

To our knowledge, there have been no studies on continuous user authentication to collaborative robots, exoskeletons or teleoperation. This thesis therefore focuses on continuous-based authentication for this domain. Authentication, in general, and continuous-based biometric authentications are discussed in the following sections.

2.4 Authentication

Authentication is a process by which claims of one form or another are verified by some means. For example, when I attempt to log into my University of Sheffield (UoS) account, I claim to be Shurook S. Almohamade (providing my UoS user ID). I am required to demonstrate to the system that it is me supplying the data. This is done by giving a password to the system that can be checked against a stored password. The assumption is that it is highly probable that only I will be able to provide this correct password. The provision of the password is the evidence the system needs to verify my claimed identity.

Passwords or passphrases are not unique to the digital age. An example of the use of passphrases in history is Open Sesame, from the story of Ali Baba and the Forty Thieves. This phrase was the only way to open the cave where Ali Baba hid his treasure. In the story, authentication relied on a spoken phrase—Open Sesame—so that only those who knew it would be allowed to enter the treasure-laden cave.

In the centuries since the story of Ali Baba and the Forty Thieves entered the popular imagination, many methods have emerged for controlling access to secured environments or verifying a person's identity. For instance, one means of authentication commonly used in the Middle Ages was a wax seal, which verified that a document had not been opened and confirmed the sender's identity. Furthermore, castle guards asked for spoken passwords to prove visitors' identities. Over time, authentication methods evolved, and handwritten signatures became the most common authentication method.

Identity documents have been adopted as authentication for verifying people's identities; for example, a passport is a document adopted in most countries to certify the holder's identity and nationality. Those holding such a document often have the right to travel to foreign nations, receive protection from the home nation and return to their original country.

In 15th-century China, Portuguese historian Joao de Barros documented the first form of biometrics—fingerprinting [25]. Chinese traders used ink to take children's fingerprints in order to confirm their identities [25].

The first uses of digital authentication, including passwords, allowed users to share time on large computers and large systems in a controlled environment [173]. Initially, text files were the only means of storing users' passwords without requiring security. The need for developing new ways of protecting these passwords became clear the first time these files were misused. This issue happened when one user wanted extra time on a central computer [173].

To access others' passwords, the user printed the password text file.

The ability to use digital authentication appeared with the development of computer systems in the early 1960s at the Massachusetts Institute of Technology. The goal of digital authentication was to protect users' files on a multi-user computer from unlawful access. Throughout the 1970s, UNIX developers used the principles of the M-209 cypher machine, which was used during World War II, to apply a password cypher to the UNIX operating system's sixth edition.

By 1974, Morris and Thompson had improved password hashing. They warned users that their chosen passwords had a significant vulnerability. This warning was based on an experimental analysis of users' password choices by performing dictionary attacks on a real system, which resulted in the retrieval of passwords for a large number of users [30].

In the early 1990s, a mechanism emerged for auditing passwords by testing their strength. Examples of these tools include COPS, Crack, Cracker Jack and npasswd. Besides, with the advent of the World Wide Web and remote human–computer authentication, there was renewed motivation to research the replacement or development of passwords [30].

2.4.1 General Concepts

The foundation of any security system is based on three concepts: identification, authentication and authorisation [98]. These concepts are detailed below and illustrated in Figure 2.1.

Identification occurs when a user or entity claims an identity; this can be done by presenting a username, ID or smart card. The term 'authentication' refers to the process of proving whether someone or something is true or valid. In computing systems, authentication is a method of verifying that individuals or objects that have tried to access a secured system or a protected piece of information are who or what they claim to be [25][149].

We can describe *authentication* as the process that runs at the start of an application before the permission for authorisation may proceed. Benarous et al. (as cited in [150]) explained that, over time, the definition of authentication has not been definitively updated. However, there are alternative components used in authentication apart from straightforward passwords.

Authorisation is a process that occurs once authentication is successful [91]. It validates that the authenticated user has the prerogative to perform operations or gain access to a service, resource or piece of data [91][98]. We can see an authorisation in action when a university student uses their student ID card to access campus buildings, print to networked printers and so on. The student presents their card, which is then checked in some way for its validity (i.e. to ensure that it has not expired) and access privileges (e.g. the student may enter the specified building). Once these points are verified, the student can then enter the building, use the desired service and so on. Based on the previous definition of authentication, we can observe two branches of authentication: (human) user authentication and machine authentication (also known as challenge–response authentication). They include computing equipment and the processes they host.

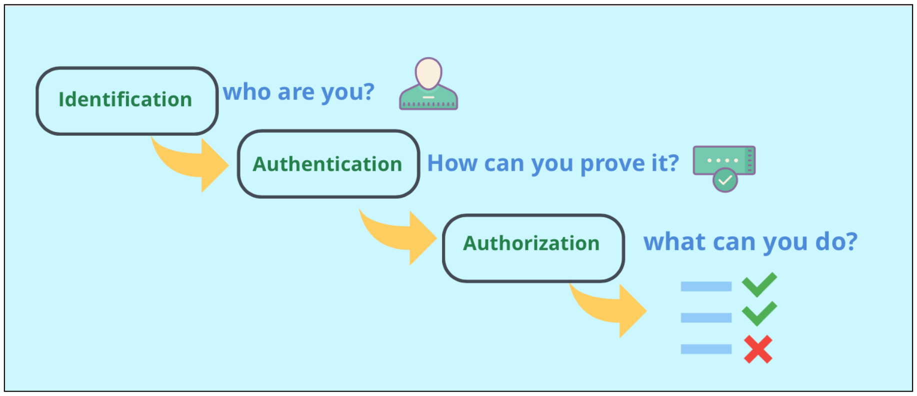


Figure 2.1: The process of identification, authentication and authorisation.

User authentication is the process of determining whether a user is whom they claim to be [98][150]. By contrast, machine authentication is defined as the process of deciding whether an entity is what it claims to be [149]. In other words, machine authentication is used for authorising computers and other devices to communicate and share information independently on wired and wireless networks (see Figure 2.2).

In general terms, challenge–response authentication (also known as zero-knowledge protocols) is a class of authentication techniques used for determining the identification of an individual or other entities demanding access to a computer or network [67]. This type of authentication, which is one authentication protocol, relies on sending a challenge or question from the first entity and requiring a valid response from the second entity to authenticate the latter. For example, for password-based challenge–response systems, the user's computer receives a random challenge from the server. The user's system calculates a response by applying a cryptographic hash function associated with the user's password as a secret key. When the response is sent to the server, the server, in turn, uses the same hashing function for the challenge data to calculate the valid response associated with the user's password saved in the server. If the result matches the answer sent by the user's computer or application, then the user has presented the valid password, and the user's computer will be authenticated. In this case, challenge–response authentication is considered a useful technique that protects against session replay attack and, sometimes, man-in-the-middle attacks when a private key is used for encrypting the challenge data (see Section 2.4.3 for more details about security attacks).

2.4.2 User Authentication

User authentication can be classified into the following three approaches: knowledge based, object based and biometrics based. These categories are detailed below and illustrated in Figure 2.3.

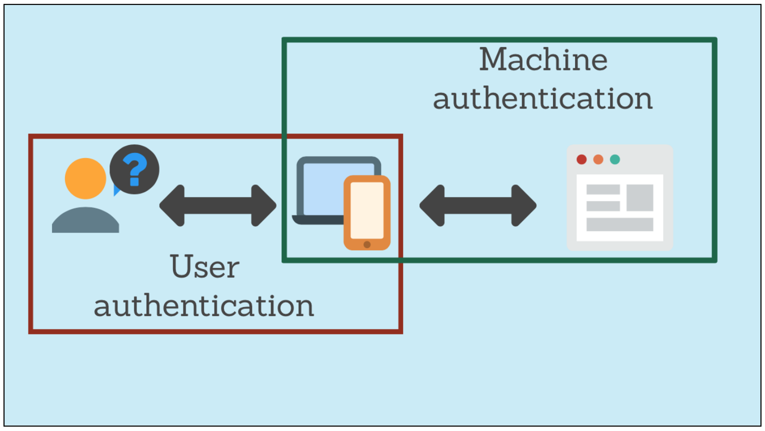


Figure 2.2: Illustration of the difference between user authentication (human–machine) and machine authentication (machine–machine).

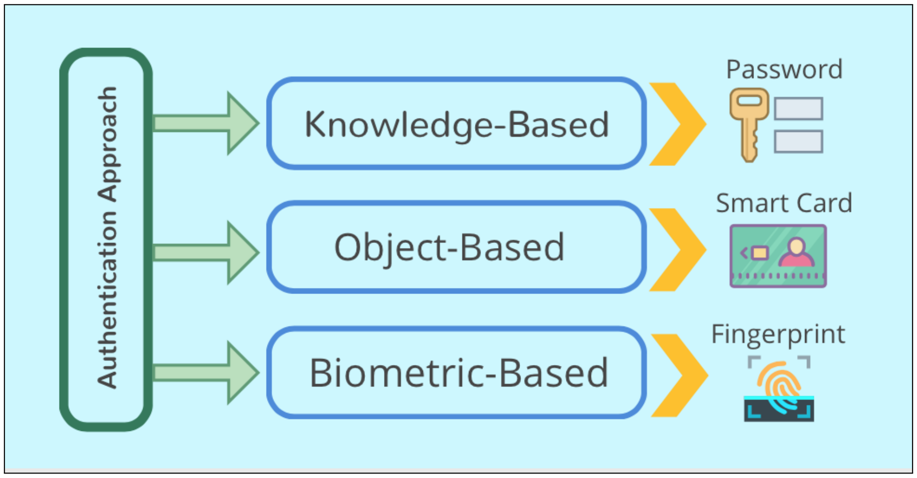


Figure 2.3: User authentication approach.

1. *Knowledge-based approach (something the user knows)*: The knowledge-based approach refers to what the user knows [149]. Knowledge-based methods include text-based passwords, graphical-based passwords, personal identification numbers (PINs) and security questions [191]. However, approaches of this kind carry various limitations, such as the possibility of being stolen, guessed (by individuals or otherwise by brute force search on modern hardware), shared or forgotten.

2. *Object-based approach (something the user has)*: The object-based approach (also called the token-based approach) connects possession of an artefact with identity (or at least membership of an authorised group). Such techniques refer to what the user has, including tokens such as smart cards or keys [149]. Thus, to enter many buildings out of hours at the UoS, one must supply a university card to a card reader at various entrances. Individuals are instructed to ensure that their cards do not fall into other

people's hands. If this instruction is upheld, then demonstrating possession of a card shows the presence of the individual associated with that card. In other applications, a user may have possession of a computational device, securing their authentication via a PIN (or some other means). Once a user has been authenticated to such a device, the device may then be used to participate in further authentication protocols. It may maintain a secret that allows this, so having the PIN (something the user knows) allows access to the device (something the user has), which can then supply information based on the secret it maintains (something it knows). This multi-factor approach is used by some UK banks for online banking authentication.

3. *Biometric-based approach (what the user is/does?)*: Biometrics is considered a more secure approach than the knowledge- and object-based approaches. Biometrics refer to a user's biological measurements, such as their fingerprints, facial features, speech patterns or qualities and behaviours [149]. One of the limitations of this approach is that biometric systems are costly. Their most serious disadvantage is that the identification process in some biometric systems can be slow or unreliable.

In addition to the aforementioned basic authentication types, Lal et al. [119] identified two other classes: something that the user can perform, such as signs and gestures (although this could be considered a form of the knowledge approach), and somewhere the user is, such as their location and the current time [119].

User Authentication Types

Single-factor Authentication (SFA): SFA is an authentication procedure that requests only one category of credentials for identifying an individual's identity [12]. Passwords are the most popular examples of SFA. The simplicity of SFA is its chief advantage [119][150]. However, this solution has a significant disadvantage in that it is less secure than multi-factor authentication (MFA).

Two-factor Authentication: 2FA is an authentication process that involves two verification steps for identifying an individual's identity by requesting two authentication factors [12]. This type of authentication appears to avoid the disadvantages of using SFA, such as the stealing of passwords [156]. In other words, 2FA affords another layer of protection that reduces the risk of authentication attacks. For example, in 2FA, an attacker who has the victim's password requires another factor following the password during the authentication process, such as sending a one-time password via text message to a mobile phone. Research has shown that one of the factors that have promoted the spread of 2FA is the use of mobile phones [156]. Currently, online banking and internet service providers most frequently use 2FA [156]. A typical example of 2FA is using an ID card, a form of object-based authentication, in addition to a PIN.

Multi-factor Authentication (MFA): MFA is an authentication process that uses multi-step verification to ascertain an individual's identity by requesting two or more different authentication factors[12] [150]. The possibility of stealing or faking three elements is very low, which means that MFA increases security dramatically. MFA may include, for example, a password, an ID card and fingerprint scan. However, these additional steps also increase costs.

Traditional User Authentication Techniques

Password Authentication

- **Textual passwords:** Textual passwords are well-established forms of knowledge-based authentication techniques used to confirm a user's identity by using characters, words and/or numbers. Although these passwords have some problems related to their security and usability, they enjoy widespread use [177]. They were used to provide authentication in early operating systems, and their use persists to this day. Passwords are simple concepts and easy to implement. With their almost universal use in authenticating at automatic teller machines (ATMs), PINs are just a specific form of password.

  A password can be stolen or predicted if the user sets a simple or weak password [29]. It can often be easily forgotten, so there is a usability issue [177]. Nevertheless, passwords are easy to use, easy to change, low cost and highly reliable. At the same time, they have many drawbacks, such as being easily forgotten, possible to guess, often written down, possible to use without the user's knowledge and prone to many security attacks (ranging from shoulder surfing to implementation-dependent brute force attacks.)

- **Graphical passwords:** Graphical passwords are forms of knowledge-based authentication that calls on a user to select an unforgettable image [197]. Scholars have observed that it can be challenging to remember text-based passwords, but graphical password schemes are potential alternatives [191]. Compared with textual passwords, 90% of users can still recall graphical passwords after a period of time [197].

  Graphical passwords use visual thought, including the selection of images, reproducing drawings as passwords rather than text [191]. For instance, in one graphical password method, images are displayed to the users on a graphical user interface, and they are asked to select from them in a specific order to authenticate themselves [191]. Graphical passwords are classified into two techniques: recognition and recall based [180].
  Recognition based: During the authentication process, users choose graphical elements, such as icons, symbols or images, from a group of pictures. These selected images should match their pre-registered images.
  Recall based: When using a recall-based approach, users are required to reproduce an element, such as a signature, as a password without being provided any hint for it [111]. For instance, users may draw their unique graphical password during the registration process. Then, during the authentication process, they are asked to draw it again in

order to confirm their identity [127].

- **Personal identification number (PIN):** A PIN is a form of knowledge-based authentication in which a short numeric sequence serves as a password for authenticating a machine's user, such as a smartphone or ATM [59]. A typical PIN ranges from four to eight digits and is associated with other factors, such as a traditional password, or an object, such as a smart card.

- **Security questions:** Many sites use security questions as security techniques. Amongst them are banking sites [160]. These security questions can be classified into two categories: sensitive and personal questions. The difference between them is that the former asks about confidential information, such as a bank account number, whereas the latter is based on personal data, such as one's date of birth or their mother's maiden name. These techniques fall under the knowledge-based authentication umbrella, which asks about what the user knows. The advantage of security questions is that they help verify the user when they try to retrieve the password; however, the answers may be available online, especially if the security questions are personal, such as the user's date of birth [160].

Token Authentication:

An authentication token is an object that holds the credentials afforded to an authenticating party as part of the authentication protocol. Token authentication is a form of object-based authentication used to authenticate one object to another [202]. The object may be a device, such as a smartphone, or installed in a host device, such as a USB drive, smart card or electronic key. Security token authentication techniques serve as second factors for authentication in addition to passwords, thereby enhancing password security and providing an extra level of protection compared with passwords alone [8]. In general, it is difficult for an attacker to get a security token, which makes it more effective and efficient than only a password; however, tokens do have some drawbacks and limitations. Compared with a password, a token requires more effort to control, and the user must physically carry it. Tokens may require both hardware and software, which in turn necessitate maintenance, installation and deployment, rendering this a high-cost approach [8]. Token authentication can be divided into mobile-based authentication and smart card authentication, which are defined as follows:

1. **Mobile-based authentication:** Mobile-based authentication uses a mobile phone as a means of authenticating a user's identity, either via text messaging or an application [203][29]

2. **Smart card authentication:** Smart card authentication uses a card. The smart card's chip can store specific information from the user (i.e. a password). The user must prove that they own the smart card, and then swipes the card into a reader to be authenticated. Information is processed on the smart card, so smart cards help reduce

the threat of stealing information stored in the computer. However, they are limited in size and often cannot store much information [203].

2.4.3 Threat Modelling for Traditional User Authentication

Traditional authentication approaches, such as passwords, are used to protect a system against unauthorised users. However, passwords are considered insecure for achieving this goal because of traditional validation flaws. They are also seemingly vulnerable when multiple attacks target a system. In this chapter, we examine some of the most common forms of attack and compare the resistance capabilities of different authentication methods against them.

Guessing Attacks

Guessing attacks lead an attacker to find the user's password using two approaches. The first approach, known as a ***brute force attack*** [180], relies on guessing and experimenting with all possible passwords. The brute force approach is commonly used to crack encrypted passwords that are preserved as encrypted text [161]. Brute force attacks are highly time consuming because of the time required to search for a password amongst all possible passwords [161].

The second approach, known as a ***dictionary attack*** [161], is faster compared with brute force attacks. Rather than evaluating all possible combinations with a brute force assault, a dictionary attack attempts to match the password with the most frequently occurring words or phrases used in everyday life. The dictionary attack has a disadvantage in that it is sometimes unable to break the password, as the password to be cracked might not be found in the dictionary itself.

Shoulder Surfing Attacks

Shoulder surfing attacks involve visual observation over the victim's shoulder to obtain passwords, PINs or other sensitive information [161]. In this type of attack, the attacker either conducts direct observation, such as looking over someone's shoulder, or uses video capturing tools [190]. Various authentication mechanisms have been developed to prevent systems from this attack. However, most of them have failed to reduce the threat [31] posed by camera-based shoulder surfing attacks [190].

Keylogger Attacks

Keylogger attacks refer to the action of monitoring victims by recording the keys struck on a keyboard. Keylogger attacks may be used to collect sensitive data, such as passwords, PINs or usernames [199]. This kind of security attack can monitor victims remotely via software or hardware [161]. Software keyloggers are programmes that must be installed on a computer to steal keystroke data. They seem to be the most frequently used methods for hackers to gain access to a victim's keystrokes. A hardware keylogger must be physically attached to the victim's computer in order to record the victim's keystrokes.

Phishing Attacks

Phishing attacks are perpetrated by installing malicious software that can disable a system or detect confidential information, such as passwords or credit card numbers. Often, the attacker sends a malicious link via e-mail or text message, which then installs a malicious programme or redirects the user to a fraudulent website after the victim clicks on the malicious link [88]. Khan [108] explained that phishing is not limited to sending a fraudulent link via e-mail; it can also occur through social networking sites or search engines. It essentially seeks to persuade users to ultimately carry out actions against their interests, for example, by convincing a user that clicking on a supplied link will have only positive consequences. By contrast, the result of doing so will compromise the user's system.

Video Recording Attacks

Video recording attacks [95] occur when an attacker records a video of users as they enter passwords. For example, in 2005, an attacker in Japan installed a mini camera on an ATM to record the PIN codes of the cards inserted. The attacker used the information to perpetrate theft.

Login Spoofing

Login spoofing [161] is a method used for obtaining a victim's password. The victim is asked to log into a malicious log-in page, commonly called a Trojan horse, with their username and password. After the username and password are registered, the password information is recorded and forwarded to the attacker, thereby breaching the account's security.

Replay Attacks

A replay attack is a type of network assault in which the attacker discovers and fraudulently delays or repeats a data transaction. In other terms, a replay attack is an attempt to compromise the security protocol by injecting replays of data transmissions from a different sender into the target receiving system, deceiving the participant into believing that the data communication was successful. This attack is also known as a playback attack, reflection attack or man-in-the-middle attack. Replay attacks may also be used to attack biometric authentication systems by copying the users' biometrics communicated to authentication systems and replying to them afterwards. For example, an attacker can steal a user's face image and show it to the camera used as an authentication device [69]. Note that encryption alone does not protect against this type of attack. It is perfectly feasible to replay an encrypted message. The protocol must incorporate elements to allow such replay to be detected.

2.5 Biometric Authentication

All of the previously mentioned techniques have drawbacks. However, with the emergence of biometrics, avoiding or lessening the disadvantages of traditional authentication is possible [161]. Biometric authentication identifies an individual by using their unique physiological and/or behavioural traits [25][102]. This approach has many advantages. Specifically, biometric features cannot be lost or forgotten. Furthermore, biometrics require the presence of the authorised person; they must be present at the time and location of authentication.

2.5.1 Concepts and Definitions of Biometrics

The term 'biometrics' is commonly linked with the ability to recognise a person using specific traits [25][102]. Thus, a pattern recognition (PR) system that identifies an individual based on a distinct physiological or behavioural trait that they have is known as a biometric system [24] [102]. The biometric features obtained from users can be divided into two major types: physiological and behavioural. Physiological biometrics refer to users' physical attributes, including their fingerprints, facial structures, iris patterns, palm prints, DNA and hand geometry [24]. Behavioural biometrics refer to attributes such as typing habits, voice patterns, signatures, keystroke dynamics or gait [24]. There are two primary stages in a biometric authentication system. The first is the enrolment stage, which is responsible for registering users' authentication data by acquiring and storing a biometric template [8]. The second stage is the authentication stage, in which comparisons are made with live authentication inputs and the biometric templates stored during the enrolment stage. A basic biometric authentication system consists of four phases, namely, the sensing, feature extraction, matching and decision phases [13], which can be described as follows:

1. **Sensing Phase:** This phase is responsible for capturing the user's biometric trait data.
2. **Feature Extraction Phase:** This phase processes the data from the previous phase to extract a feature that represents a biometric trait.
3. **Matching Phase:** This phase is responsible for comparing the extracted features to the database to produce matching rates.
4. **Decision Phase:** This phase is responsible for using the information from the matching phase to decide to accept or reject a claimed identity.

Biometric systems operate as verification or identification modes [24][129]. The testing phase is the main difference between these two modes of operation [172].

The ***verification mode*** refers to the procedure that matches the live biometric feature with the (claimed) individual's biometric template, which is stored in the system database, to verify that person's identity. In this mode, the authentication system approves or rejects the user's claimed identity (see Figure 2.4)[172].

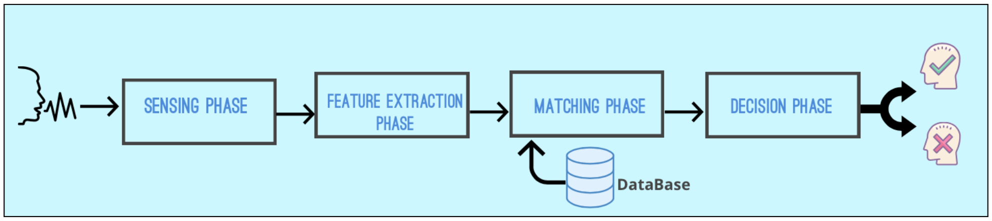


Figure 2.4: Biometric systems (verification mode).

The ***identification mode*** refers to the procedure of searching the whole template database to identify an individual. This procedure calls for searching using a one-to-many approach, unlike the verification mode, which uses the one-to-one approach [129]. In this mode, the test phase recognises an anonymous user (see Figure2.5) [172]. Verification is generally used in computing-based authentication, whereas identification is often used for identifying unknown people from videos and images.

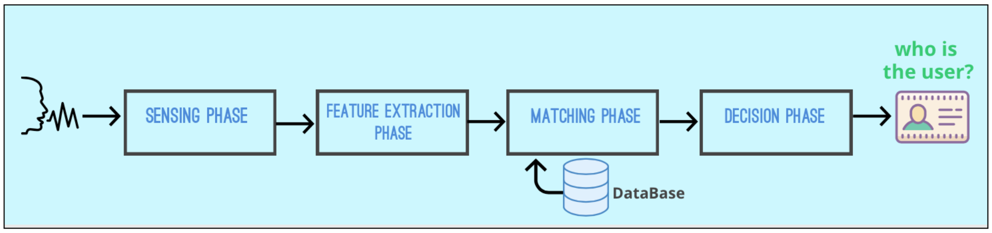


Figure 2.5: Biometric systems (identification mode).

There are two divisions in the identification mode: a closed set and an open set. In the closed set, authentication occurs only across a group of enrolled users for identifying the user. In the open set, authentication occurs not only across a group of enrolled users but also across users from outside the enrolled group [172]. Open set identification helps in determining whether the user has been enrolled in the system. Accordingly, the authentication system can decide to reject or identify the user as an enrolled user.

Based on the number of biometrics used, biometric systems can be classified as either uni-modal or multimodal [175]. A ***uni-modal biometric system*** uses a single physiological or behavioural characteristic for authenticating users, such as a single fingerprint [175]. Although relying on a single source of information for authentication is easier and less costly than relying on several sources, this comes with drawbacks, such as noise in the captured data [170]. By contrast, a ***multimodal biometric system*** uses multiple physiological and/or behavioural characteristics for authenticating users. These may include fingerprints and facial recognition [175]. Such systems are used to overcome the limitations associated with uni-modal systems [170]. This is sometimes analogous to MFA.

Physiological Biometrics

Physiological biometrics comprise the first category of biometrics and are based on unique physical characteristics and individual attributes. Physiologically based biometrics appear to be most often used because of their reliability and validated quality. A summary of the most popular physiological biometric techniques is given below.

- **Fingerprint recognition:** Fingerprint recognition is the use of the surface topography of a fingerprint, captured by optical or ultrasound tools, for verifying a user's claimed identity. Fingerprint recognition systems are easy to use and install. They are considered comparatively inexpensive and consume little power. Moreover, fingerprinting is considered a unique method of measurement, as humans' fingerprints are all different. The security, reliability and accuracy of fingerprint recognition are relatively high [171]. It requires only a small amount of memory because the template size for a fingerprint is small, resulting in rapid matching [171]. Despite their general reliability, fingerprints are not permanent, as the likelihood of finger injury increases over time. For example, scars or cuts to a finger may affect the performance of a fingerprint recognition system. In addition, noise resulting from dirt can produce obstacles to recognition performance accuracy [171].

- **Facial recognition:** Facial recognition technology has been widely used as an identification method in biometric security systems for two reasons. First, the face is the easiest feature to use for authentication purposes. Second, it requires no physical connection between users and the device. Another advantage of facial recognition technology is that it is quick to use and does not require a large amount of storage capacity during identification [189]. Some researchers, such as [171], assumed that facial recognition is socially acceptable. However, it may not suit certain categories of users, including women who wear a face covering, such as a hijab, for religious reasons. Another disadvantage of facial recognition technology is its lack of permanence; human faces can be affected by several factors, including light, age, individual actions and emotional state.

- **Iris recognition:** Iris recognition refers to a biometric means of capturing a photo of the unique patterns found in an individual's irises [34]. Biometric iris recognition has several advantages; it is speedy, accurate and reliable, and it does not require direct physical contact with the scanner. Glasses and contact lenses do not obstruct the iris recognition process [171]. Unlike facial recognition, iris recognition is not affected by age, as human irises remain constant throughout the user's life [171]. Iris recognition is less common than other forms of biometric identification because it requires specific devices, whereas other identification methods, such as facial recognition, rely more heavily on software. Another reason for the lack of popularity of this technique despite its advantages is the perception by some users that it poses harm to the eye. However, iris biometrics have recently become more accessible in terms of cost and installation because of technological advancement, although it remains expensive compared with software-based biometric systems.

- **Palm prints:** Palm prints are related to the characteristics of the hand's internal surface, such as lines and wrinkles [189]. Palm prints are unique. No two people have the same palm print characteristics. However, similar to fingerprints, wounds may change the inside hand surface. This may result in inappropriate inputs influencing the decision phase of a biometric recognition system with incorrect inputs. In addition, the approach raises non-universality concerns because it does not include people who have been born with hand deformities or lack hands.

- **Hand geometry:** Hand geometry relies on the shape of a user's hands. It uses readers for measuring hands in many dimensions. To authenticate a user with hand geometry, the system compares the captured measurements with those stored in a database [16]. In a comprehensive survey of biometric systems, Sabhanayagam et al. (2018) [171] demonstrated the many advantages of hand geometry recognition systems. One of these is that is an easy-to-use, reliable and permanent technology. In addition, the results of the recognition process are not affected by the status of the skin, such as moisture levels or texture. However, the authors also mentioned some drawbacks, such as the lack of uniqueness of hand geometry, as well as the low accuracy and cost of the system. There are also some factors that can influence the performance of the recognition process, such as injuries and the wearing of jewellery. Finally, the authors failed to consider existing groups of people who cannot put their hand on a scanner device correctly because of arthritis; this is another factor that affects the performance of the recognition process [171].

- **DNA:** DNA biometrics rely on a form of tissue, such as blood, saliva or hair, to determine a user's identity [25]. Biometric systems that rely on DNA are well established in crime detection. Human DNA analysis is now possible in about 10 minutes [25]. Although this is a unique and precise technique, it does not feature real-time matching; it takes longer to process than other methods. This means that it is not suitable for validation access control applications that need real-time matching, such as in airports, where many people require authentication. In addition, DNA recognition systems are expensive and rather inconvenient technologies [171].

- **Ear recognition:** This technique relies on the ear's shape and appearance, capturing images of the ear to determine a user's identity [25]. One major advantage of an ear identification system is its quick recognition process, which leads to decreased processing times. Ear biometrics are frequently likened to face biometrics. Ears have a number of advantages over full faces, including lower spatial resolution, a more uniform colour distribution, and less variation in orientation [120]. In contrast to facial recognition systems, ears are neither affected by makeup or eyeglasses, nor do they have emotional characteristics such as facial expression [146]. However, similar to face recognition, ear recognition may not be suitable for certain categories of users, such as hijab-wearing women, for religious reasons. One of the drawbacks of ear recognition is the inability of the ear's simple distinguishing traits to produce a strong identification of an individual [105].

- **Retina geometry technology:** This method has very high accuracy and is a unique technique that uses blood vessel patterns in the retina to identify users. It is extremely expensive, however, and some users think it is dangerous to the eye. Moreover, some diseases, such as cataracts, may affect the accuracy and performance of retina recognition systems [171].

- **Lip print recognition:** This technique uses lip features, such as colour, shape, motion and texture, to determine an individual's identity. Lip print biometrics is an interesting way of recognising individuals; however, it is not as commonly used as other biometric features [153]. Similar to fingerprints, the features of one's lip print are unique [176], simple, largely permanent and cost effective to identify. The major advantages of lip prints are their reliability and accuracy. Lip prints are used widely in the forensics field [162].

- **Heart sound signals:** This is a method that uses heart sounds for individual identification. These signals are generally acceptable by most users and provide sufficient resistance from many attacks against biometric systems [64]. However, collecting heart sounds is a time-consuming operation, and electronic stethoscopes must be positioned in particular positions on the chest to obtain high-quality signals.

Behavioural Biometrics

Behavioural biometrics is the second category of biometrics. It is based on individuals' behaviour and conduct, such as their writing style. In general, physiological biometric approaches tend to outperform other techniques in terms of uniqueness, permanence and performance. These approaches, however, are considered invasive because they often require some sort of physical interaction with consumers. Behavioural biometrics, on the other hand, tend to change with time, although they can still operate in a biometric system. Behavioural biometric approaches offer higher levels of acceptance and user-friendliness, and they are less intrusive. There are various applications of behavioural biometrics, as described below.

- **Behavioural profiling:** The technique of authenticating a individual based on their interactions with applications and/or services is known as behavioural profiling [44]. This technology is non-intrusive and may be used to keep track of users' identities as they operate on their computers or smartphones.

- **Biometric signature:** A biometric signature refers to the practice of authenticating users via a signature captured by an input device, such as a tablet, computer display or other touch-sensitive technology. Biometric signatures are either static or dynamic.

Static signatures authenticate users using only the final shape of a signature [58]. By contrast, dynamic signatures recognise dynamic features throughout the signing process, such as speed, acceleration or pressure relating to the pen action [58] [86]. The strength of dynamic signatures is in the difficulties of simulating another user's signing behaviour; this makes the approach highly resistant to fraud. Despite this, however, dynamic signatures have some disadvantages. Some users may experience difficulty authenticating because of inconsistencies in the behaviour of their signature, which increase the potential for false rejection. In addition, people with muscular illnesses cannot create a reliable signature each time.

- **Keystroke dynamics:** Keystroke dynamics refers to automated means of authentication based on a user's typing behaviour or rhythm on the keyboard [129]. Because each person has a unique typing style, keystroke dynamics can be used for confirming an individual's identity [113]. Unlike some other biometrics, keystroke dynamics requires no special hardware, just a conventional keyboard. This is an important feature, as it makes this technique less expensive than other biometric approaches. It is essentially a software-based application approach. However, one of the fundamental problems of keystroke dynamics is that an individual's writing rhythm may be influenced by outside factors, such as tiredness, mood or medication effects.

- **Mouse dynamics:** Movement, drag-and-drop and point-and-click motions are all examples of mouse dynamics, which is a form of behavioural biometrics that capture and analyse human interactions with a graphical user interface through a mouse input device [212].

- **Gesture:** Gesture authentication allows users to authenticate using their gestures. The gestures are similar to a password in that they require mental effort; however, the advantages of gestures are that they can be performed more quickly than inputting a traditional password, and they demand less accuracy. There are three types of gestures:

  1. ***Grid-based gestures*** [182] allow users to authenticate by connecting dots in a grid via a touchscreen.
  2. ***Free-form gestures*** [182] allow users to authenticate by drawing a trajectory on a blank screen without a visual reference, such as a grid.
  3. ***In-air*** gestures allow users to authenticate by tracking their gestures without requiring the touching of a screen. AirAuth [13] is an authentication system that tracks users' hand gestures. It uses a short-range depth camera to analyse the biometric characteristics and movements of the user's hand. Unlike in-air gestures, grid-based and free-form gestures are vulnerable to shoulder surfing and smudge attacks [15].

- **Gait recognition:** Gait refers to a person's way of walking, and it is one of the many behavioural characteristics of an individual that can be used for authentication

[51][129]. There are also other uses for analysing an individual's gait, such as identifying offenders in criminal cases or identifying and evaluating pathological conditions, such as Parkinson's disease. Some factors can affect the accuracy of gait recognition systems, including external conditions, e.g. clothes, viewing angle or lighting. Internal factors, such as illness, body weight or pregnancy, can also affect gait [135].

- **Eye movement:** There are many different types of eye movements that humans can make, as well as eye movements that are voluntary, involuntary and even reflexive [62]. Eye movement biometrics measure a person's pupil size (changes) and gaze stability. Because these do not involve any physical touch with the users [178], recent developments in video-based eye-tracking technology make eye tracking appropriate to a traditional workplace [62]. The requirement for accurate calibration is one of the significant challenges in eye movement [61].

Physiological/Behavioural Biometrics

Some biometric characteristics fall under both the physiological and behavioural biometric categories, such as voice recognition.

- **Voice Recognition** Voice recognition is a software-based biometric technology that uses audio to recognise a user's identity. It is a mixture of physiological and behavioural biometrics that depend on characteristics influenced by physiological or behavioural elements. The former includes the health of a person's vocal cords and their physical shape and size, whereas the latter includes the user's emotional status while speaking, as well as their accent and tone of voice [114][184]. Although easy to use, voice recognition technology is not universal, as individuals who are mute cannot use this technique. Furthermore, a user's voice can be influenced by factors such as illness and emotional state. Background noise poses a challenge for voice recognition, as noise can produce false input that may affect the decision phase of the biometric recognition system [114][184].

2.5.2 Biometrics System Applications

Sabhanayagam et al. [171] classified the applications that use biometric technology into three main groups: commercial, governmental and forensic applications. The ***commercial application*** of biometrics refers to biometric systems in large commercial organisations and customer-facing environments. These include logical or physical access control, time and attendance records, and banking and financial services. The ***government application*** of biometrics involves biometric systems that help the government protect sensitive data or even provide services to citizens. These include immigration checks, communications systems, border control and healthcare and social services delivery. Finally, the ***forensic application*** of biometrics refers to biometric systems that contribute to forensic investigations by correlating traces to the individuals present in a database. This includes achieving justice, law enforcement and surveillance.

2.5.3 Biometric Evaluation: Types and Metrics

Types of Evaluations

Biometric performance evaluations can be classified into three main types: technology, scenario and operational. These are described below.

Technology evaluation is the most common type; it tests technology with the aim of determining technological progress and identifying the most suitable biometric approaches in specific areas. These evaluations also provide performance data that are used to select algorithms for scenario evaluations. In contrast to the other evaluation types (discussed below), technology evaluations are short in duration [129][158].

Scenario evaluation aims to determine whether a biometric technology meets all the performance requirements of specific applications by testing them in typical real-world application conditions. The objective of a scenario evaluation can also be to test combinations of sensors and algorithms [129][158].

Operational evaluation aims to determine the effect of implementing a biometric system on workflow. Operational evaluations have the same objectives as scenario evaluations, except that these tests are conducted using real-world applications and real-end users[129][158].

Performance Metrics

Several metrics are used to evaluate the performance of any biometric authentication system as outlined below [25] [55] [99] [193] [198]. There are two categories of metrics according to the type of application used for evaluating the performance of an authentication system. These are verification one-to-one (1:1) metrics and identification one-to-many (1:M) metrics.

The common metrics are as follows:

1. *Failure to enrol (FTE) rate:* The FTE rate represents the percentage of users who cannot supply an appropriate reference template in a biometric system database. In other words, users fail to enrol in the biometric system.

2. *Failure to acquire (FTA) rate:* FTA occurs when the extraction of a biometric feature process is unsuccessful because of a failure to capture, a lack of quality samples or an inadequate number of features.

Examples of failures include difficulties with the physical sample (dirty or scarred fingerprints), sensor issues (swiping the finger too quickly) and environmental concerns (low lighting for facial recognition). These are due to inadequate human–computer interaction (or lack of training) and sensitivity of the recording equipment.

The metrics for verification include the following:

1. *True accept rate (TAR):* The TAR represents the possibility that the system matches a valid user to that user's stored template within the system. The TAR is defined by the equation 2.1.

$$TAR = \frac{TA}{TA + FR} \tag{2.1}$$

where TA represents the number of *true accepts* (where the system rightly matches a valid user) and FR represents the number of *false rejects* (where the system rejects a valid user).

2. *False accept rate (FAR):* The FAR represents the number of people incorrectly deemed to be valid users based on templates stored in a biometric system. The FAR is defined by the equation 2.2.

$$FAR = \frac{FA}{FA + TR} \tag{2.2}$$

where FA represents the number of *false accepts* (indicating that the system incorrectly matches an impostor to a verified user) and TR represents the number of *true rejects* (indicating that the system correctly rejects an impostor).

3. *False reject rate (FRR):* The FRR represents the number of valid users who were incorrectly rejected from a biometric system. The FRR is defined by the equation 2.3.

$$FRR = \frac{FR}{FR + TA} \tag{2.3}$$

4. *Equal error rate (EER):* The EER indicates the point at which the FAR and FRR are equal. The lower the system's performance, the higher the EER value, and vice versa.

Additionally, metrics are used while the system is in identification mode. These include the following:

1. True positive identification rate (TPIR). This is the rate at which the system returns the user's proper identity. In identification systems, a ranked list of users who are most closely related with the profile, instead of a single person, might be returned. The user is presumed to be enrolled into the system. Several variants of TPIR may be reported. These reflect varying degrees of stringency regarding what constitutes a successful identification. For example, an identification might be considered successful if it appears in the first, first three or first five results.

2. False positive identification rate (FPIR). This is the rate with which users who are not enrolled in the system are incorrectly identified. This error rate exists only in open-set identification, as all users are enrolled in closed-set identification.

3. False negative identification rate (FNIR). This is the rate at which the system fails to return the correct identity for a user. The user is considered to be enrolled and directly associated with the TPIR (FNIR = 1 – TPIR).

Data Presentation Curve Metrics

The common metrics that use curves for describing authentication systems' performance are the receiver operating characteristic (ROC) curve, the detection error trade-off (DET) curve and the cumulative match characteristic (CMC) curve. These can be described as follows:

1. **ROC curve:** ROC curves are common and useful graphical depictions of classification performance [60]. ROC curves report on the performance of a biometric system (in 1:1 verification). In an ROC curve, a point represents the true and false accept rates achieved by a specific decision threshold. The FAR is plotted on the X-axis and the TAR is plotted on the Y-axis.
2. **DET curve:** Researchers generally use a DET curve to report on the performance of biometric systems in verification mode. The DET curve is a plot of FAR versus FRR that depicts a system's performance at various decision thresholds [76]. In the DET curve, the FRR is plotted on the X-axis and the FAR is plotted on the Y-axis.
3. **CMC curve:** A CMC curve can be used to evaluate a biometric system's performance in identification mode [55]. The CMC curve is a plot of rank against identification probability that shows how likely a sample is to be amongst the top closest matches [76].

2.5.4 Biometrics Comparison

This section provides some comparative tables for the most common biometrics based on various quantitative and qualitative aspects.

Qualitative Analysis

Based on the required biometric characteristics: The biological measures applicable to biometrics consist of any human characteristic (physiological or behavioural) that fits the following criteria[102][129]:

- **Uniqueness:** This criterion is generally regarded as essential for most biometrics. A unique characteristic is any feature specific to one person (i.e. no two people share an identical version of this characteristic), such as fingerprints.
- **Universality:** This criterion establishes that the source of the biometric measurement is present in each person, as is the case with DNA. DNA is universal because, although its specific content differs from person to person, every person's cells contain DNA.
- **Permanence:** This criterion indicates that the biometric characteristics of each individual remain constant over time. For example, the iris is considered a permanent biometric element because it remains unchanged over decades. Unlike the iris, facial features may vary with age, and fingers are vulnerable to injury.

- **Collectability:** Collectability criteria define how easily a sensor can collect a sample.

  Collectability criteria dictate that a biometric characteristic is easy to assemble and is quantitatively measurable.

- **Acceptability:** This criterion refers to both the user's acceptance of the authentication system and the confidence that the system is not harmful to users in the long term. For example, the use of infrared light in iris recognition could potentially cause harm to the iris if it is consistently overexposed.

- **Circumvention:** The circumvention criterion indicates the security of the authentication system. This addresses the strength of the biometric characteristics against attacks and different methods of fraud, such as fake biometric traits.

- **Performance:** The performance criteria indicate that the biometric characteristic must be accurate, speedy, robust and operative for the specific environment.

Table 2.4: Comparison of the most common biometrics based on the required characteristics (Low: L, Medium: M and High: H)[171, 1].

Biometric	Uniqueness	Universality	Permanence	Collectability	Acceptability	Circumvention	Performance
Fingerprint	H	M	H	M	M	M	H
Face	M	H	M	H	H	H	L
Iris	H	H	H	H	M	L	H
Retina	H	H	H	M	L	L	H
Palm	H	M	H	M	M	M	H
Hand Geometry	M	H	L	H	M	M	M
DNA	H	H	H	L	L	L	H
Ear	M	M	H	M	H	M	M
Signature	L	L	L	H	H	H	M
Keystroke	L	L	L	M	M	M	L
Gait	L	L	L	H	M	M	L
Voice	L	M	L	M	H	H	L

Based on significant factors: In Table 2.5, we focus on some factors from a social perspective. These include safety, ease of use, popularity, speed and social introduction.

Based on biometric users' requirements: Table 2.6 shows a comparison between the biometrics, depending on the most important requirements for users. These include resistance to fraud and privacy, in addition to accuracy and cost.

Quantitative Analysis

Based on performance evaluation metrics: Performance evaluation metrics to differentiate amongst the different biometrics types, as illustrated in Table 2.7. These metrics include the FRR, FAR, EER and FTE rates. The table also lists some factors that affect the performance rate of each biometric technique.

Table 2.5: Comparison of the most common biometrics based on significant factors (Low: L, Medium: M and High: H)[171, 185, 133].

Biometric	Ease of Use	Popularity	Speed	socially introduced
Fingerprint	H	H	H	1981
Face	H	H	M	2000
Iris	M	M	M	1995
Retina	L	L	M	1999
Palm	M	L	M	1994
Hand Geometry	H	L	H	1986
DNA	L	H	L	1965
Ear	H	L	M	2002
Signature	H	H	H	1970
Keystroke	L	L	M	2005
Gait	H	L	M	2002
Voice	H	H	H	1998

2.5.5 Machine Learning (ML) and Biometrics

ML is a science that aims to make computers capable of simulating human learning activities. It has also been characterised as a discipline focusing on developing a collection of algorithms that increase the accuracy of applications' outputs. From these definitions, it has been concluded that, in the context of biometric systems, ML is a science that studies biometric features with the intention of simulating the human ability to determine identity [54].

ML algorithms may assist in identifying an individual's identity by distinguishing and extracting biometric features. Typically, ML techniques are categorised into four broad categories: supervised learning, unsupervised learning, semi-supervised learning and reinforcement learning (see Figure 2.6). In the following, we present a summary of each of these types.

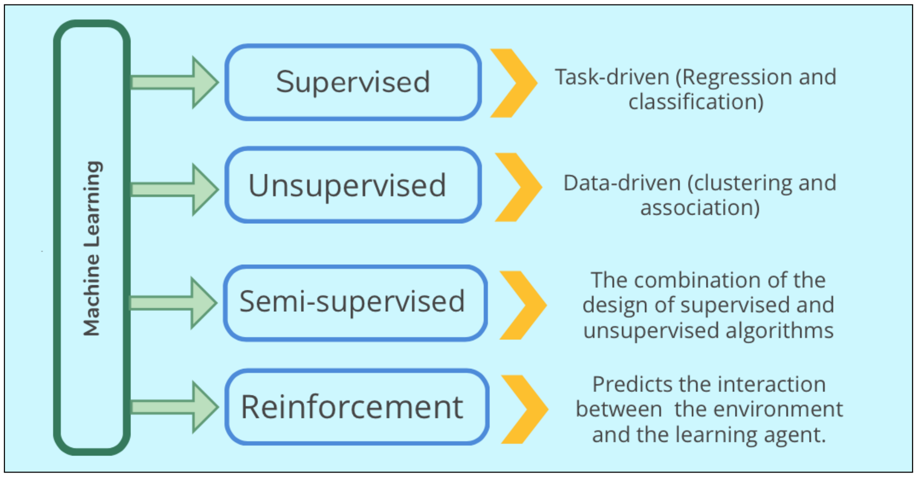

Machine Learning
Supervised
Task-driven (Regression and classification)
Unsupervised
Data-driven (clustering and association)
Semi-supervised
The combination of the design of supervised and unsupervised algorithms
Reinforcement
Predicts the interaction between the environment and the learning agent.

Figure 2.6: Machine learning methods.

Table 2.6: Comparison of the most common biometrics based on biometrics users' requirements (Low: L, Medium: M and High: H) [185, 171].

Biometric	Resistance to fraud	Privacy	Accuracy	Cost
Fingerprint	L	H	H	L
Face	M	H	M	M
Iris	M	H	H	H
Retina	H	L	H	H
Palm	M	H	M	L
Hand Geometry	H	L	M	H
DNA	H	L	H	H
Ear	H	L	M	M
Signature	M	H	M	M
Keystroke	H	L	M	M
Gait	H	L	M	M
Voice	M	M	L	L

Table 2.7: Comparison of the most common biometrics based on performance evaluation [171, 185].

Biometric	FRR (%)	FAR(%)	EER(%)	FTE(%)	Error Incidence
Fingerprint	0.4 -2	0.1-2	2	0.1	Dryness, dirt, age, injury
Face	1-10	0.1-1	-	-	Lighting, age, glasses, hair
Iris	0.99-1.4	0.1- 0.94	0.01	0.5	Lighting, glasses
Retina	0.04	0.91	0.8	0.8	Glasses
Palm	-	-	-	-	Injury
Hand Geometry	2	2	1	-	Hand injury, wearing jewellery
DNA	-	-	-	-	
Ear	-	-	-	-	
Signature	-	-	-	-	Changing signature
Keystroke	0.1	7	1.8	-	Tiredness, mood, medication effects
Gait	-	-	-	-	Clothing, lighting, illness, weight, pregnancy
Voice	5-10	2-5	6	-	Noise, illness

Supervised learning: The objective of supervised learning is to reach a desired level of accuracy by correcting predictions via a training process when the machine's predictions are incorrect [132]. This means that the algorithms used in supervised learning learn to predict output based on input data. The training data in supervised learning used as input for the algorithm are called labelled data [78]. The label therefore defines what the target outcome for the developed ML classifier predictor will be. Supervised learning can solve problems related to regression and classification. The common algorithms used in supervised ML are listed in Table 2.8.

Table 2.8: Common algorithms used in supervised learning

Regression algorithms	Classification algorithms
Ordinary least aquares regression (OLSR)	naive Bayes
Linear regression	support vector machine (SVM)
Logistic regression	k-nearest neighbour (kNN)
Stepwise regression	linear discriminant analysis (LDA)
Multivariate adaptive regression aplines (MARS)	random forest (RF)
Locally estimated scatterplot smoothing (LOESS)	
Ensemble algorithms	
Decision tree (DT)	

Unsupervised learning: Unsupervised learning aims to determine and present the structure found in input data as a means of learning more about those data [132]. The algorithms learn to discover structures based on the input data. In contrast to supervised learning, unsupervised learning uses the term ‘unlabelled’ data to refer to training data [78]. Unsupervised learning problems can be classified as either clustering or association problems. Clustering is a fundamental concept in unsupervised learning. It is primarily concerned with identifying a structure or pattern within an uncategorised set of data. Using association rules, we can create connections between data objects in large databases. The aim of this unsupervised technique is to find relevant relationships between variables in large datasets. The common algorithms used in unsupervised ML are listed in Table 2.9.

As shown in Table 2.9, research on association analysis uses the unsupervised machine learning technique called *Equivalence Class Clustering and bottom-up Lattice Traversal (ECLAT)*. This algorithm was developed by Zaki et al. [215]. The ECLAT algorithm's primary purpose is to estimate the strength of correlation between various item sets that correspond to multiple transactions. Apriori [4] is the most conventional algorithm used for the same purpose in industry. However, ECLAT is usually preferred to Apriori since it employs a depth-first search strategy as opposed to Apriori's breadth-first search strategy, which ultimately results in faster performance and being better suited for parallel processing.

Table 2.9: Common algorithms used in unsupervised learning

Clustering	Association
k-Means	Apriori algorithm
k-Medians	ECLAT algorithm
Expectation Maximisation	
Hierarchical Clustering	

Reinforcement learning: Reinforcement learning is a kind of learning that focuses on teaching a system to control itself in such a way that it maximises a numerical performance metric that represents a long-term goal [192]. Unlike supervised learning, reinforcement learning only gives partial feedback on the learner's predictions. The forecasts may also influence the future condition of the controlled system [192]. The most common algorithms used in reinforcement learning are deep learning (DL), decision trees, SVM and kernel perceptrons.

Semi-supervised learning: Semi-supervised learning aims to comprehend the changes in learning behaviour caused by labelled data (e.g. classifications in supervised learning) and unlabelled data (e.g. clustering in unsupervised learning), and then to use this combination for algorithm design [220]. The most popular algorithms used in semi-supervised learning are self-training algorithms [169] and co-training algorithms [26].

Any approach to ML depends on the same four components: the dataset, feature selection, the learning algorithm and module evaluation. These represent what is known as the ML design cycle [134]. The input used in the ML method is called the *dataset*. It sometimes requires a pre-processing stage, such as data cleaning, data normalisation, data aggregation, data abstraction/new data construction, data reduction or a combination of these. Typically, the data in the dataset are divided into the training set and the testing set. *Feature selection* is a technique utilised for discovering and removing irrelevant and redundant information. The main goal of the feature selection method is to build a small subset of highly predictive features by avoiding non-essential training data. Popular feature selection approaches involve the wrapper and filter methods. The former identifies the accuracy of the feature subsets, whereas the latter distinguishes and eliminates undesirable features. The learning algorithm can be exposed as a function (x) that takes a new input x from a training set of data. It then predicts the output value y for the data in the testing set. The *module evaluation* step is concerned with defining the learning algorithm's effectiveness and performance when applied to different collected datasets using an evaluation metric and dependable calculation methods.

Algorithms Used in Biometric Systems

Previously, we provided a general overview of the four fundamental types of ML. This section addresses the algorithms used in biometric systems, including artificial neural networks (ANNs), DL and PR.

ANNs are biologically inspired statistical paradigms. They have also been described as computer programmes invented to mimic the human brain in how it processes data and solves problems [3]. Neural network algorithms are ML-based methods adopted to resolve several real-world issues. They can be applied to many applications, such as image or speech recognition and natural language processing. Hopfield networks, back-propagation, radial basis function networks and perceptrons are the four most widely utilized algorithms in ANNs.

DL is an ML algorithm that uses multiple layers of neural networks to learn feature representation, especially when dealing with most biometric systems. It is also applied to a wide variety of other areas, including robotics, computer vision and natural language processing [21]. Learning via DL algorithms can be supervised (e.g. classification), unsupervised (e.g. extracting biometric data) or semi-supervised. The most common algorithms used for DL are convolutional neural networks, deep Boltzmann machines, deep belief networks, recurrent neural networks and stacked auto-encoders.

PR aims for supervised or unsupervised classification [100]. The ability to learn from a set of samples (training set) is an essential and desirable feature of the majority of pattern recognition systems [100]. Template matching, statistical classification, syntactic matching, and neural networks are the four most well-known methods for PR [100]. Data mining, document classification, multimedia database retrieval, speech recognition, and biometrics recognition are some of PR applications [100].

2.5.6 Threat Modelling for Biometrics

Biometric technologies have emerged as a means of avoiding the weaknesses and issues involved in conventional authentication methods. However, biometric authentication is part of the overall authentication framework, which renders it vulnerable to various types of attacks. The aim of these attacks is to either impersonate someone or to prevent someone from being authenticated.

In the standard procedure of a biometric system, biometric data pass through several stages: collection, processing, sending via a communication channel, storage and retrieval. At every stage of the process, maintaining the security and privacy of the biometric data is necessary. Several types of attacks can threaten biometric systems, as shown in Figure 2.7. These attacks can be classified into two groups: direct attacks and indirect attacks [200]. In the former, the attacker does not need any understanding of the authentication system's operations; these attacks target the sensing phase. In the latter, for an attack to be successful, the attacker must be aware of the authentication system's operations. These attacks target the feature extraction, matching and decision phases; the template database; and the communication channels between phases.

Direct Attacks

1. **Denial of service (DoS)** [165] attacks are intended to shut down the sensor device in a biometric system, rendering it unavailable to its legitimate users.

2. **Fake biometrics** symbolise spoofing attacks, fake physical biometrics and fake digital biometrics.

   - Fake physical biometric attacks use a fake biometric feature, such as a synthetic fingerprint made with wax or a face mask, which is presented to the sensor [90].
   - Fake digital biometrics can consist of [165] (a) false data based on easily accessible biometric data, such as digital facial images. Masquerade attacks are a term used

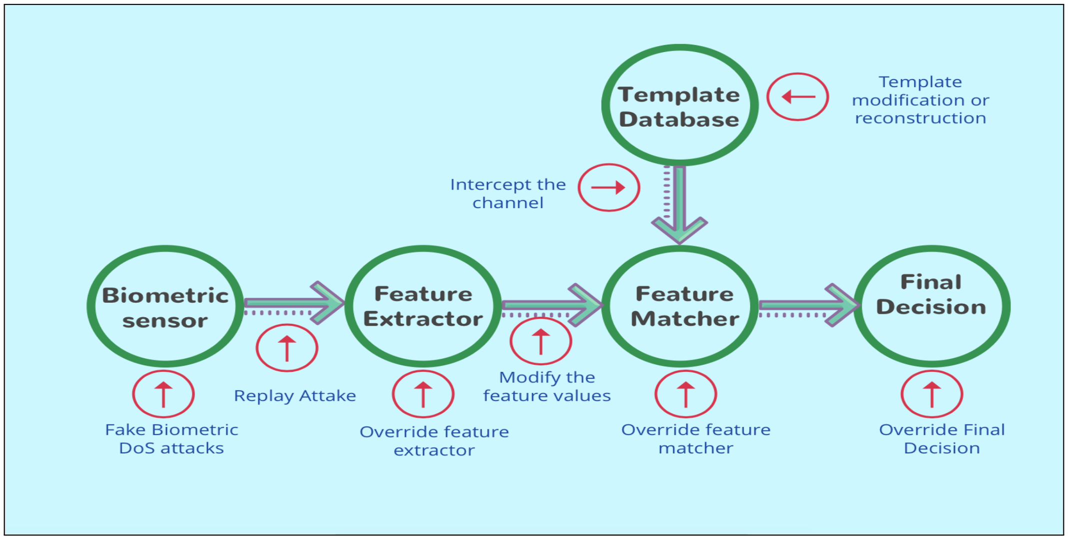


Figure 2.7: Biometric authentication system attacks [165].

to describe these types of attacks. (b) Inside the biometric system, a reference set replay attack can occur. Furthermore, the attackers must have knowledge of the biometric system and, in most cases, system access.

3. **Latent print reactivation** [165] refers to the abuse of features such as fingerprints that are captured obliquely by lifting a latent sample. Fraudulent users take and reuse these captured features for authentication.

Indirect Attacks

1. **Template modification or reconstruction** occurs when an attacker uses a database template to modify, remove or introduce new templates. This may lead to two outcomes. First, fraudsters may be able to use the system. Second, they may prevent authorised users from doing so.

2. In an **override attack**, the attacker uses an executable program, such as a Trojan horse, to attack three modules of a biometric system: the feature extraction phase, the matching phase and the decision phase. As a result, the attacker can accomplish the following:

   - Override the feature extraction and produce false feature sets
   - Override the feature matching to produce a false match for legitimate users or a true match for fraudulent users
   - Override the decision phase to produce acceptance of the fraudsters or false rejection of legitimate users

3. By **intercepting communication channels**, an attacker can interfere with the communication channels amongst various modules in the structure of the biometric system during its transmission. Then, the attacker can accomplish the following:

   - Cut the communication link to deny legitimate users access to the system
   - Intercept the channel between the sensor module and the feature extractor module to record biometric data for reuse (This type of attack is called a replay attack. An example would be using a recorded audio signal.)
   - Intercept the channel between the feature extractor module and the feature matcher module to modify or steal the feature values of the original user[121]
   - Intercept the channel between the system database and the feature matcher module to modify the content of the templates before they are presented to the feature matcher

4. When ***modifying access rights***, an attacker may take advantage of a DoS attack to modify (either by increasing or decreasing) a user's rights to breach the security of a biometric system. The attacker can also claim administrator privileges, which allow them access to sensitive information and data [165].

2.6 Continuous Authentication (CA)

Section 2.4 covers a one-time process or the principle of traditional authentication (a user is authenticated or not based on a decision made at a certain moment). CA refers to a security system that continuously (or at least often) observes user activities during a session and determines whether the user is genuine [80]. The advantages of CA over a traditional authentication method may be measured in terms of security, safety and convenience [80]. CA aims to limit the possibility of impersonation in terms of security. For example, if an attacker takes a smartphone after obtaining the password illegally, CA may enable the device to lock itself after seeing that the use behaviour varies from that of the genuine user. As far as safety is concerned, continual monitoring of users may avoid potentially dangerous situations. In terms of comfort, CA analysis of the user's activities is transparent and does not interfere with the user's actions, such as by regularly requiring the user to re-authenticate.

Most CA accesses begin in the log-in mode, which verifies the user's identity and obtains their template from the database if permission is successful [53]. After the log-in, the system moves to the verification mode to continuously check the identity of the user and ensure that they are the same person authenticated at the beginning of the session [53]. The log-in phase may utilise the same biometric verification as the continuous verification step, it can require other means of identification (e.g. additional biometrics, passwords, cards or tokens), or it can use a hybrid of both [53].

One of the technologies supporting CA is behavioural biometrics. Behavioural biometrics continuously profile a user's behaviour based on natural interactions without interrupting users continually. Re-authentication and/or CA using behavioural biometrics can be less disruptive than alternatives, e.g. short inactivity time-outs requiring periodic password re-entry. In addition, a random intruder cannot easily target CA based on behavioural biometrics [125].

2.6.1 Continuous Authentication Using Behavioural Biometrics

CA procedures are believed to improve the security and dependability of systems, and biometric technologies have become increasingly important components of security designs. Behavioural biometrics is gaining traction as a method of verifying a user's identification. The term 'behavioural biometrics' refers to the distinct behavioural characteristics that may be used to verify a person's identity. Behavioural biometrics, in contrast to traditional authentication and physiological biometrics, identify individuals based on how they do a particular task, rather than on static information or physical features.

User authentication using behavioural biometrics is described as unobtrusive and cost effective [125]. With unobtrusive sensing, sensors may monitor actions and behaviours constantly, and the resulting data can be collected and used to optimise usability. When people engage with internet of things (IoT) devices or ambient surroundings without providing explicit input [80], behavioural data may be collected. Furthermore, user authentication may be done in a transparent and unobtrusive manner with no user distraction [125]. For the most part, physiological biometrics depend on specialised technology to acquire data. They tend to be costly, and they make broad implementation difficult. Behavioural biometrics, on the other hand, may be seen and sampled by embedded sensors in IoT devices (for example, a microphone, a touchscreen, a smartphone's acceleration, and wearable technology) [125]. IoT devices provide the capability to detect behaviour without the need for additional hardware, making behavioural biometrics more affordable and easier to deploy [125]. Substantially, the behavioural biometric-based objectives of CA are to determine whether the user has the permission to access the IoT device and to identify who the present user is [125]. CA based on behavioural biometrics may be classified into two types:

1. **Anomaly detection (AD):** This technique can distinguish between normal and abnormal patterns.

2. **Classification:** In this technique, a predictive model is developed to optimise inter-class differences for user identification (i.e. authorised versus unauthorised users).

2.6.2 Performance Evaluation of Continuous Authentication Using Behavioural Biometrics

Most studies use the same metrics to evaluate non-continuous biometric authentication (referenced in Section 2.5.3). The most common metrics are EER, FAR and FRR.

However, in [32], they used the average number of genuine actions (ANGA) and the average number of impostor actions (ANIA), with high values of ANGA and low values of ANIA representing the best results. The ANIA repesents the average number of tasks that

Table 2.10: Evaluation of continuous authentication based on four cases [33].

Rating	Description
Very good	Genuine users are never locked out, and all impostor users are locked out.
Good	This rating has two parts: • Genuine users are never locked out, and some impostor users are not locked out. • Genuine users are locked out, and all impostor users are locked out.
Bad	Genuine users are locked out, and some impostor users are not.
Very bad	Genuine users are locked out, whereas impostor users are not, and the ANIA is higher than the ANGA.

impostors can perform before they are identified, whereas the ANGA represents the average number of tasks that genuine users can perform before they are rejected.

Equation 2.4 shows how to calculate the ANIA of impostor j [33].

$$\text{ANIA}_g^j = \frac{1}{k} \cdot \sum_{j=1}^{k} T_k \tag{2.4}$$

where k is the number of times impostor j was locked out if they are classified as a user other than the genuine user g after $T_1, T_2 ... T_k$ tasks. If we assume that N represents all participants, the ANIA of overall impostors $(N-1)$ against one genuine user can be calculated by (2.5) [33].

$$\text{ANIA}_g = \frac{1}{N-1} \cdot \sum_{j=1}^{N-1} \text{ANIA}_g^j \tag{2.5}$$

Consequently, the equation 2.6 is used to determine the ANIA against any genuine user in the system.

$$\text{ANIA} = \frac{1}{N} \cdot \sum_{g=1}^{N} \text{ANIA}_g \tag{2.6}$$

Similarly, the ANGA is calculated, where genuine user g is tested against their own template.

In [141], they used four ratings (very good, good, bad and very bad) to evaluate their CA scheme. These ratings are assigned based on the rates of legitimate user lockouts and impostor user non-detection. Table 2.10 illustrates these cases. The categorisation **applies to a single user**.

2.6.3 Threat Model against Behaviour-based CA

The continuous presence of the originally authenticated consumer, particularly in a shared workplace, could prevent so-called lunchtime attacks. Such attacks happen when a previously authenticated consumer steps away from their workplace, enabling the adversary to take over their authentication session and participate in possibly malicious activity [103]. Re-authentication and/or CA using behavioural biometrics can be less disruptive than the case with too short inactivity time-outs requiring periodic password re-entry. In addition, a random intruder cannot easily target CA based on behavioural biometrics [125]. However, behavioural biometrics do not inherently make continuous authentication systems secure. A behavioural biometric system may face a variety of threats, including malware and shoulder surfing attacks, mimicry, impersonation, spoofing and replay, as well as statistical, algorithmic and robotics attacks [187]. These attacks are classified as zero-effort attacks or non-zero-effort attacks.

Zero-effort attacks: Zero-effort attacks are often used to test the accuracy and durability of biometric authentication systems [131]. This measure is useful for comparing individuals or inter-class distributions. Typically, zero-effort evaluation is based on the similarity of templates between the attacker and the genuine user and is related to a biometric characteristic's uniqueness [187].

Non-zero-effort attacks: Non-zero-effort attack requires the attacker performing sophisticated activity to successfully mimic a genuine user. The complexity of an adversarial attack is significantly influenced by the available resources, time and knowledge about the biometric system and the victim [142].

2.6.4 State of the Art

In this part, we analyse the current state of the art, both in terms of the metrics reported and the ML methods used to achieve the findings. We analysed 28 systems using eight distinct biometrics, with a particular emphasis on recently published work. While each of these systems has a different experimental design, they all provide CA.

Table 2.11 lists all the principal works that use CA based on behavioural biometrics. As can be observed, several CA approaches use various devices and achieve good authentication performance. It has been noted that most researchers are interested in studying the CA system on smartphones. **Existing solutions, on the other hand, do not look into CA in a robotics context.**

In terms of methodologies, it is worth noting that the classification method is more commonly used than anomaly detection; the RF, SVM and KNN classification algorithms are most frequently used.

Based on Table 2.12, we can see that EER, FAR and FRR are the most common metrics used to evaluate the biometric system.

In addition, we conduct a literature review of the following methodological components that may have an influence on error rates: threat model (see Section 2.6.3) and ML hyper-parameters tuning.

Hyper-parameters are modifiable parameters that regulate the model training process. When all the features have been extracted and normalised, a suitable classifier must be selected. Numerous hyper-parameters must be created depending on the classifier. For example, the SVM has kernel type, soft margin constant C and bandwidth of kernel function $sigma$. Hyper-parameters tuning (sometimes referred to as hyper-parameters optimisation) is the process of determining the optimal process of determining optimal, or at least high performing, combination of hyper-parameters.

Two of the most common ways for hyper-parameters tuning are grid search (GS) and random search (RS). GS takes the ranges of individual features and reduces each range to a discrete set of ”representative" points, e.g. the continuous interval (0,1) might be represented by the set 0,0.2,0.4,0.6,0.8,1.0. Exhaustive grid search will attempt all combinations of feature values from such sets. Thus, a search over two parameters with range [0,1] would evaluate at all possible pairs (0,0), (0,0.2), (0,0.6)...(1.0,1.0). RS will repeatedly sample from each domain to form a set of parameters to be be evaluated. Thus, a sequence of candidates for this example of the form (x, y) would be generated where x is randomly selected from (0,1) and so is y.

As shown in Table 2.13, all studies evaluate their CA system against zero-effort attacks, whereas only eight studies evaluate their system against non-zero-effort attacks. Additionally, we can see that only nine studies use hyper-parameter tuning as part of their approach, and none of them use RS methods.

Table 2.11: Summary of continuous authentication works using behavioural biometrics.

			ML		# of Users	Performance
Biometric	Publications	Platform	Algorithm	Method		
Behavioural profiling	[75] in 2016	smartphone	SVM	Classification	200	1% EER
	[38] in 2017	smartphone	DL	Classification	20	2.2% EER
	[11] in 2018	smartphone	RF	Classification	10	96.5% F1-score
	[123] in 2018	smartphone	SVM	Classification	100	4.66% EER
	[174] in 2019	smart office	RF	Classification	5	96.76% F1-Score
	[6] in 2019	smartphone	GB,RF,KNN	Classification	76	26.98% EER
Touch Gestures	[72] in 2012	smartphone	KNN, SVM	Classification	41	0%–4% EER
	[218] in 2013	smartphone	Distance metric	Classification	30	2.62% EER
	[213] in 2019	smartphone	OCSVM,iForest	AD	45	95.85% Accuracy
	[7] in 2020	smartphone	RF	Classification	26	92.81% Accuracy
Signature	[35] in 2016	smartphone	MLP, KNN, RF	Classification	30	3.1% FAR
Keystroke Dynamics	[2] in 2018	smartwatch	Distance metric	Classification	34	99.2% Accuracy
	[74] in 2015	computer	NB, SVM	Classification	67	1.0% FRR
	[97] in 2014	computer	SVM	Classification	110	100% Accuracy
Mouse Dynamics	[140] in 2013	computer	SVM	Classification	49	96 ANIA
	[181] in 2012	computer	SVM, NN, KNN	Classification	28	0.37% FAR
	[66] in 2012	computer	RF	AD	25	7.5% EER
Gait	[151] in 2021	smart socks	SVM, softmax	Classification	15	0.01% EER
		smart shoes	SVM, softmax	Classification	10	0.16%EER
	[209] in 2020	smartwatch	KNN	Classification	36	3.5% EER
	[144] in 2019	smartwatch	RF	Classification	10	8.2% EER
	[142] in 2017	smartphone	DTW	Classification	35	13% EER
	[219] in 2015	smartphone	Distance metric	Classification	51	7.22% EER
	[157] in 2015	smart kiosk	SVM	Classification	38	92% Accuracy
	[145] in 2012	smartphone	KNN	Classification	36	8.24% EER
Eye Movement	[178] in 2019	smart cars	LDA,SVM,NN	Classification	22	8% EER
	[217] in 2018	smart glasses	KNN, SVM, SRC	Classification	30	6.9% EER
	[62] in 2016	computer	KNN,SVM	Classification	30	1% EER
Voice	[68] in 2017	voice assistants	SVM	Classification	18	97% Accuracy

LDA: Linear Discriminant Analysis, NN: Neural Networks, GB: gradient boosting, SRC: Sparse Representation Classification, RF: Random Forest

SVM: Support Vector Machine, DTW: Dynamic Time Warping, KNN: K-Nearest Neighbors, DL: Deep learning, iForest: Isolated Forest, OCSVM: One-class SVM

Table 2.12: Metrics used to evaluate behaviour-based continuous authentication systems in related works.

Biometric	References	Accuracy	F1-score	Conf.matrix	TAR	TRR	FAR	FRR	EER	ROC	ANIA	ANGA
Behavioural profiling	[75] in 2016	×	×	×	×	×	✓	✓	✓	✓	×	×
	[38] in 2017	×	×	×	×	×	×	×	✓	✓	×	×
	[11] in 2018	✓	✓	×	×	×	×	×	×	×	×	×
	[123] in 2018	×	×	×	×	×	✓	✓	✓	×	×	×
	[174] in 2019	×	✓	×	×	×	×	×	×	×	×	×
	[6] in 2019	×	×	×	×	×	×	×	✓	×	×	×
Touch Gestures	[72] in 2012	×	×	×	×	×	×	×	✓	×	×	×
	[218] in 2013	×	×	×	×	×	×	×	✓	✓	×	×
	[213] in 2019	✓	✓	×	×	×	×	×	×	×	×	×
	[7] in 2020	✓	✓	×	×	×	×	×	×	×	×	×
Signature	[35] in 2016	×	×	×	✓	✓	✓	✓	×	×	×	×
Keystroke Dynamics	[2] in 2018	✓	×	×	×	×	×	×	×	×	×	×
	[74] in 2015	×	×	×	×	×	✓	✓	×	×	×	×
	[97] in 2014	×	×	×	×	×	×	×	×	×	×	×
Mouse Dynamics	[140] in 2013	×	×	×	×	×	×	×	×	×	✓	✓
	[181] in 2012	×	×	×	×	×	✓	✓	×	×	×	×
	[66] in 2012	×	×	×	×	×	✓	✓	✓	✓	×	×
Gait	[151] in 2021	×	×	✓	×	×	✓	×	✓	×	×	×
	[209] in 2020	✓	×	×	×	×	✓	✓	✓	×	×	×
	[144] in 2019	✓	×	✓	×	×	×	×	✓	×	×	×
	[142] in 2017	×	×	×	×	×	×	×	✓	×	×	×
	[219] in 2015	×	×	×	×	×	×	×	✓	✓	×	×
	[157] in 2015	✓	×	×	×	×	×	×	×	×	×	×
	[145] in 2012	×	×	×	×	×	×	×	✓	×	×	×
Eye Movement	[178] in 2019	×	×	×	×	×	×	×	✓	×	×	×
	[217] in 2018	✓	×	×	×	×	✓	✓	✓	×	×	×
	[62] in 2016	×	×	×	×	×	×	×	✓	×	×	×
Voice	[68] in 2017	✓	×	×	×	×	✓	×	×	×	×	×

✓Explicitly reported, × Not reported

Table 2.13: Design choices in related works that used behaviour-based continuous authentication

		Threat Model		Hyper-parameters	
Biometric	Publications	Zero-effort Attacks	Non-zero-effort Attacks	Values	Method
Behavioural profiling	[75] in 2016	✓	×	×	×
	[38] in 2017	✓	×	✓	×
	[11] in 2018	✓	×	×	×
	[123] in 2018	✓	×	✓	GS
	[174] in 2019	✓	×	×	×
	[6] in 2019	✓	×	×	×
Touch Gestures	[72] in 2012	✓	×	✓	×
	[218] in 2013	✓	×	✓	GS
	[213] in 2019	✓	×	×	×
	[7] in 2020	✓	×	×	×
Signature	[35] in 2016	✓	×	×	×
Keystroke Dynamics	[2] in 2018	✓	✓	×	×
	[74] in 2015	✓	✓	×	×
	[97] in 2014	✓	×	✓	×
Mouse Dynamics	[140] in 2013	✓	×	×	×
	[181] in 2012	✓	×	✓	×
	[66] in 2012	✓	×	×	×
Gait	[151] in 2021	✓	✓	✓	GS
	[209] in 2020	✓	✓	×	×
	[144] in 2019	✓	×	×	×
	[142] in 2017	✓	✓	×	×
	[219] in 2015	✓	×	×	×
	[157] in 2015	✓	×	×	×
	[145] in 2012	✓	×	×	×
Eye Movement	[178] in 2019	✓	×	×	×
	[217] in 2018	✓	✓	✓	GS
	[62] in 2016	✓	✓	✓	GS
Voice	[68] in 2017	✓	✓	×	×

✓Reported, × Not reported

2.7 Research Questions

Section 2.3 identifies the need for a new security mechanism that can offer ongoing and visible protection against robotics abuse. The section ends by emphasising the need for a strengthened authentication mechanism and by outlining potential alternatives.

We conclude that additional research is necessary to determine the importance of CA for manufacturing in collaborative robots, as well as for current human–robot interaction systems, such as exoskeletons and teleoperation. Additionally, we conclude in this thesis that contextual factors, such as unobtrusiveness, support the adoption of behavioural biometrics. As a result, the following research questions have been addressed:

1. How can the identity of human operators be authenticated continuously when working with a collaborative robot?

2. How can the identity of human operators be authenticated continuously using wearable sensors, (such as that present in an exoskeleton)?

3. How can the identity of human operators be authenticated continuously when working with teleoperated robotic systems?

Chapter 3

User Authentication for Collaborative Robots

3.1 Introduction

Traditionally, robots have been segregated from humans by walls, fences and other barriers to ensure safety. However, recent advances in collaborative robotics have provided promising opportunities for robots to share spaces with human workers.

Collaborative robots [194] are designed with more sophisticated sensing and control mechanisms than traditional industrial robots are, and, in the main, they are designed to handle lighter payloads. They are said to combine the benefits of automation (speed, precision, accuracy and repeatability) with the strengths of human workers (dexterity, perception, flexibility and cognitive ability). Along with advances in digital technologies, such as the Internet of Things (IoT), augmented reality and digital twins, collaborative robots will enable more flexible, bespoke processes. This makes them attractive to many manufacturers that have not been able to benefit from large-scale automation.

However, reductions in physical safety barriers and increases in technical complexity give rise to a number of challenging safety and security issues which must be resolved before the benefits of human–robot collaboration can be fully realised. One such issue is user authentication [128]. As collaborative robot use becomes more widespread, there will be an increased need to authenticate users and ensure that they have the appropriate skills, training and authorisation to access, re-program, update and control different elements of collaborative robot systems. At present, traditional authentication methods, such as passwords and identity cards, are used in lockout functionality, but they may be bypassed or abused by workers, leaving safety and security risks unresolved.

Collaborative robot tasks in manufacturing often involve direct interactions between the user and the collaborative robot, e.g. when the user physically moves a manipulator or takes part in some handover of items. The popular physical interactions with collaborative robots are training by demonstration, gravity assist and precision placement of end-effectors in processes with uncertain geometries or locations (e.g. painting, disassembly, assembly, adhesive and welding).

Some users are more forceful or quicker in their interactions, or they may otherwise exhibit an interactive modus operandi that is distinguishably theirs. Consequently, a collaborative robot that can sense how it is manipulated can use that information to distinguish users. As collaborative robots are compliant, we propose the use of this feature (combined with robots' internal positions and force sensors) to measure the actions of human operators (or co-workers) and form a biometric for their continuous authentication.

We believe that this is the first *continuous authentication* approach to be developed in the context of collaborative robots. This is important because collaborative robots engage with their co-workers on a continual basis, which may severely compromise the utility of traditional one-off password schemes. In practice, we envisage that it will be used in the following: in one-off schemes for initial authentication and in continuous authentication for the duration of a work session. We believe that the work presented in this chapter is the first example of biometric authentication in the context of collaborative robots (and robots, in general).

A major benefit of our approach is that user-to-collaborative robot authentication can be implemented with **no additional sensing**. The source data are sensed and used as part of the operational control system of the collaborative robot. If better-performing classification algorithms become available, they can also be directly incorporated through minor software changes.

3.2 Threat Model

In a closed-world environment, such as an organisation, an unauthorised device user is more likely to be an insider threat—someone who comes from within the organisation. In a collaborative robot environment, there will be a greater requirement to authenticate people in order to guarantee that they have the necessary skills, training and authorisation to access, re-program, update and control various aspects of collaborative robot systems.

In this chapter, we will discuss a widely used technique for establishing the accuracy and robustness of biometric authentication schemes. This approach is called a zero-effort attack or intrinsic failure [101]. The threat arises from the fact that there is always a non-zero possibility that two biometric samples from two distinct individuals are sufficiently similar to yield a positive match.

Zero-effort attacks model the case in which an attacker has no information on the behaviour of the target victim. Usually, zero-effort attacks are implemented by comparing biometric samples from different individuals; i.e. the sample profile of one user is assessed for its acceptability as a supplied profile for the second (target) user.

3.3 Proposed User to Collaborative Robot Authentication

We propose the application of continuous biometric authentication to the use of an industrial collaborative robot (see Figure 3.1). Most collaborative robots have integrated sensors, including joint position encoders, force and torque sensors, and even cameras. Here, we use specific sensors to capture co-workers' behaviours in order to implement continuous biometric authentication **without the need for additional, potentially intrusive hardware**. We conducted two experiments in which we asked the subjects to guide a robot arm around a maze (see Fig. 3.2).

1. *whole-task authentication*: Authentication occurs once at the end of the task (one navigation of the maze). Each user performed 15 maze navigation tasks with a trust value calculated after each task. (The trust model is described in Section 3.3.1.) This value determined whether the user was authorised to continue to the next task.

2. *multiple-segment authentication*: Here, we authenticated each user three times during each task as the user passed specific points in the maze. If users were authenticated, they were allowed to continue performing the task.

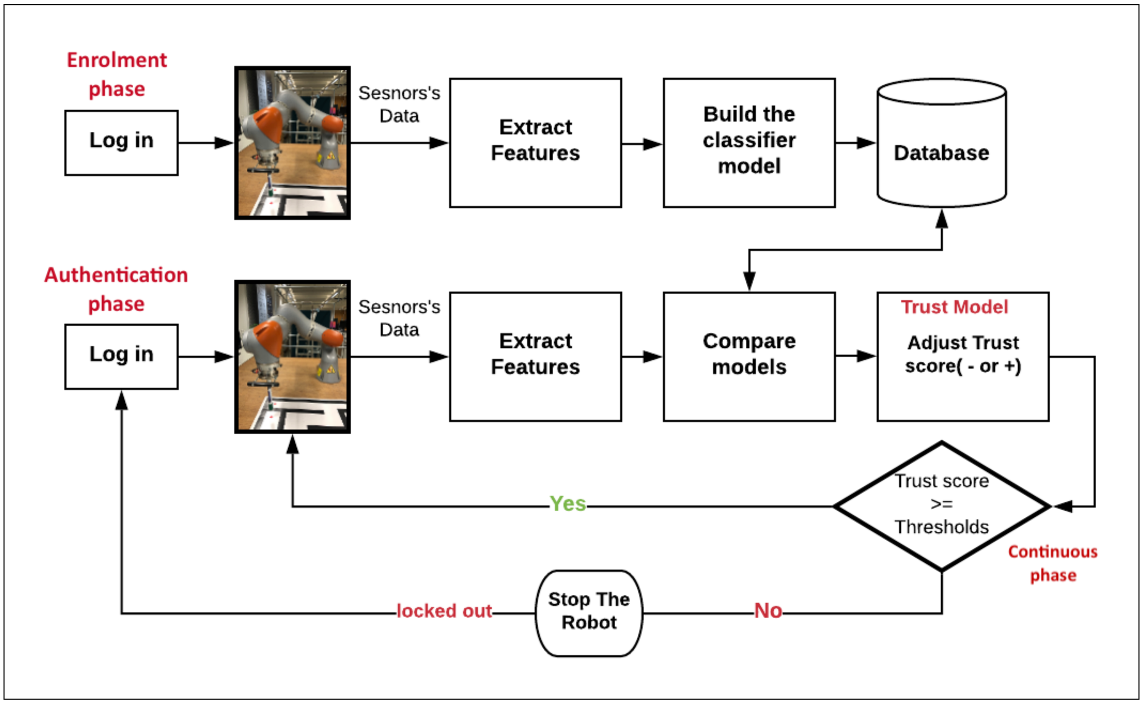


Figure 3.1: Continuous biometric authentication block diagram of our system.

We divided each experiment into three phases: the enrolment phase, the authentication phase and the continuous phase, as shown in Figure 3.1. In the *enrolment phase*, we obtained readings from the robot's sensors and extracted the potential features for user authentication. Those features from the force and torque sensors were the most informative and were used to create the users' profile templates. In the *authentication phase*, these templates were used for user authentication. Each time the robot's co-worker started interacting with the robot, our authentication system compared that user's profile template with all the profile templates in the database to obtain a probability value for each user in the database; the highest probability value was taken to identify the user. However, only the probability value of the authorised user was used to update the current user's trust value. In the *continuous phase*, the trust value was used to determine whether the user was allowed to continue working with the robot or be locked out of the system, reverting to the main authentication log-in, as shown in Figure 3.1.

3.3.1 Trust Model

We use the trust model first proposed by Bours [32] for continuous, behaviour-based biometric authentication. It adjusts the trust score of the current user by matching their dynamic profile template with the authorised user's template [32]. As a default, the user starts with 100 as a trust score. This score is updated (increased or decreased) according to the probability of the genuineness (classification probability score) of the user by using Equation (3.1). If the behaviours of the authorised and current users are similar, the system's trust in the current user increases; otherwise, if the behaviour of the current user is sufficiently different from that of the authorised user, the trust score decreases.

$$C = \begin{cases} \min\left(C + \frac{Z}{2}, 100\right) & \text{if} \quad P \geq 0.5 \\ \max\left(C - \frac{Z}{2}, 0\right) & \text{if} \quad 0.3 \leq P < 0.5 \\ \max(C - (2Z), 0) & \text{if} \quad P < 0.3 \end{cases} \tag{3.1}$$

, where C is the trust score of the user, P is the probability score of the current user against the legitimate user's template, and Z is a constant governing the rate of increase or decrease in the trust score. (In our experiments, Z = 15 in the whole-task authentication and 7.5 in the multiple-segment authentication). The constant Z is set to a value ensuring that the current user is rejected immediately if the probability value becomes low (less than 0.5). The trust score can never exceed 100 or be less than 0. Equation (3.2) presents the decision-making process after calculating the trust value.

$$Decision = \begin{cases} \text{if} \quad C \geq T & \text{Trusted user - continue to next task} \\ \text{if} \quad C < T & \text{Not trusted user - lock out} \end{cases} \tag{3.2}$$

, where T represents the threshold between the trusted user and the untrusted user. (In our experiments, the value $T = 80$ was used.)

3.3.2 Experimental Methodology

Experimental Design

The experiment involved participants interacting with an industrial robot arm to solve a maze. A 2D maze was attached to the work surface within the robot's operating envelope. Start and end points were indicated by red and green circles, and additional authentication test points were marked with a yellow circle, as shown in Figure 3.2. A handle and pointer were

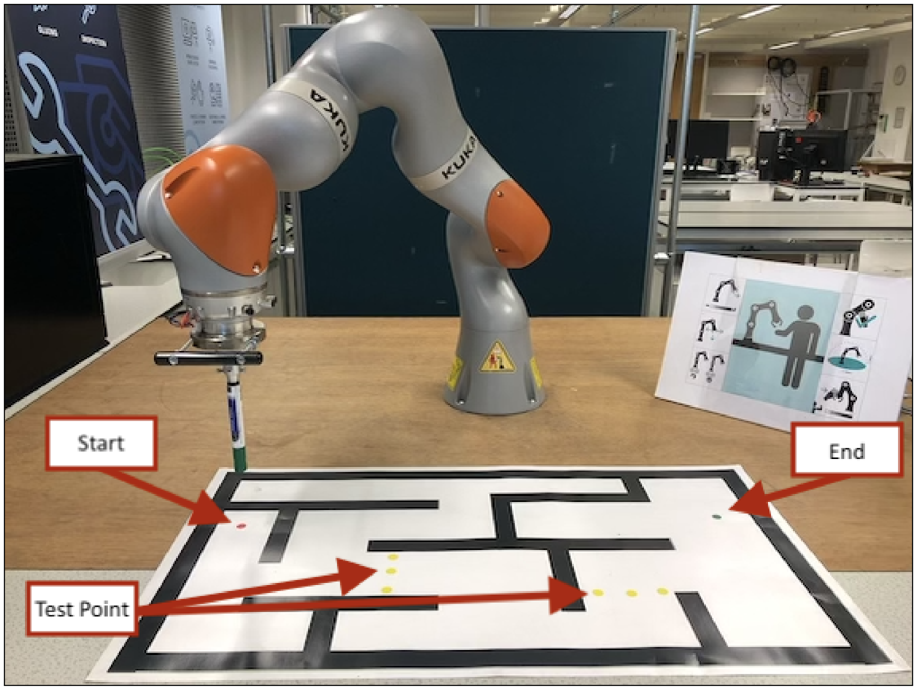


Figure 3.2: Experimental design.

attached to the robot's end-effector to provide an intuitive mechanism for manipulating the robot through the maze.

Selected Collaborative Robot

We used a KUKA iiwa R800 lightweight industrial robotic arm (see Figure 3.2.) The KUKA iiwa R800 has seven joints, each of which has force, torque and position sensing. Data from these sensors were logged during the experiments to capture co-workers' behaviours while manipulating the robot, although we used only the end-effector data in this chapter for classification purposes.

Subjects and Data Collection

The experiments took place on the Sheffield University campus in the Sheffield Robotics Lab. We recruited 30 volunteers (16 males and 14 females) from the University of Sheffield's students and faculty. Users were asked to guide the robot's attached pointer around the maze and trace a trajectory from the start point (red circle) to the endpoint (green circle). They were asked to repeat the same task 15 times. The participants were given a brief introduction to the purpose of the study, and then they performed three practice runs for which data were not recorded. Our data collection controller was based on the Robot Operating System (ROS)-integrated application programming interface for the KUKA iiwa [139]. The robot was placed in compliant mode (i.e., enabling physical interaction between humans and robots), with each user instructed to trace a path from the start point to the end point of the maze. Force and torque data at the end-effector were continually logged (every 0.1 s) as each user traced this path. (We also recorded end-effector position data.) When the user released the end-effector upon task completion, the robot autonomously returned to the start point to begin the next run. In addition, we also calculated the magnitudes of the force and torque.

Feature Extraction and Feature Selection

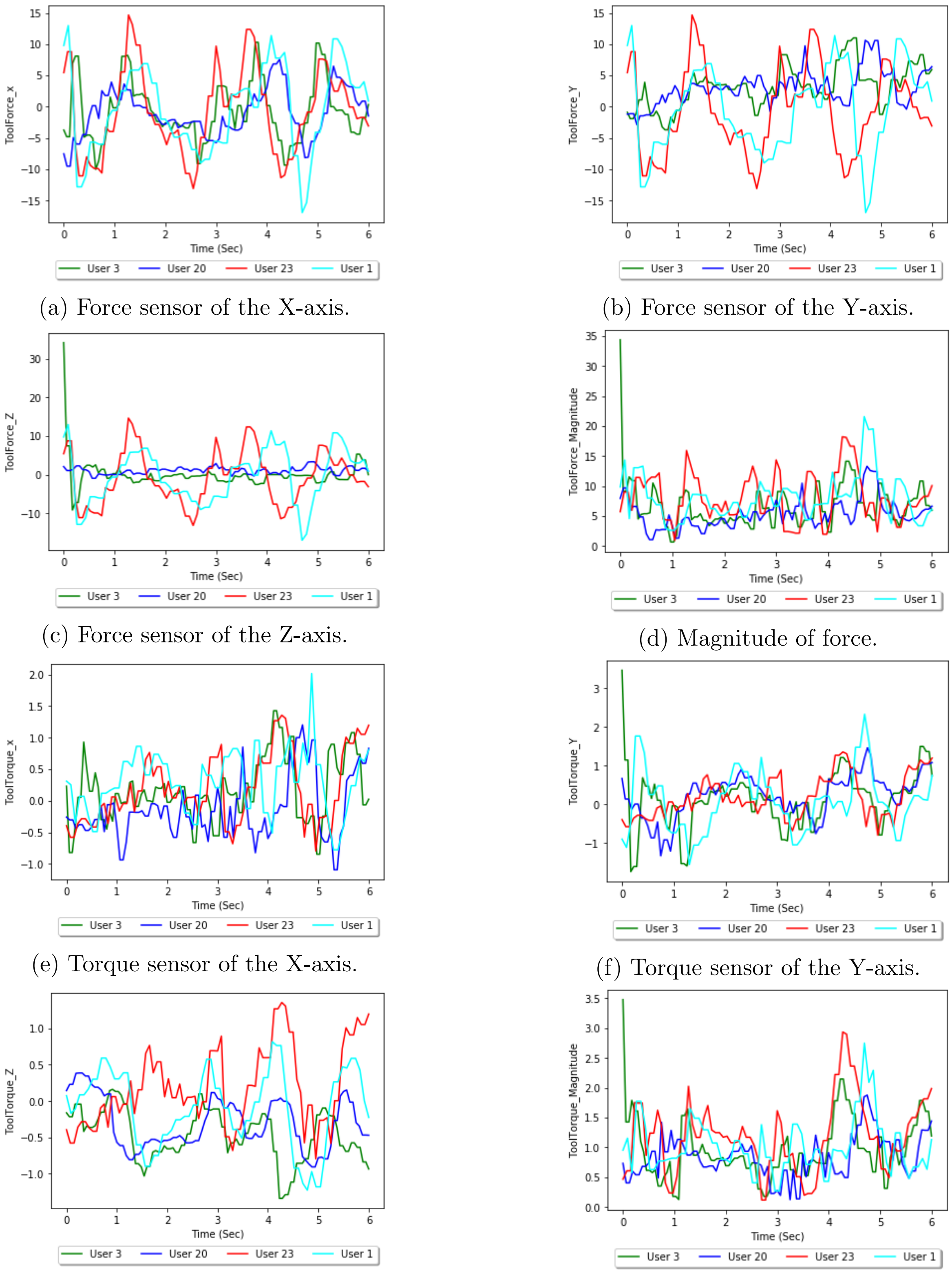
After data recording, the next step was to extract relevant features from the stream sensor data. We sampled the components of the force and torque applied to the end-effector along the X, Y and Z axes together with their overall magnitudes. (Magnitudes can, of course, be derived from the components.) Figure 3.3 shows how these vary across example runs by four users. We used the first four statistical moment features: mean, standard deviation (SD), skewness and kurtosis. Table 3.1 demonstrates the mathematical formulas for determining these statistical characteristics. The feature extraction process yielded a total of $32 = 2(force\_or\_torque) \times 4(component\_measurements) \times 4(moment\_measures)$ features. To this, we added a task number and time (the time period to complete the task), thus increasing the number of features to 34.

Table 3.1: Equations of the statistical moments used as features, where X_i is the sample of a data stream, and N is the total number of samples.

Features	Equation	Features	Equation
Mean	$\mu = \frac{\sum_{i=1}^{N} X_i}{N}$	SD	$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(X_i-\mu)^2}{N}}$
Skewness	$S = \frac{\frac{1}{N}\sum_{i=1}^{N}(X_i-\mu)^3}{\sigma^3}$	Kurtosis	$K = \frac{\frac{1}{N}\sum_{i=1}^{N}(X_i-\mu)^4}{\sigma^4}$

We selected the most appropriate features to reduce training time and improve the machine learning algorithm's performance. We used a technique that selected features depending on how they affect the performance of a given model. Recursive Feature Elimination (RFE) is one such technique provided by scikit-learn. The RFE method is a powerful algorithm [216] that provides an effective method for defining important features before they are introduced into a machine learning algorithm [40]. Due to its adaptability and simplicity of implementation, it is one of the most common feature selection algorithms. The technique may be applied to any model, and it generates an optimal set of performance-enhancing features.

RFE can be a useful and cost-effective strategy for reducing model complexity by discarding features that contribute nothing or little to the classification task. Consequently, feature selection based on feature relevance prior to creating the final RF model can be extremely beneficial for enhancing the prediction accuracy [77]. The reduced model complexity can also lead to faster classifications at run-time. The purpose of RFE is to



(a) Force sensor of the X-axis.

(b) Force sensor of the Y-axis.

(c) Force sensor of the Z-axis.

(d) Magnitude of force.

(e) Torque sensor of the X-axis.

(f) Torque sensor of the Y-axis.

(g) Torque sensor of the Z-axis.

(h) Magnitude of torque.

Figure 3.3: Comparison of the force and torque data of four users while performing a task. Task duration has been normalised to $6s$.

eliminate features by searching over fewer and smaller groups of features in a recursive manner. Initially, the estimator is trained on a limited set of features, with each feature's significance indicated by an attribute. The least significant characteristics are then deleted from the current collection. On the reduced set, this process is repeated until the desired number of features is obtained. We applied RFE using a random forest (RF) classifier.

In our experiment, we analysed and evaluated our feature set using the recursive feature elimination (RFE) selection approach. We used the top 19 features of the 34 features that make up the full set.

Considered Classifiers

Our approach uses the multi-class classification approach. Each user is profiled as the authorised user, and the remaining users are profiled as unauthorised users for validation objectives.

We implemented the RF, SVM and KNN classifiers. We trained these classifiers on the full set of extracted features with three training–test splits (75%–25%, 70%–30% and 65%–35% of the dataset) using the *train_ test_ split()* method (from the *scikit-learn* library.) We also applied the standard split method that uses the first part of the data as the training set and the remaining samples as the test set. This is called hold-out validation. In our experiments, we used the first nine tasks of each user as the training set and the remaining six tasks as the test set.

We also conducted 5-fold cross-validation. The term 'cross-validation' refers to a method of creating training and validation sets. There are several cross-validation techniques. Cross-validation with k-folds is the most commonly used method. In k-folds cross-validation, the training dataset is partitioned into k folds [23]. Each of the k folds is alternately used as the hold-out testing set; a classifier is trained on the remaining $k-1$. The overall performance is defined as the average of all k folds. Typically, the number of folds is dictated by the number of samples in the target dataset. We used 5-fold cross-validation, which means that 20% of the dataset is used for testing. We typically found this more accurate than using 10% of the data when using 10-fold validation.

3.3.3 Evaluation Using Hold-Out Validation: Results and Discussion

In the whole-task experiments, each of the 30 users performed 15 task runs, resulting in $450 = 30 \times 15$ profiles. In the multiple-segment authentication experiment, each task had three segments, thus resulting in $1350 = 30 \times 15 \times 3$ profiles.

Performance Evaluation of the Single-Use Biometric Authentication System

We first evaluated whether the user of a single witnessed task (or sub-task) could be identified. We had multiple task templates from each user and could use them to train a classifier. We could then identify how additional templates from the set (not used in training) are classified. The results are reported on the basis of FAR, TAR, EER and f1 score.

Table 3.2 presents a summary of the classifiers' results for each training regime. Table 3.2 investigates four representative metrics to evaluate the performance of single task authentication: the TAR, FAR, EER and f1 score.

According to the Table 3.2, RF performed better than SVM and KNN under all training regimes. When we used 6 tasks as a test set, RF's EER of 0.37% was the lowest and F1-score was the highest at 93.94%.

With an F1-score of 82.66%, the best performance for the SVM classifier was obtained when we employed 25% of the dataset as a training set. Similar to SVM, the KNN classifier performed best when 25% of the dataset was used as a training set, with a f1-score of 73.92%.

Consequently, we chose RF as the classifier with a training–test split of (9–6 tasks) for our subsequent experiments. The scikit-learn Python package [154] was used for training and evaluation.

To find the optimal hyper-parameters, we used a random search method for hyper-parameter optimisation [22]. For the RF classifier, for parameter $n\_estimators$, we searched through 200–2000; for max_depth, we searched through 10–110; for $min\_samples\_split$, we searched over 2-10; and for $min\_samples\_leaf$, we searched over 1-4. The parameter selections for RF for which we report results in this experiment are listed below.

- $n\_estimators = 1400$ (i.e. number of trees)
- $max\_depth = 100$ (i.e. maximum depth of the tree)
- $min\_samples\_split = 2$ (i.e. minimum sample number needed for separating at an internal node)
- $min\_sample\_leaf = 1$ (i.e. number of samples needed to be at a leaf node)

Table 3.2: Results of different classifiers with different training–test splits

Classifier	Metric	Test set 25%	Test set 30%	Test set 35%	Test set 6 tasks
RF	TAR	89.38%	88.15%	85.44%	**94.44%**
	FAR	0.37%	0.41%	0.50%	**0.19%**
	EER	0.71%	0.79%	0.97%	**0.37%**
	f1 score	89.44%	87.94%	85.48%	**93.94%**
SVM	TAR	82.3%	78.52 %	74.05%	50.56%
	FAR	0.61%	0.74%	0.89%	1.7%
	EER	1.18%	1.43%	1.73%	3.3%
	f1 score	82.66%	79.32%	74.67%	49.46%
KNN	TAR	75.22%	71.11%	67.72%	43.89%
	FAR	0.85%	1.00%	1.11%	1.93%
	EER	1.65%	1.93%	2.15%	3.74%
	f1 score	73.92%	70.09%	66.53%	40.72%

Table 3.3: Evaluation of the RF classifier on full sets of features and a subset of features over each experiment, with a training–test split of (9–6 tasks).

Experiment	No.Features	FAR	TAR	EER	f1 score
whole-task	34	0.19%	94.44%	0.37%	93.94%
authentication	19	0.13%	96.11%	0.26%	95.94%
multiple-segment	34	0.45%	86.85%	0.88%	86.35%
authentication	19	0.43%	87.41%	0.84%	87.05%

Table 3.3 shows the performance of the RF classifier on RFE-based feature subsets over two experiments.

In both experiments, we can see that limiting the number of features improves the performance of a classifier. As seen in the table 3.3, when the number of features was reduced from 34 to 19 in the whole-task authentication experiment, the EER decreased from 0.37% to 0.26%. Similarly, in the multiple-segment authentication experiment, the EER decreased from 0.88% to 0.84% when the number of features was reduced from 34 to 19. On the subset of 19 features, whole-task authentication performed better than multiple-segment authentication, as shown in Table 3.3.

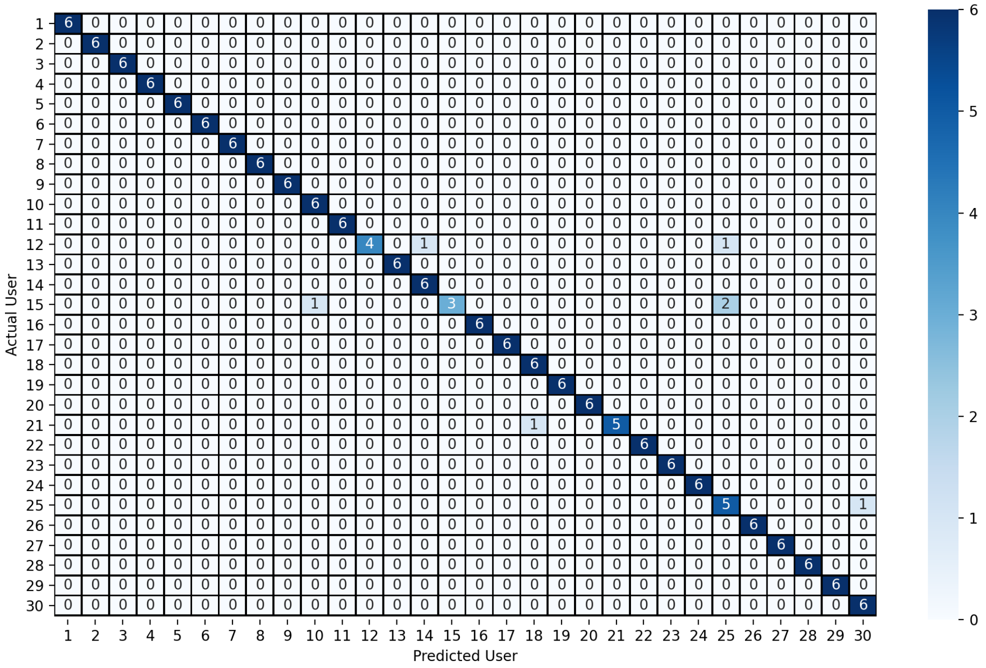
The corresponding confusion matrix for all 30 subjects is shown as a heat map. The heat map shows how tasks from the test set are classified. The corresponding RF was developed with a (9–6 tasks) training–test split, so the heat map (see Figure 3.4) of the whole-task authentication experiment shows the results for classifying $180 = 30 \times 6$ test task templates. The heat map (see Figure 3.5) of the multiple-segment authentication experiment shows the results for classifying $540 = 30 \times 18$ test sub-task templates.

Performance Evaluation of the Continuous Biometric Authentication (CBA) System

To evaluate CA, we used the average number of genuine actions (ANGA) and the average number of imposter actions (ANIA) [32], with high values of ANGA and low values of ANIA representing the best results.

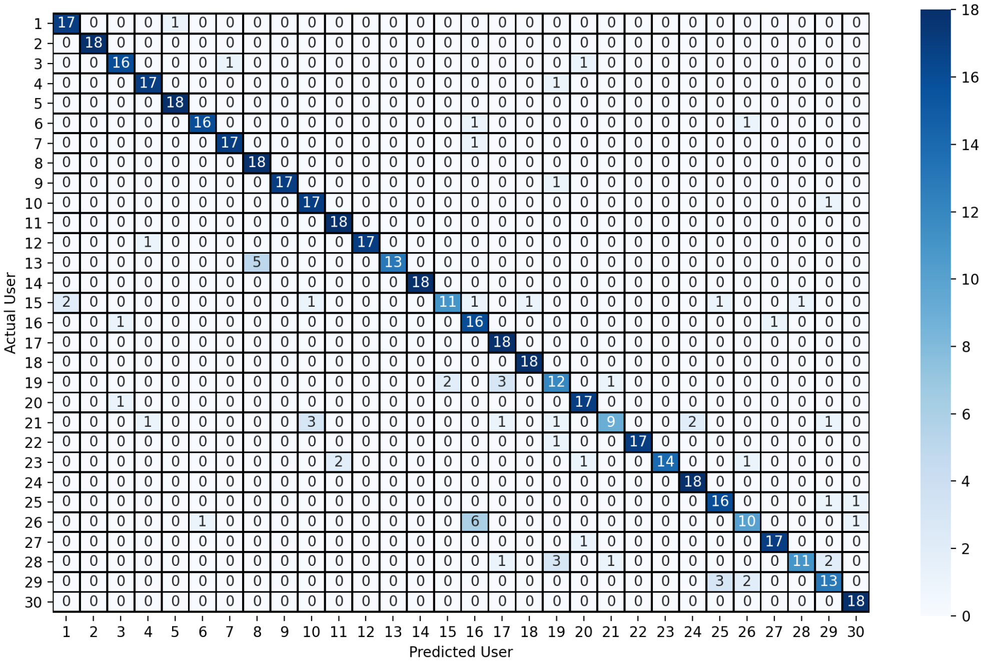
In the whole-task authentication experiment, we tested 30 users (*each user is profiled as genuine, and the remaining ones are profiled as imposters*). This yielded an ANIA of 1, meaning that all the imposters managed only one task out of six before being identified as imposters. We also obtained an ANGA score of 5.23 when we tested 30 genuine users for six tasks.

However, we obtained an ANIA of 2 in the multiple-segment authentication experiments, meaning that all the imposters managed only two sub-tasks out of 18 before being identified. The ANGA score for the multiple-segment authentication experiment was 12.17 when we tested 30 genuine users on 18 sub-tasks.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	4	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	1	0	0	0	0	3	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	5	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	1
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6

Figure 3.4: Confusion matrix for all 30 subjects in a whole-task authentication experiment, with a training–test split of (9–6 tasks)



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	17	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	16	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
4	0	0	0	17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	16	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0
7	0	0	0	0	0	0	17	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	17	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
11	0	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	1	0	0	0	0	0	0	0	17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	5	0	0	0	0	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	2	0	0	0	0	0	0	0	0	1	0	0	0	0	11	1	0	1	0	0	0	0	0	0	1	0	0	1	0	0
16	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	16	0	0	0	0	0	0	0	0	0	0	1	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	3	0	12	0	1	0	0	0	0	0	0	0	0	0
20	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	17	0	0	0	0	0	0	0	0	0	0
21	0	0	0	1	0	0	0	0	0	3	0	0	0	0	0	0	1	0	1	0	9	0	0	2	0	0	0	0	1	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	17	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	1	0	0	14	0	0	1	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	0	0	0	1	1
26	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	10	0	0	0	1
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	17	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3	0	1	0	0	0	0	0	0	11	2	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	2	0	0	13	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18

Figure 3.5: Confusion matrix for all 30 subjects in a multiple-segment authentication experiment, with a training–test split of (9–6 tasks)

3.3.4 Evaluation Using K-fold Cross-Validation: Results and Discussion

We used 5-fold cross-validation on the features vector to monitor the effectiveness of the proposed approach. The classifier results using 5-fold cross-validation are summarised in Table 3.4. As with hold-out validation, we found that RF gave the highest f1 score and the lowest EER. The parameter selections for RF for which we report the results in this experiment are as follows: $n\_estimators = 1400$, $max\_depth = 100$, $min\_samples\_split = 2$ and $min\_sample\_leaf = 1$.

Table 3.4: Results of different classifiers using 5-fold cross-validation.

Classifier	Metric	Average
RF	TAR	**91.99%**
	FAR	**0.27%**
	EER	**0.53%**
	f1 score	**91.77%**
SVM	TAR	35.78%
	FAR	2.21%
	EER	4.28%
	f1 score	40.22%
KNN	TAR	43.55%
	FAR	1.94%
	EER	3.76%
	f1 score	45.44%

Table 3.5 shows the performance of the RF classifier on RFE-based feature subsets over two experiments. According to Table 3.5, RF had the best f1 score of 93.80% in the experiment on whole-task authentication. When we compare the 5-fold cross-validation findings to the hold-out validation results, we notice that they are quite close.

Table 3.5: Evaluation of the RF classifier on full sets of features and a subset of features over each experiment using 5-fold cross-validation

Experiment	No.Features	FAR	TAR	EER	f1 score
whole-task	34	0.27%	91.99%	0.53%	91.77%
authentication	19	0.20%	94.00%	0.38%	93.80%
multiple-segment	34	0.36%	89.46%	0.70%	89.61%
authentication	19	0.34%	90.71%	0.62%	90.80%

In the whole-task authentication experiment, we tested 30 users (each user is profiled as *genuine* and the remaining users as *imposters*) using 80% trust score threshold. This yields an average of ANIA of 0.033 (out of three tasks). We also obtained an ANGA of 2.74 (out of three tasks) when we tested 30 genuine users. However, we obtained an average of ANIA of 1.73 (out of nine sub-tasks) in the multiple-segment authentication experiments using 80% threshold, meaning that all the imposters managed only 19.22% of sub-tasks before being identified. The ANGA for the multiple-segment authentication experiment was 7.26 (out of nine sub-tasks) when we tested 30 genuine users.

3.4 Proposed User to Collaborative Robot Authentication Using Time Series Feature Extraction Library (TSFEL)

3.4.1 Experimental Methodology

This experiment was carried out to determine whether the type of extracted features had an impact on the experimental outcomes. In other words, would it be possible to obtain better outcomes if feature types other than statistical ones were implemented?

To conduct this experiment, we used the same dataset that was described previously in Section 3.3.2. Similar to our previous experiment 3.3, we sampled the components of the force and torque applied to the end-effector along the X, Y and Z axes together with their overall magnitudes. However, we used a different method for feature extraction and multiple-segment authentication (see Figure 3.6). We did not use the trust model in this experiment (the decision relies on the classifier instead of the trust model.)

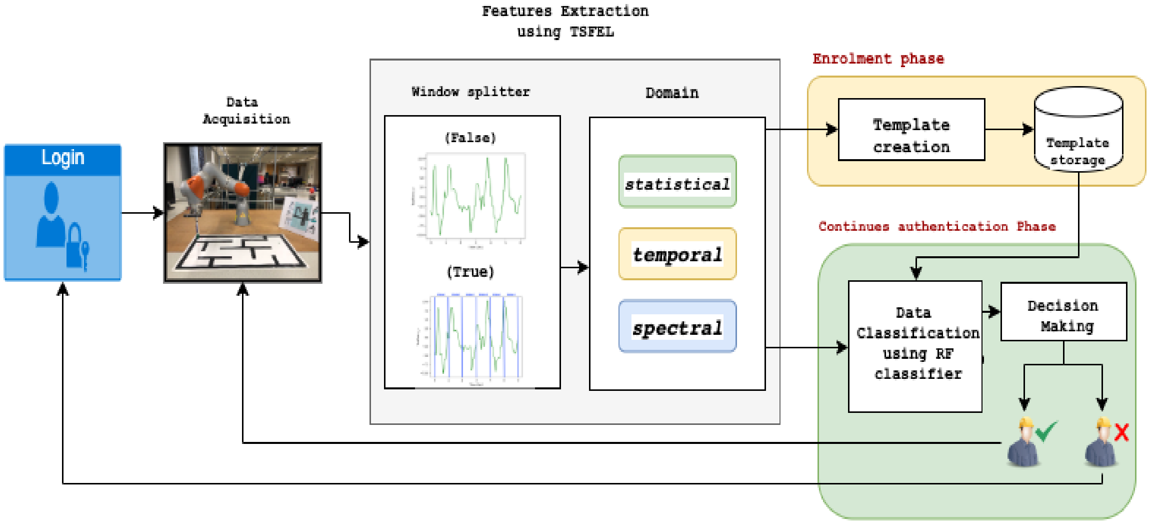


Figure 3.6: Continuous biometric authentication block diagram using TSFEL.

Feature Extraction and Feature Selection

In this experiment, we used the Time Series Feature Extraction Library (TSFEL) [19] (see Fig.3.6), a Python package for feature extraction on time series data. TSFEL allows for experimental feature extraction tasks on time series to be performed with minimal programming effort. It aims to facilitate exploratory data analysis and feature extraction on time series while considering processing costs [19]. TSFEL computes over 60 distinct features, which are classified into three types based on the domain in which they are measured:

temporal, statistical and spectral. Table.3.6 shows the listing of the available features in TSFEL.

The TSFEL processing pipeline is illustrated in Figure. 3.7. Initially, the time series are provided as inputs for the primary TSFEL extraction method as either arrays that have been loaded into memory or as files. Then, a series of pre-processing tasks are executed to ensure signal quality and synchronisation of time series, and to ensure that window computation is performed appropriately. Following feature extraction, the output is saved using a common schema so that it can be processed by the majority of data mining and classification platforms. Rows in the schema are indexed windows and the extracted features are stored in the appropriate columns

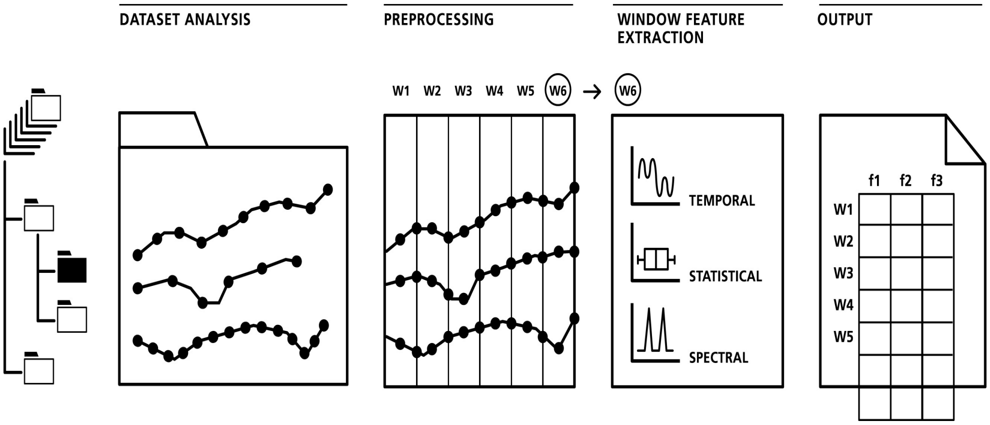


Figure 3.7: The pipeline for TSFEL processing (from [19] with permission).

Before starting the feature extraction process, this library allows us to choose the method for splitting the time series by using the parameter ‘window_splitter’. If the value of the parameter window_splitter is *true*, the time series will be split into equally sized periods or *windows* , and then the features will be extracted from each window. However, if the parameter’s value is *false* in this case, the time series will not be split, and the features will be extracted for the entire time series as one window.

On this basis, we conducted two experiments: whole-task and multiple-segment authentication. In whole-task authentication, the time series will not be split, and the features will be extracted for the entire time series as one window. In multiple-segment authentication, TSFEL will split the time series into equally sized periods or *windows*, and then the features will be extracted from each window. In this work, the time series of each task is sampled at 10 Hz, divided into windows containing 25 samples (i.e. 25 samples = 2.5 s).

After extracting features with TSFEL, we found that the dimensions of the feature vectors were extremely large. The analysis of high-dimensional data is a problem for academics in the domains of machine learning techniques [36]. Feature selection can save computation time, enhance learning accuracy and help comprehend the learning method or data by reducing unnecessary and redundant data [36].

To solve this issue, we eliminate the low-variance features (features containing less information) using the variance threshold feature selection method (from the *scikit-learn* library.) The variance threshold is a basic feature selection method. It eliminates any feature whose variance falls below a specified threshold. By default, it eliminates all zero-variance features — those that have the same value across all samples [154].

In addition, we remove strongly linked features (using the *correlated_features* method from the *TEFEL* library) to reduce computational costs.

Table 3.6: List of Available Features in TSFEL [19]

Statistical Domain	Temporal Domain	Spectral Domain
ECDF	Absolute energy	FFT mean coefficient
ECDF slope	Area under the curve	Fundamental frequency
ECDF Percentile	Autocorrelation	Human range energy
ECDF Percentile count	Centroid	LPCC
Interquartile range	Entropy	MFCC
Kurtosis	Mean absolute diff	Max power spectrum
Max	Mean diff	Maximum frequency
Mean	Median absolute diff	Median frequency
Mean absolute deviation	Median diff	Power bandwidth
Median	Negative turning points	Spectral centroid
Median absolute deviation	Peak-to-peak distance	Spectral decrease
Min	Positive turning points	Spectral distance
Root mean square	Signal distance	Spectral entropy
Skewness	Slope	Spectral kurtosis
Standard deviation	Sum absolute diff	Spectral spread
Variance	Total energy	Spectral variation
Histogram	Zero crossing rate	Spectral maximum peaks
	Neighbourhood peaks	Spectral skewness
		Spectral slope
		Spectral roll-off
		Spectral roll-on
		Wavelet absolute mean
		Wavelet standard deviation
		Wavelet variance
		Wavelet Entropy
		Wavelet Energy

ECDF: Empirical Cumulative Distribution Function, FFT: Fast Fourier Transform,
LPCC: Linear Prediction Cepstral Coefficients, MFCC: Mel Frequency Cepstral Coefficients.

3.4.2 Results and Discussion

We utilised RF as a classifier to evaluate our multi-class authentication system (see Appendix A for more results using different classifiers). Machine learning is performed using the scikit-learn Python package.

Table 3.7a and Table 3.8a show the results of using 5-fold cross-validation with the statistical features in experiments applying whole-task and multiple-segment authentication. In whole-task authentication, the mean of EER was 0.47%, whereas that in multiple-segment authentication was 1.36%.

Table 3.7b and Table 3.8b show the results using the temporal features in experiments with whole-task and multiple-segment authentication. In whole-task authentication, the mean of EER was 0.91%, whereas that in multiple-segment authentication was 1.67%. Table 3.7c and Table 3.8c display the results of the spectral features in experiments with whole-task and multiple-segment authentication. In whole-task authentication, the mean of EER was 2.91%, whereas that in multiple-segment authentication was 1.53%. Additionally, as we can see in Table 3.7d and Table 3.8d, we evaluated the possibility of using all features (statistical, temporal and spectral) and found that the mean of EER for whole-task authentication was 3.08%. The mean of EER for multiple-segment authentication was 1.27%.

The previously presented results show that the use of statistical features gave the best results with the lowest EER (0.47%) in whole-task authentication. By contrast, we find that using all features in multiple-segment authentication gave the best EER (1.27%).

Table 3.7: Evaluation matrix using the RF classifier in whole-task authentication.

(a) Statistical features

Fold	f1 score	TAR	FAR	EER
1	94.38%	94.44%	0.19%	0.37%
2	97.77%	97.78%	0.07%	0.15%
3	92.01%	92.22%	0.26%	0.51%
4	90.69%	91.11%	0.31%	0.59%
5	88.87%	88.76%	0.38%	0.74%
Mean	92.74%	92.86%	0.24%	0.47 %

(b) Temporal features

Fold	f1 score	TAR	FAR	EER
1	82.37%	83.33%	0.57%	1.10%
2	90.71%	91.11%	0.31%	0.59%
3	90.74%	91.11%	0.31%	0.59%
4	86.47%	86.66%	0.45%	0.88%
5	78.03%	78.88%	0.72%	1.40%
Mean	85.66%	86.22%	0.47%	0.91%

(c) Spectral features

Fold	f1 score	TAR	FAR	EER
1	56.56%	56.66%	1.49%	2.88%
2	50.60%	51.11%	1.68%	3.25%
3	55.99%	56.66%	1.49%	2.88%
4	63.74%	64.44%	1.23%	2.37%
5	51.41%	52.22%	1.64%	3.18%
Mean	55.66%	56.22%	1.51%	2.91%

(d) All features

Fold	f1 score	TAR	FAR	EER
1	54.28%	54.44%	1.57%	3.04%
2	46.96%	47,78%	1.80%	3.48%
3	57.75%	55.56%	1.53%	2.96%
4	61.44%	62.22%	1.30%	2.52%
5	50.04%	48.89%	1.76%	3.41%
Mean	54.09%	53.78%	1.59%	3.08%

3.5 Limitations

This study has several limitations. First, COVID-19-related lockdowns and social distancing restrictions necessitated significant adjustments to the experimental methodologies. Initially, the examination was intended to assess the system against zero-effort and non-Zero-effort attacks, such as shoulder surfing. However, the system was evaluated exclusively using

Table 3.8: Evaluation matrix using the RF classifier in multiple-segment authentication.

(a) Statistical features

Fold	f1 score	TAR	FAR	EER
1	75.95%	76.37%	0.81%	1.57%
2	79.03%	80.23%	0.68%	1.32%
3	82.96%	83.42%	0.57%	1.12%
4	78.80%	79.01%	0.72%	1.39%
5	78.48%	79.01%	0.72%	1.39%
Mean	79.05%	79.61%	0.70%	1.36%

(b) Temporal features

Fold	f1 score	TAR	FAR	EER
1	69.62%	71.42%	0.98%	1.90%
2	71.99%	72.52%	0.95%	1.83%
3	74.78%	75.69%	0.83%	1.62%
4	74.21%	75.13%	0.85%	1.66%
5	79.58%	80.11%	0.69%	1.33%
Mean	74.04%	74.97%	0.86%	1.67%

(c) Spectral features

Fold	f1 score	TAR	FAR	EER
1	74.73%	75.82%	0.83%	1.61 %
2	77.82%	78.57%	0.74%	1.43 %
3	74.70%	75.14%	0.86%	1.66%
4	75.97%	76.79%	0.80%	1.55%
5	78.14%	79.01%	0.72%	1.39%
Mean	76.27%	77.07%	0.79%	1.53%

(d) All features

Fold	f1 score	TAR	FAR	EER
1	78.29%	79.12%	0.72%	1.39%
2	81.97%	82.32%	0.61%	1.18%
3	79.83%	80.11%	0.69%	1.33%
4	81.53%	80.66%	0.67%	1.29%
5	81.51%	82.32%	0.61%	1.18%
Mean	80.63%	80.91%	0.68%	1.27%

scenarios of zero-effort attacks.

Second, the experiment does not evaluate the system's effectiveness when the participant is interrupted while performing the tasks (e.g. talking to another person). Third, the approach is beneficial when humans and robots interact directly, but it is ineffective when they do not collaborate directly (cell, coexistence, synchronised and cooperation).

3.6 Summary

In this chapter, we proposed a novel continuous, behavioural–biometric authentication system for a collaborative robot by using internal robot sensor data to authenticate users who engage physically with the collaborative robot. This method increases security over existing systems while avoiding additional worker processes and potentially intrusive monitoring. Additionally, TSFEL was used to assess the effects of the types of extracted features on the experiment outcomes. In whole-task authentication, we found that using statistical features produced the best results with the lowest EER. Using all features in multiple-segment authentication, on the other hand, yielded the best result, with the lowest EER.

Chapter 4

User Authentication in a Wearable Sensor System

4.1 Introduction

In our research, we are interested in the area of human–robot collaboration, in which the close interaction between humans and robots present particular challenges relating to personal safety and security [79][164] [107]. In this regard, exoskeletons present one of the most interesting challenges [201][82], with close, physical interaction required throughout the duration of use. Such frameworks are an emerging technology with primary applications in healthcare and industry, particularly in logistics in which they are being deployed to reduce health complaints related to activities such as heavy lifting [148]. While the exoskeleton market is currently relatively small (USD 499 million in 2021), it is expected to grow rapidly to an estimated USD 3,340 million in 2026) [65].

In this chapter, we examine the implementation of behavioural biometric CA using wearable sensors, as would be found in an exoskeleton. Because of restrictions in access to physical equipment and facilities arising from COVID-19 during the course of our research, we demonstrate our methods on a public dataset recorded specifically for industrial collaborative robotic applications [136]. Specifically, we use data recorded from a WiFi-enabled sensorised glove, which is used to monitor a user's hand movements. We use a subset of the larger public dataset, which focuses on six manufacturing actions (e.g. screwing and carrying operations). As such, it is an example of direct interaction in physical tasks; the operator wearing the glove is actually carrying out the manual actions. However, the glove also serves as a proxy for a wearable exoskeleton that could collect such data from a user during normal operation (e.g. as part of an exoskeletal flight suit for drone piloting [168]).

In chapter 3, we explored CA approaches applied to the use of collaborative robot manipulators. Biometric data were provided by the robot arm's joint information (i.e. position, force and torque) during direct physical manipulation by the human co-worker (a mode termed *collaboration* [20]). What both elements of our user-to-robot authentication work have in common is that *they require no data to make authentication decisions over and above* *those generated through normal operational activity.* Here, we use the sensor data provided by an e-glove (originally collected for industrial collaborative robotics research purposes) as the basis of our continuous biometric system. The data arise from performance of the task; we simply choose to leverage them for security purposes. A consequence of adopting a *data already sensed* approach is that it is also frictionless from an end-user viewpoint, as users are not required to make any specific effort other than perform their routine job tasks. Security implementation (CA in this study) is a purely analytic task; data collection comes for free.

4.2 Threat Model

To test our authentication system, we assume that an attacker has access to the physical operating environment and interface device. We focus on two main forms of attack that the attacker could perform:

1. **Zero-effort attacks:** As we mentioned in Chapter 3, zero-effort attacks are common mechanisms for determining the accurate design and durability of biometric authentication schemes.

2. **Statistical attacks:** In this type of attack, a skilled attacker (either a human or a robot) can be a powerful threat [2][186]. Synthetic data are derived using simple concepts from a selected group. The concept behind this attack is to bypass the authentication scheme using a random combination of the most common features of the population. For example, in [179], they utilised a robotic finger to conduct physical authentication attacks on touch-based biometric devices by using population statistics of touch activity on smartphones. They found that the system's equal error rate (EER) increased as a consequence of their attack.

4.3 Proposed Methods

Our proposed system profiles a user's working behaviour with a WiFi-ed sensorised glove to provide continuous user authentication (see Figure 4.1).

The glove measures and reports the wearer's finger pressure data (refer to Section 4.3.1). Subsequently, the data are cleaned to remove noise, as described in 4.3.1. Statistical features, as illustrated in Section 4.3.1, are extracted from each data stream to create a profile template for each user. These reference templates are based on multiple task repetitions. Each time a user begins performing a task, our authentication method compares the user's current (dynamic) behavioural profile template against all reference profile templates in the database to obtain a probability value of it being a specific user. The highest probable value is used to identify the individual in a decision-making phase.

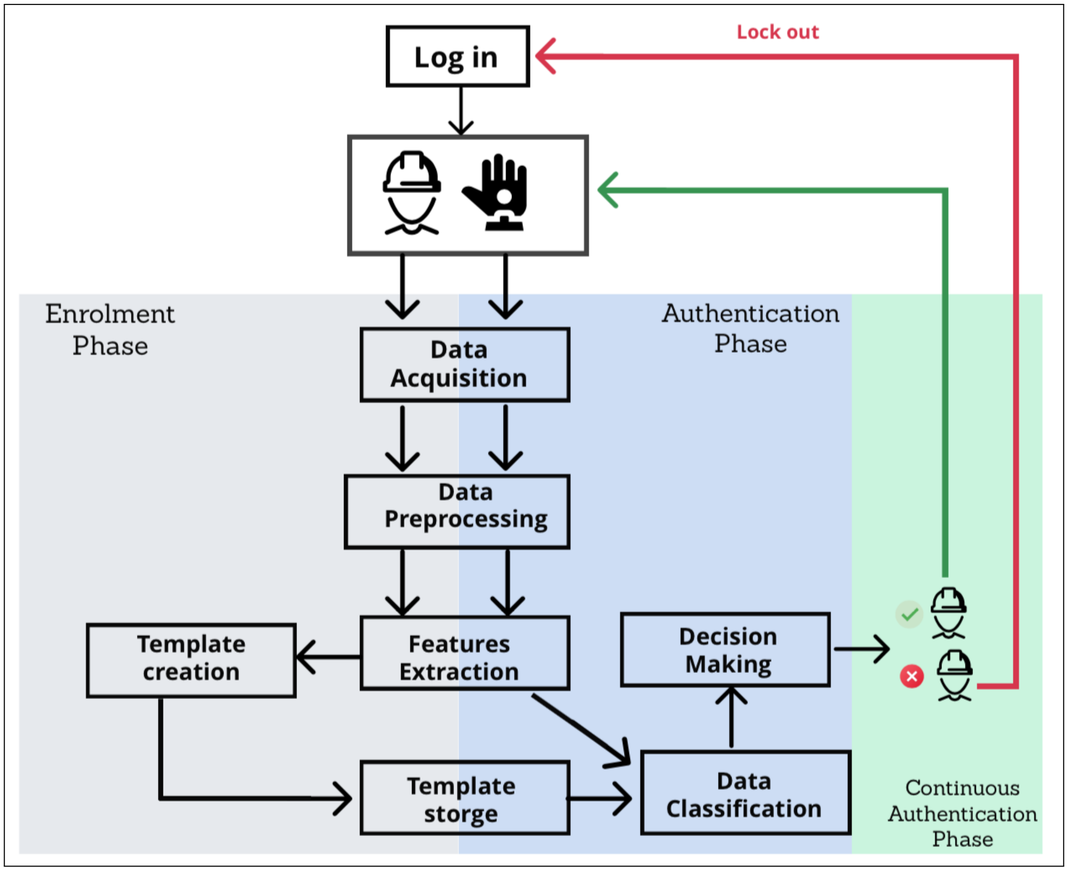


Figure 4.1: The classification process for continuous user authentication

4.3.1 Experimental Methodology

Dataset

Our work used a public dataset specifically created for classifying human motion in industrial settings and for developing collaborative robotic applications [136]. The data contain samples of six industry-oriented activities inspired by a car manufacturing use case (see Figure 4.2). These activities are described below [136]:

- Screw high: move to the shelf and screw at a height of 175 cm
- Screw middle: move to the shelf and screw at a height of 115 cm
- Screw low: move to the shelf and screw at a height of 60 cm
- Untie the knot: untie a knot on a 45 cm-high table
- Carry 5 kg: place a 5 kg weight on a 55 cm-high table, move to the shelf and place the load on a 20 cm-high shelf and

- Carry 10kg: place a 10 kg weight on a 55 cm-high table, move to the shelf and place the load on a 110 cm-high shelf)

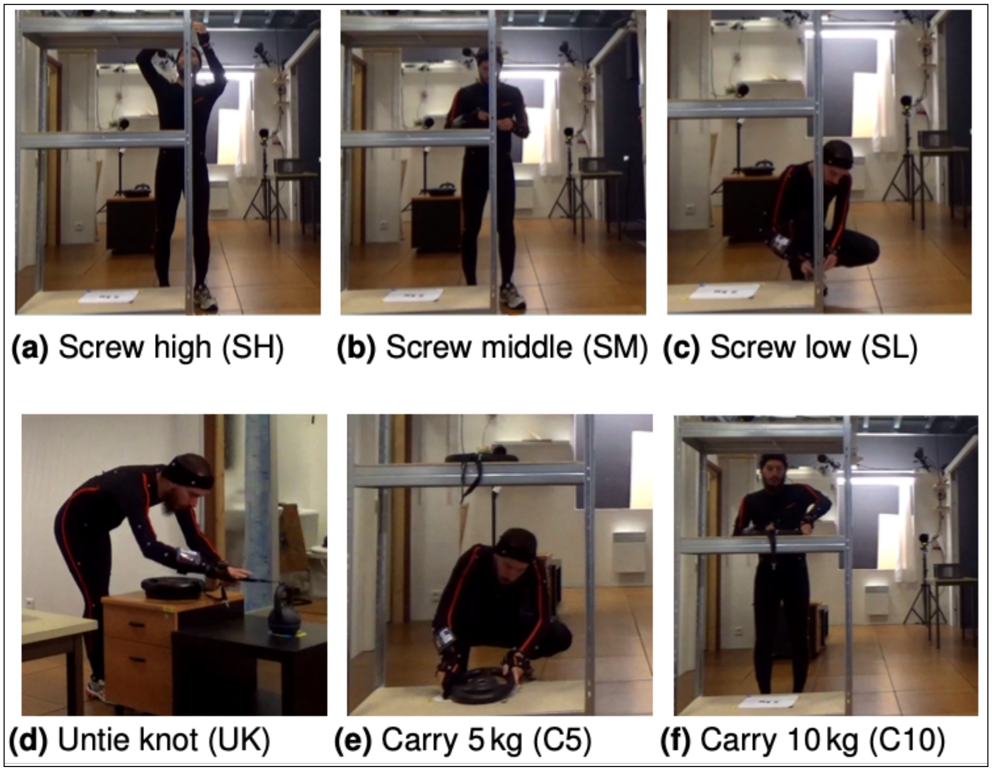


Figure 4.2: A picture of a participant performing the six actions described in the dataset (from [136] with permission.)

The dataset includes 13 participants' finger pressure force samples captured with an e-glove from Emphasis Telematics (see Figure 4.3). Each participant performed 15 trials. Each trial was around 90 s long (i.e. three different sequences of activities, with each sequence repeated five times). A single trial consisted of one of the following six predefined sequences:

1. Screw low, screw middle, screw high, untie the knot, carry 10 kg and carry 5 kg
2. Screw high, screw middle, screw low, untie the knot, carry 10 kg and carry 5 kg
3. Screw low, screw middle, untie the knot, carry 10 kg, screw high and carry 5 kg
4. Screw low, untie the knot, carry 10 kg, screw middle, carry 5 kg and screw high
5. Untie the knot, carry 10 kg, screw high, screw middle, carry 5 kg and screw low
6. Untie the knot, carry 10 kg, carry 5 kg, screw high, screw middle and screw low

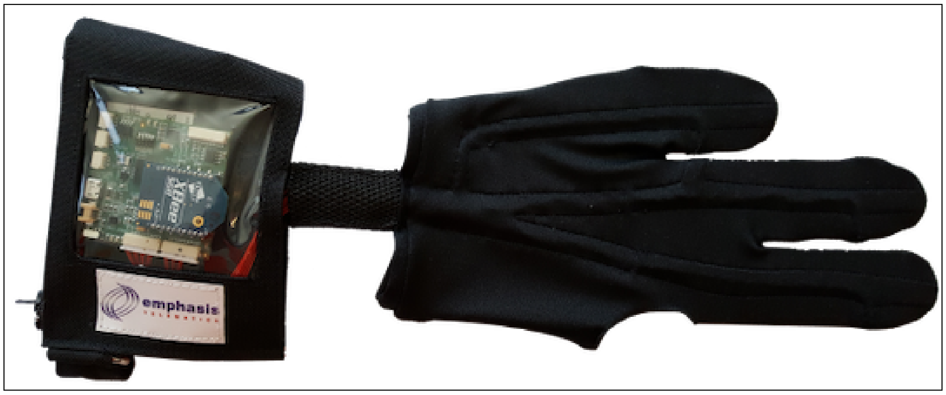


Figure 4.3: The e-glove Basic [196]

Data Pre-processing

Sensor data from commercial wearables are prone to noise data [70]. These data require a filtering or smoothing method to considerably reduce the quantity of high-frequency noise and acquire as accurate and clean data as possible. We apply the digital low-pass Butterworth filter using the *lfilter* function from the SciPy library [206] to remove high-frequency noise components without distorting the target signal [104] and obtain a smoother version of the original data.

Feature Extraction and Feature Subset Selection

The sensor data cannot be used directly by a user authentication classifier until behavioural characteristics are derived from the data. The dataset provides four pressure sensors (i.e. on the palm and the tips of the thumb, index and middle fingers) and three flexion sensor data streams (i.e. the thumb, index and middle fingers).

In this chapter, we use the TSFEL [19]. As we mentioned in Section 3.4, the TSFEL is a Python package for feature extraction on time series data. TSFEL computes over 60 distinct features across the statistical, temporal and spectral domains.

Feature selection is used to select the most appropriate features for building the classification model. To improve efficiency, we aimed to reduce the dimension of the feature vector by finding a limited set of essential features that provide good classification performance. Redundancies and noise can be eliminated after the sensor data are extracted, thus minimising the machine learning algorithm's error, time and computing complexity. To overcome the high-dimensional feature vector, we removed features with low variance (features containing less information). Additionally, we removed highly correlated features to decrease computational costs.

Considered Classifier

A variety of machine learning classification approaches can be used. Here, to evaluate our multi-class authentication system, we used RF as the classifier (see Appendix A for results using different classifiers). The scikit-learn Python package [154] was used to perform machine learning. We applied five-fold cross-validation on the features vector to monitor the effectiveness of the proposed approach. Test feature vectors are classified as legitimate or imposters.

Hyper-parametrisation

The parametric choices in machine learning algorithms may have significant effects on the results [43]. Accordingly, we experimented with a range of choices for the significant parameters of the RF classifier. We used an RS approach for hyper-parameter optimisation [22] to obtain the best combination of RF technique parameters that fit our dataset.

For the RF classifier, for parameter $n\_estimators$, we searched through 200–2000; for max_depth, we searched through 10–110; for $min\_samples\_split$, we searched over 2–10; and for $min\_samples\_leaf$, we searched over 1–4. The parameter selections for RF for which we report the results in this experiment are listed below.

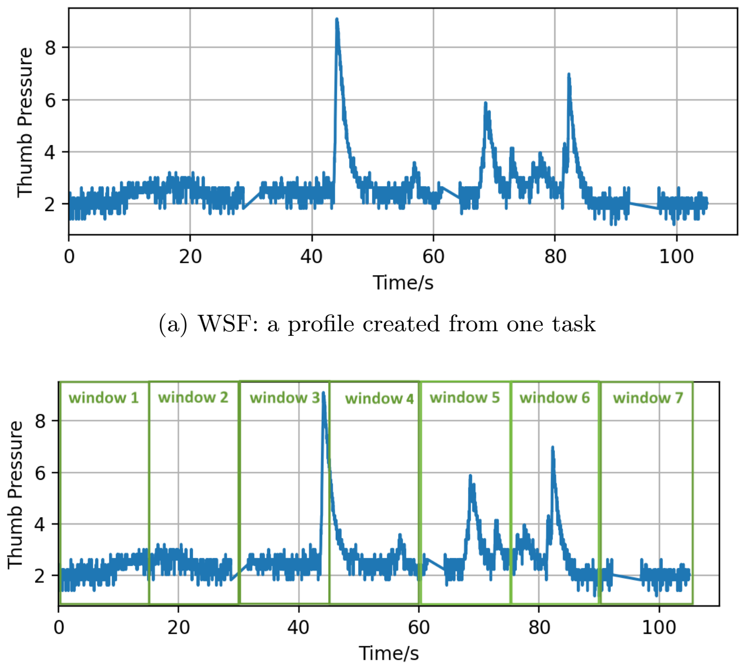
- $n\_estimators = 1000$ (i.e. number of trees)
- $max\_depth = 100$ (i.e. maximum depth of the tree)
- $min\_samples\_split = 5$ (i.e. minimum sample number needed for separating at an internal node)
- $min\_sample\_leaf = 1$ (i.e. number of samples needed to be at a leaf node)

Metrics

We investigate four representative metrics to evaluate the performance of single task authentication: the F1 score, TAR, FAR and EER. The F1 score corresponds to the equally weighted average of precision and recall. TAR represents the probability that the system matches a valid user to its stored template within the system; it is calculated according to Equation 2.1. FAR represents the number of users incorrectly deemed to be valid based on templates stored in the biometric system; it is calculated according to Equation 2.2. EER represents the position in which the valid and invalid error rates are equal. As the EER number increases, the system's performance worsens and vice versa.

To evaluate the performance of our CA scheme, we use ANGA and ANIA [33].

We also use four ratings (very good, good, bad and very bad) for the evaluation [141]. These ratings are assigned based on the rates of legitimate user lockouts and impostor user non-detection. Table 2.10 illustrates these cases. The categorisation **applies to a single user**. We apply this table to assign an appropriate rating to each of our 13 users (i.e. the performance of the authentication scheme when each user is considered the genuine user).



(a) WSF: a profile created from one task

(b) WST: multiple profiles created from one task

Figure 4.4: Example of how *window_ splitter* works in the TSFEL. User # 10's thumb pressure data are utilised.

4.4 Results and and Discussion

We know of no previous work on exoskeleton authentication. Therefore, we cannot compare like for like, and the results presented here form a benchmark for future researchers.

We conducted two experiments based on the TSFEL parameter *window_ splitter* (see Section 3.4).

1. *Window_ splitter = False (WSF)*: In this experiment, the time series in the single task is not split into windows. Rather, the features are extracted from the entire task's time-series data, and then a template is created for this task. In this case, 15 templates are created for each user (see Figure 4.4a). Each template represents a sequence of subtasks.

2. *Window_ splitter = True (WST)*: In this experiment, the time series for a single task is split into windows (see Figure 4.4b). In this case, feature extraction occurs in each window, and then a template is created for each window. Multiple templates are created for each task. The time series of each task is sampled at 50 Hz, divided into windows containing 750 samples (i.e. 750 samples = 15 s).

To evaluate the impact of window size in the WST experiment, we examined our authentication system for window sizes of 250, 500, 750 and 1,000. Table 4.1 summarises the results of using different window sizes; the F1 score increases with an increase in window size.

Table 4.1: Performance of different window sizes in the WST experiment.

window size	F1 score	EER
250	82.0%	3.0%
500	85.1%	2.3%
750	88.4%	1.8%
1000	88.6%	1.7%

4.4.1 Performance Evaluation of Zero-Effort Attacks

To test predictive efficiency, we used five-fold cross-validation, which defends against over-fitting by splitting the dataset into folds and estimating the precision of each fold. This method produces a reasonable estimate of the predictive accuracy of the final trained model with the dataset. In our five-fold case, the trial data are partitioned into five-folds. Each fold is then used to evaluate a model obtained by training on the four other folds. The average performance measures across the folds are commonly used as general measures of performance. Table 4.2 shows the results of the WSF experiment. The average F1 score using WSF is 99.4%, and the average EER is 0.08%. These results are excellent. In the WST experiment, we find that the average F1 score is 88.4% when using a window size of 750 (see Table 4.3). The average EER is 1.8%.

Table 4.2: Biometrics evaluation matrix using the RF classifier in the WSF experiment.

Fold	F1 score	TAR	FAR	EER
1	100%	100%	0.0%	0.0%
2	100%	100%	0.0%	0.0%
3	97.0%	97.4%	0.2%	0.4%
4	100%	100%	0.0%	0.0%
5	100%	100%	0.0%	0.0%
Mean	99.4%	99.5%	0.04%	0.08%

Based on the evaluation of CA using four ratings (very good, good, bad and very bad), we present the results in Tables 4.4, 4.5. As shown in Table 4.4, the best results in the WSF experiment are in folds 1, 2, 4 and 5; all participants are in the very good group, with an ANGA of 39, indicating that all genuine participants perform all the tasks without being locked out of the system. The imposters for this group of users were detected, for which the ANIA average was 0.

In fold 3, 11 participants are in the very good group, with an ANGA of 33. The remaining users fall into the good group, with an ANGA of 5 and an ANIA of 1.

Overall, in the WSF experiment, the ANGA average is 38.8 tasks (out of 39 tasks), which indicates that genuine users can perform 99.48% of the tasks. In comparison, the ANIA of

Table 4.3: Biometrics evaluation matrix using the RF classifier in the WST experiment.

fold	F1_score	TAR	FAR	EER
1	89.0%	88.7%	0.9%	1.7%
2	87.0%	86.9%	1.1%	2.0%
3	86.0%	85.8%	1.2%	2.2%
4	89.0%	89.4%	0.9%	1.6%
5	91.0%	91.1%	0.7%	1.4%
Mean	88.4%	88.38%	0.96%	1.8%

Table 4.4: Performance of CA for the RF classifier on a selected feature set using WSF.

Fold	Group	# of user	ANGA	ANIA
1	very good	13	39	0
	good	0	-	-
	bad	0	-	-
	very bad	0	-	-
2	very good	13	39	0
	good	0	-	-
	bad	0	-	-
	very bad	0	-	-
3	very good	11	33	0
	good	2	5	1
	bad	0	-	-
	very bad	0	-	-
4	very good	13	39	0
	good	0	-	-
	bad	0	-	-
	very bad	0	-	-
5	very good	13	39	0
	good	0	-	-
	bad	0	-	-
	very bad	0	-	-

the system is 0.2 task, which indicates that imposter users can perform 0.512% of the tasks before being indicated as imposters.

In the WST experiment, Table 4.5 shows that in fold 5 (best split), one participant is in the very good group, with an ANGA of 26, which indicates that the genuine participant performs all the sub-tasks without being locked out of the system. The imposters for this group of users were detected, and the ANIA average is 0. Four users fall into the good group, with an ANGA of 84. The imposters in this group were locked out after performing four of the sub-tasks, which means some imposters can perform some sub-tasks before they are detected as unauthorised users.

Overall, in the WST experiment, the genuine users can perform 251.2 tasks out of 283 tasks or 88.76% of tasks (ANGA). In comparison, the imposters users can perform only 33.8 tasks or 11.94% of the tasks (ANIA) before being indicated as imposters.

Table 4.5: Performance of CA for the RF classifier on the selected feature set using WST and a window size of 750.

Fold	Group	# of user	ANGA	ANIA
1	very good	1	26	0
	good	3	64	13
	bad	9	153	27
	very bad	-	-	-
2	very good	0	-	-
	good	2	46	3
	bad	11	199	35
	very bad	0	-	-
3	very good	0	-	-
	good	2	49	6
	bad	11	190	33
	very bad	0	-	-
4	very good	1	26	0
	good	1	19	0
	bad	11	207	30
	very bad	0	-	-
5	very good	1	26	0
	good	4	84	4
	bad	8	167	18
	very bad	0	-	-

4.4.2 Performance Evaluation of Statistical Attacks

Until this stage, the study has used the zero-effort attack model. Now we create statistical attacks based on the algorithm provided by [2] to test how our authentication system manages non-zero-effort (statistical attack) impostors, as discussed in Section 4.2. In a statistical attack scenario, we assume the intruder has access to a large number of input samples, but does not have them from the target. For example, an attacker might use the same sensor device (e-glove) to create synthetic input data. To do so, the attacker might ask a large group of people to wear e-gloves and perform the same tasks that the target user would, such as carrying weights, untying knots, and using a screwdriver. The attacker's goal is to bypass the authentication system and gain unauthorised access. The attacker's knowledge may include the following: 1. The type of wearable sensor utilised to measure the user's behavioural data. 2. The type and number of features captured by the sensor. The attacker's capability is limited to generating input samples, and providing them to the authentication system.

The principal concept in statistical attacks is generating forged samples based on the most popular feature values in the samples of a given population. To provide it, we take the following steps, which are inspired by [2]:

1. Assume there are P users, N samples per user, and that each sample has F features. In our experiments $P = 13$, $N = 15$, and $F = 7$.

2. Let U_i denote user i, $U_{i,j}$ denote sample j of user i, and $U_{i,j,f}$ denote feature f of sample

j of user i.

3. Let $COMBINED = U_{1,1}, ..., U_{1,N}, U_{2,1}, ..., U_{2,N}, ..., U_{P,1}, ..., U_{P,N}$ be the combined samples for all users.

4. Each user U_t is selected as a target (victim) user, and samples of others' data are used to produce forged data. To generate forged samples, a formal histogram is created for each feature using the combined data from the set of participants excluding the target user.

   For each target user U_t, $t = 1..P$

   - $Hist_{t,1} = histogram(< U_{i,j,1} >_{i=1..P\ (i \neq t),\ j=1..N})$
     $Hist_{t,2} = histogram(< U_{i,j,2} >_{i=1..P\ (i \neq t),\ j=1..N})$
     ...
     $Hist_{t,F} = histogram(< U_{i,j,F} >_{i=1..P\ (i \neq t),\ j=1..N})$

   - Generate the required number of forged samples for target user U_t. Each feature f in a sample is sampled from the three most highly populated bins (selecting a random number from the union of the ranges of the three bins) in the corresponding histogram $hist_{t,f}$. This can be repeated until the requested number of forged samples has been generated.

5. After generating the forged inputs, the next step is to feed these samples into the authentication system to attack the targeted user.

6. The final step is to measure the impact of the statistical attack on our authentication system.

We generate 30 forged input files for each targeted user, utilising different histogram's bins (i.e., interval numbers): 50, 150, 250, 350, and 450. Assuming the attacker has a limited amount of time to enter the forged sample, we use the three most frequent features in each bin.

To evaluate the statistical attack against our authentication system, we measure the attacker acceptance rate (AAR). The AAR is calculated, which indicates the percentage of forged samples that pass the authentication system. Unlike a zero-effort attack, for each user, we use the original data (15 templates) as a training set and the forged data (30 templates) as the test set to evaluate the authentication system.

$$\text{AAR} = \frac{\text{Successful forged samples}}{\text{All generated forged samples}} \tag{4.1}$$

Figure 4.5 shows the AAR results for several statistical attacks (parametrised by bin size). The highest AAR in the WST experiment is 6.38% using $bin = 250$. In the WSF experiment, the highest AAR is 9.54% using $bin = 50$. As can be seen from Tables 4.6 and 4.7, some individual users seem to be immune from the statistical attack, whilst others are susceptible.

Table 4.6: The acceptance rate (AR) obtained by statistical attacks for each user in the WSF experiment.

	Bin Size				
User	50	150	250	350	450
1	0.0	0.0	0.0	0.0	0.0
2	0.28	0.07	0.07	0.07	0.07
3	0.0	0.0	0.0	0.0	0.0
4	0.17	0.63	0.76	0.76	0.76
5	0.0	0.0	0.0	0.0	0.0
6	0.45	0.29	0.03	0.1	0.1
7	0.34	0.14	0.0	0.14	0.17
8	0.0	0.0	0.0	0.0	0.0
9	0.0	0.0	0.0	0.0	0.0
10	0.0	0.0	0.0	0.0	0.0
11	0.0	0.0	0.0	0.0	0.0
12	0.0	0.0	0.0	0.0	0.0
13	0.0	0.0	0.0	0.0	0.0

Table 4.7: The acceptance rate (AR) obtained by statistical attacks for each user in the WST experiment.

	Bin Size				
User	50	150	250	350	450
1	0.0	0.0	0.04	0.0	0.02
2	0.0	0.0	0.0	0.0	0.0
3	0.0	0.0	0.0	0.0	0.0
4	0.0	0.04	0.01	0.07	0.02
5	0.24	0.0	0.0	0.0	0.0
6	0.24	0.03	0.05	0.0	0.0
7	0.09	0.17	0.12	0.03	0.08
8	0.0	0.0	0.0	0.0	0.0
9	0.0	0.0	0.0	0.0	0.0
10	0.0	0.0	0.0	0.0	0.0
11	0.0	0.01	0.02	0.0	0.01
12	0.04	0.33	0.38	0.21	0.33
13	0.01	0.15	0.21	0.24	0.33

However, we also need to consider the practicalities of launching a statistical attack. The context essentially assumes either (a) wide-scale collusion (i.e., the other 12 users conspire to form a profile), (b) the biometric profile data has been otherwise obtained, or (c) a statistical profile created without direct knowledge of the authorised user base will be used. The first (a) seems highly unlikely, and the second (b) speaks to a major security breach in any case. In the third (c), the degree to which an independently created profile would have the same success is doubtful. The user base is likely small, and it is also a *skilled* user base. This would be difficult to replicate efficiently. However, the statistical attack results are undoubtedly interesting and will inform further research.

We also need to be careful about what we understand by an attack. It covers the case where one user deliberately and maliciously tries to masquerade as another user without that user's consent. Still, it also includes a user masquerading with the express approval of the target user, i.e., a colleague being 'helpful' at some time. For tasks that require physical interaction, this is a major consideration. Management will want to ensure that only appropriately trained users can access certain services.

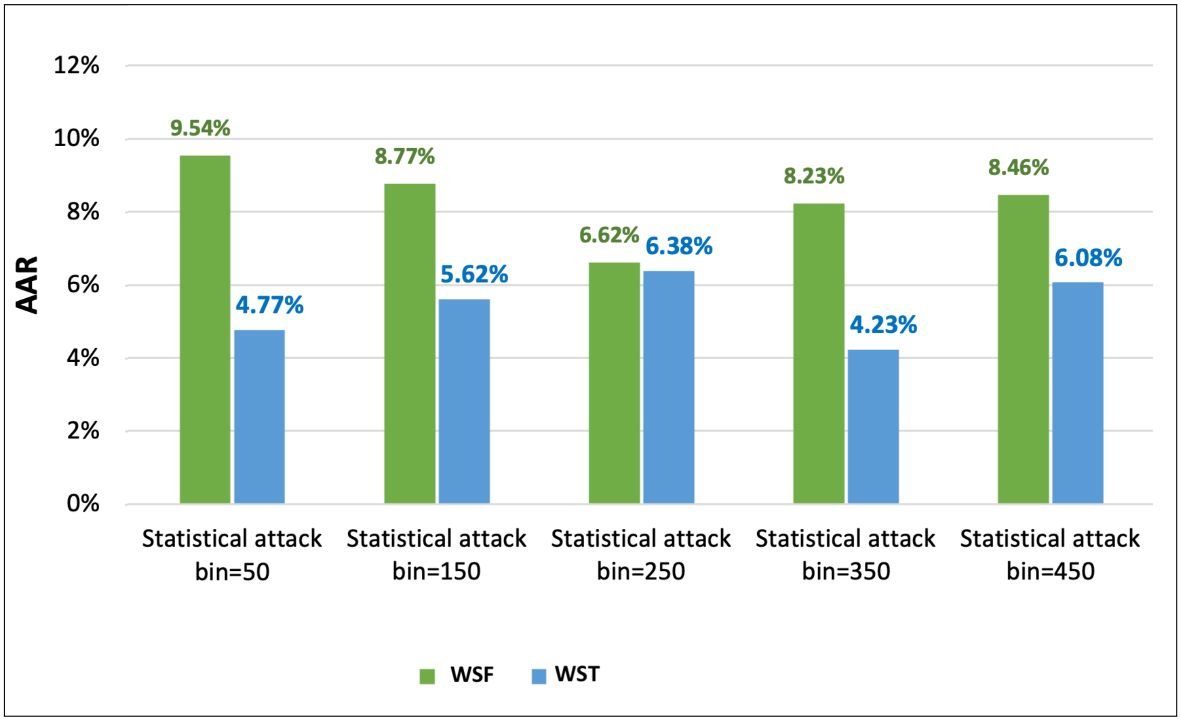


Figure 4.5: The AAR obtained by statistical attacks in both experiments (WSF and WST).

4.5 Limitations

As with many research projects at this time, COVID-19 has had a major impact on our work. While this investigation was originally planned as a physical experiment with human participants, local lockdowns and social distancing restrictions have resulted in major revisions to our experimental protocols. Specifically, we had to rely on publicly available datsets. While closely related to our target application, the dataset used here is limited in the number of recorded participants. Thus, the proposed behavioural-based biometric system's performance could not be tested over a large number of subjects. We do not see this as a major issue, though, because in a real-world application domain, the sets of users we wish to authenticate are likely similarly limited. Furthermore, the issue of known users masquerading as their colleagues to decrease downtime and increase productivity is much more of a concern than the threat from unknown external intruders; the security aim often involves ensuring that only appropriately trained people have access.

In practice, users will also be skilled users. Creating a feasible statistical profile from an external set of users would require that set to be similarly skilled. Furthermore, we have evaluated on a limited set of fairly simple tasks. The more sophisticated the tasks addressed, the greater the difficulty in synthesising a statistical profile from external users.

4.6 Summary

In this chapter, we have shown that a continuous form of authentication may be implemented using wearable sensors, such as those embedded in exoskeletons or haptic interfaces. Specifically, we demonstrate authentication through a user's sensed physical manipulations via an e-glove. Essentially, the way a user touches, squeezes and generally interacts using the glove is distinctive. Sensor traces from one user are different from those from another user or an intruder, even when the same task is performed. A machine learning technique was used to synthesise the mapping of dynamic behaviour feature vectors to users in the reference database. The mapping was obtained by training using an RF approach, and very promising CA outcomes, both in terms of rejecting imposters (i.e. low ANIA) and accepting legitimate users (i.e. high ANGA), were achieved.

Our approach has further desirable characteristics. As part of its normal operation, the e-glove provides a multi-channel stream of pressure data. These data may be collected for a variety of purposes, such as robot control, teleoperation, robot training or ergonomic measurement. Our approach shows that such data could also serve a secondary purpose, as they could form the basis for effective CA. *No additional data need to be collected.* Thus, the approach is very cheap in implementation terms.

The results for zero-effort attacks are very encouraging. Although the practicality of a statistical attack is unclear for our direct and envisaged scenarios, it still provides an interesting and conservative means of stress testing. In this chapter, authentication is interpreted, as the target user is the most likely user. The approach is based on a vector of probabilities of each user's likelihood of generating the supplied profile. A user is always identified as the most likely match. However, we might also like to consider absolute values of probabilities, e.g. in which the probability of a match must exceed some threshold (as well as being the most likely).

Chapter 5

User Authentication in Human–Robot Teleoperation Systems

5.1 Introduction

Teleoperation is the control of an object (in this example, a robot) to enable an operator to execute a task from a distance. This is frequently done in a hostile environment where human access is difficult but human intellect is required.

Robot teleoperation is a significant area of research, with applications spanning nuclear, offshore, space, and manufacturing environments, as well as those needing human-in-the-loop control for sensitive operations. Verifying the identity of operators is critical for safety and security in such systems, and techniques such as that suggested in this chapter have a substantial potential for providing continuous user authentication.

In teleoperation systems, the open and unpredictable nature of the communication channel between the operator and the robot renders it more vulnerable to attacks [28]. The use of existing technologies, such as data encryption and command signature verification, may cause delays in the operator-to-remote robot connection, decreasing the system's usefulness [27]. Verifying the identity of operators using their unique operating signatures is essential to enhance the safety and security of teleoperated robotic systems. Human control is not a one-off activity; it is continuous for the duration of a task, a workload period or a mission (all of which may entail a significant time). There is a need to provide continuous user authentication in order to remotely control a robotic system.

Testing such systems using a mimicry attack regime is critical for stressing them from a security standpoint. Evaluating the range of information available to an attacker enables more informed security management decisions, for example, to reduce the likelihood of high levels of information being available to an attacker.

Previously, in Chapter 3, we investigated continuous authentication for collaborative robot manipulators. The human co-worker used the robot arm's joint information (position, force, and torque) to collect biometric data. In Chapter 4, we investigated the implementation of continuous behavioural biometric authentication using wearable sensors similar to those found in an exoskeleton. We used data from a WiFi-enabled sensorised glove that monitors a user's hand movements. In this chapter, we examine the continuous authentication of behavioural biometrics in the context of control and programming of industrial and teleoperated robots. We analyse a situation in which attackers are provided information about their victims' behavioural patterns, and they make a deliberate effort to mimic them. If imitation is feasible, the equal error rates will become unacceptably high. Consequently, individual working behaviours would be inappropriate for use as biometrics features.

5.2 Related Work

As far as we are aware, no prior study has examined or implemented mimicking threats against behaviour-based biometrics authentication in human–robot interaction. However, several studies have investigated impersonation threats against behavioural biometric authentication techniques, such as touch-based identification, gait analysis and keystroke dynamics.

In [109], the authors evaluated two basic methods of malicious insider attacks against touch-based identification systems. They conducted a targeted imitation attack and showed that touch-based identification systems fail against shoulder surfing and offline training attacks. They found that shoulder surfing attacks have an 84% bypass success rate, with the majority of successful attackers monitoring the victim's behaviour for less than two minutes, based on tests with three different touch input implicit authentication schemes and 256 distinct attacker–victim pairings.

In [110], the authors assessed the vulnerability of keyboard dynamics to imitation attacks when password hardening is used on smartphones. They created augmented reality software that runs on the attacker's smartphone and uses computer vision and keyboard data to offer real-time assistance throughout the victim's phone's password input process. In their tests, 30 users launched over 400 impersonation attacks. The authors showed that imitating keystroke behaviour on virtual keyboards is simple for an attacker. They also demonstrated the flexibility of their augmented reality-based approach by successfully conducting imitation attacks on a continuous authentication system based on swiping behaviour.

In [138], the authors created a software tool to collect and analyse gait acceleration data from wearable sensors. Additionally, the study was based on an experiment involving intensive training of test participants and various feedback sources, including video and statistical analyses. The attack scores were studied to ascertain whether the participants are improving their mimicry abilities, or, more simply, whether they are learning. Fifty individuals were registered in a gait authentication system for the trial. With an EER of 6.2%, the error rates are comparable to those of state-of-the-art gait technology. The authors pointed out that replicating gait is a difficult job and that our physiological features work against us when we attempt to alter something as basic as our walking patterns. They found that the participants show no evidence of learning, and the outcomes of the majority of attackers deteriorate with time, demonstrating that training has little effect on their success.

In [117], the authors showed how a digital treadmill may be used to mimic an individual's stride patterns recorded using a smartphone accelerometer. They also created an attack for a baseline gait-based authentication system and thoroughly evaluated its effectiveness using an 18-user dataset. The attack raises the average false acceptance rate (FAR) for the RF from 5.8% to 43.66% by using just two attackers and a basic digital treadmill with speed control capabilities. In particular, the FAR of 11 of the 18 users increased to 70% and above.

5.3 Threat Model and Attacks

Continuous authentication systems are subject to many attacks. However, we will not address the full range of threats to such systems in this chapter. Rather, we will focus on authentication threats from users who wish to pretend to be particular targeted users. We can categorise attackers by the amount of information they have on the behaviour of the target victim. They may have no information at all, be able to access observational information, e.g. by shoulder surfing the target user or having access to videos of the target user working, or have detailed behavioural information, e.g. stored behavioural biometric information.

Access to detailed information may allow the attacker to develop a training system that provides detailed feedback on how close the attacker's behaviour is to that of the target victim. This is one mechanism we explore in this chapter. This is the best case for an attacker and the most severe evaluation stress for a biometrics continuous authentication approach. Knowledge of how a system performs against attackers across the range of information available will enable the most appropriate further security measures to be taken, e.g. measures to ensure that detailed biometric information is not leaked.

The types of attacks that we investigate are detailed below.

5.3.1 Zero-Effort Attacks

As we mentioned in Chapter 3, zero-effort attacks are often used to assess the accuracy and reliability of biometric authentication systems [131]. We used this evaluation technique in previous chapters (Chapter 3 and 4.)

5.3.2 Imitation Attacks

In imitation attacks, an attacker must first be familiar with their victim's working behaviour to imitate them. In this chapter, we examined two malicious insider imitation attacks: shoulder surfing and offline training attacks.

1. **Shoulder surfing attacks.** In this attack, insiders with malicious intent can observe their victim's interactions. As a result, adversaries can try to mimic measurable characteristics. Whether shoulder surfing has an advantage in terms of mimicking measurable characteristics is unknown. Researchers have spent substantial time developing novel authentication methods to overcome the challenge of shoulder surfing.

2. **Offline imitation training attacks.** In this attack, malicious insiders can obtain their victim's raw data by extracting the victim's profile from a breached biometrics database. Additionally, insiders may utilise the raw data to learn and emulate their victim's behaviour once they have access to it. We operationalised this idea to the extent of providing online mimicry training.

We are aware that our approach does not exhaust the potential for attacks. Indeed, if detailed biometric information becomes available, a bot could be created to achieve successful authentication. We leave consideration of such attacks and bot detection for future work.

5.4 Experimental Design Considerations

5.4.1 Experimental Choices

We used V-REP as the robot simulator (currently, it has been re-branded to CoppeliaSim [167]). V-REP is a popular robotic simulator for educational and research applications, and it comes with a free academic licence. Compared with Gazebo simulations, V-REP software can be installed and run without the need for a powerful graphics card and does not require the use of a powerful CPU [73]. In addition to its many sensors or robot models, V-REP includes several functions for creating a virtual world. Users may engage with the virtual world throughout the simulation, making it more interesting. The experiments use a simulation of KUKA LBR iiwa R800, which is a popular collaborative robotic arm.

5.4.2 Experimental Design

Here, we describe how to identify a robot's operator using the velocity and accelerometer data we acquired from their interactions with the robot while completing a specific task. The task was to move an object, a ball, from a start point (red circle) to an endpoint (yellow circle) and solve a maze 15 times, as shown in Fig. 5.1. The robot was tasked with tracking the ball's movements. In the experiments, the user moves the ball using a mouse. Therefore, we assumed that the movement of the mouse would be a movement of the user's hand, representing the behaviour or the user's interaction with the robot. The experiment consisted of three primary stages: designing and implementing the data collection process in the V-REP simulator using Python; extracting informative features from the acceleration and velocity data along two axes, X and Y; and using the features to train and build a model for classifying individuals based on their working behaviour patterns.

5.4.3 Data Collection

We used the V-REP simulator and mouse to collect our data on the task. During the experiment, the simulator gave the position and velocity of the object; we could then use this information to calculate the acceleration along the X-axis (horizontal movement of the object) and Y-axis (forward and backward object movements) using Equation 5.1. In addition

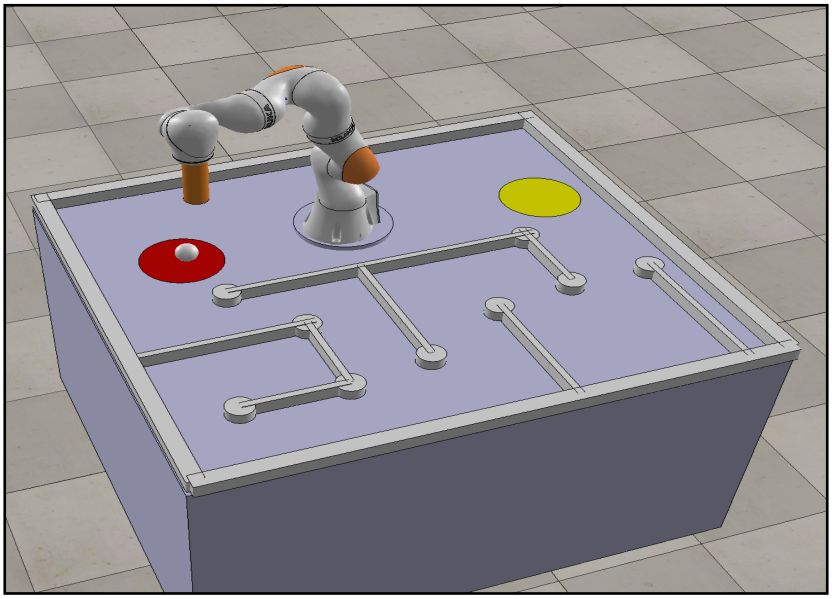


Figure 5.1: Experimental design

to the raw data (position, velocity and acceleration), we collected three video recordings of each victim.

$$Acceleration = \frac{final\ velocity - initial\ velocity}{Total\ Time} = \frac{\triangle v}{\triangle t} \tag{5.1}$$

Thirty-two individuals, comprising 22 males and 10 females with an average age of 28 years, volunteered to participate in this simulation-based experiment. Each volunteer used the mouse to move the object in simulation mode, and performed the same task activity (moving an object to solve the maze). The volunteers' data (e.g. acceleration, velocity and position) were exported to a CSV file.

We can be confident about the sincere commitment of the locally recruited students to obey all aspects of our protocols. It must be acknowledged, however, that a larger sample size would clearly be beneficial. Crowdsourcing platforms such as Amazon's Mechanical Turk (MTurk) could be used. However, this comes with the risk that participants will submit with multiple MTurk IDs [57] and so generate highly similar biometric profiles that appear to be from different users. For instance, participants who accessed the trial(s) via virtual private servers (VPSs) could have provided fraudulent data[57]. These virtual machines allow users with multiple MTurk IDs to participate in the same study many times without being identified [57]. Consequently, an unrepresentative sample of user profiles may be generated, which in turn may give misleading results. For example, developed models will likely not distinguish users that are, in reality, the same person, leading to increased false positive classifications.

5.4.4 Feature Extraction and Feature Subset Selection

Before the extraction of features, the data were divided into segments in two different ways; specifically, we used time-based and point-based segments. In the time-based segments, each segment was t sec long. In our case, each task is sampled at 20 Hz, divided into windows containing 60 samples (i.e. 60 samples = 3 s).

In the point-based segmentation, we divided the data depending on four points, as shown in Fig. 5.2: start point, test point 1, test point 2 and end point. Thus, all the position points between two points represent a segment.

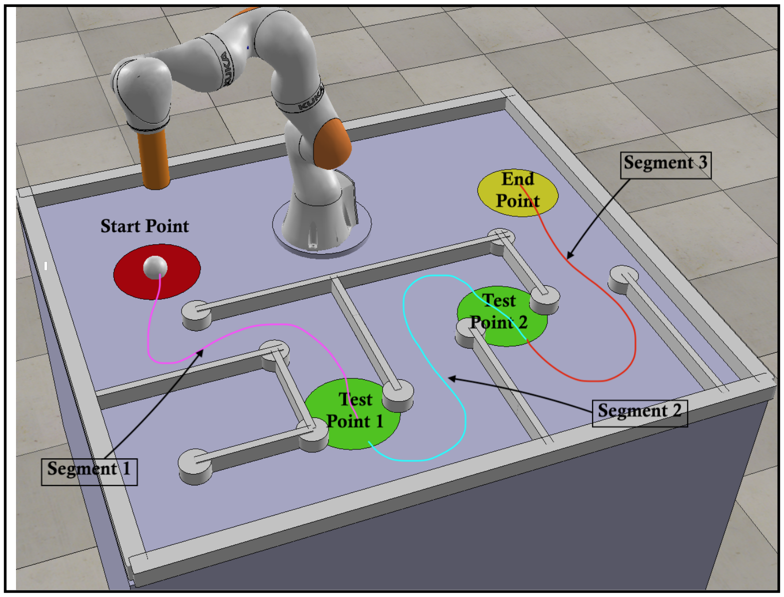


Figure 5.2: Data segmentation: illustration of point-based segments.

We extracted the characteristics of the acceleration along the X and Y axes and the velocity and acceleration magnitude for each user as they performed the task. These features are listed in Table 5.1. The feature extraction process yielded a total of 62 features. There are six primary monitored variables: acceleration_x, acceleration_y, acceleration_magnitude, velocity_x, velocity_y and velocity_magnitude. We calculated over each of these six variables seven statistics and three temporal measures. We added a task number and time (the period to complete the segment), which increased the number of features to 62.

To minimise training time and improve the accuracy of the ML algorithm, we selected the most appropriate features. We then analysed and evaluated our feature set using the recursive feature elimination selection method [84]. In our experiment, the number of features was reduced to 26.

Table 5.1: List of features

Domain	moment_measures	Length
Statistical	Mean, Median, Minimum, Maximum, Skewness, Kurtosis, Standard deviation	$7 * 6 = 42$
Temporal	Entropy, Total energy, Peak-to-peak distance	$3 * 6 = 18$
other	Time, Task number	2
Total		62

5.4.5 Considered Classifiers and Parameter Value Selection

Our method is focused on binary classification. Verifying experiments were conducted using the RF and SVM classifiers (see the Appendix A for more results using different classifiers). A binary classifier with the classes *genuine user* and *impostor user* is trained for each user of the continuous authentication scheme. Furthermore, each classifier is trained with an equal amount of genuine and impostor data to avoid bias. We defined a classification threshold (sometimes referred to as the decision threshold) of 65%. To determine the optimal hyper-parameters, we used a grid search method.

For the RF classifier, for parameter $n\_estimators$, we searched over 200–2000; for max_depth, we searched through 10–110; for $min\_samples\_split$, we searched over 2, 5 and 10; and for $min\_samples\_leaf$, we searched over 1, 2 and 4. The parameter selections for RF for which we report the results in this chapter are listed below.

- $n\_estimators = 200$ (i.e. number of trees)
- $max\_depth = 10$ (i.e. maximum depth of the tree)
- $min\_samples\_split = 2$ (i.e. minimum sample number needed for separating at an internal node)
- $min\_sample\_leaf = 1$ (i.e. number of samples needed to be at a leaf node)

For the SVM classifier, for parameter C, we searched over 0.1, 1, 10 and 100, and for parameter $gamma$, we searched over 1, 0.1, 0.01 and 0.001. The parameter selections for SVM were $kernel = linear$ (i.e. the mechanism by which data are taken as input and transformed into the format necessary for processing), $C = 1$ (i.e. regularisation parameter) and $gamma = 0.1$ (i.e. kernel coefficient.)

5.5 Attack Design

The primary aim of designing offline training attacks is to determine whether the feedback provided to the attackers will assist them in imitating legitimate users. We provided three types of feedback to attackers:

1. **Feature feedback:** When the attacker has access to the template, they will see which features are incorrect (in our case, this includes X, Y position, time and speed).
2. **Decision feedback:** As in a standard scheme, an attacker is either accepted or rejected.
3. **Score feedback:** This is the probability score obtained from the classifier. It refers to the probability that the user is authentic, as calculated by the classifier.

Suppose attackers can increase their chances of being accepted as another genuine user as a result of the provided feedback. In this case, we may infer that learning from another person's interaction behaviour is possible. However, where there is just a slight change or none at all, we may assume that replicating another person's interaction behaviour is very challenging. Unlike shoulder surfing attacks, the attackers would not see how the victims are doing the task, making the attacker's task more challenging. However, we want to replicate a situation in which the attacker has retrieved the victim's template from a compromised biometrics system. This is the optimal situation from an attacker's point of view because it enables them to create an accurate detector replica with the parameters of the victim for the attacker's training needs [195].

We create an interface that uses input and visual display created from a victim's raw data to train an attacker to imitate the victim's behaviour (see Fig. 5.3). The training interface shows the simulation's trajectory for the chosen victim (X, Y position data). The attacker then runs the simulation to replicate the victim's trajectory based on the initial data. Suppose that the attacker is rejected by the authentication method. In this case, a window containing a comparison of the attacker's and victim's behaviours in terms of speed, duration and trajectory is presented to the attacker (see Fig. 5.4b). In addition to the probability of authenticity calculated by the classifier, the degree of proximity or distance to the victim's template is indicated. Recommendations that assist the attacker in improving their next attempt, e.g. highlighting a need to speed up, slow down or pay attention to the path, are likewise given.

5.5.1 Recruitment and Motivation of Participants

In a real-world attack, attackers are motivated to bypass the authentication mechanism for malicious purposes. We used performance-based monetary awards to encourage participants to launch best effort attacks in our experiments. Each participant was rewarded £5 for every attempt that was accepted in the attack experiment.

5.5.2 Procedures for the Attack

The approach started with each subject submitting raw data using the collecting Python controller described in Section 5.4.2. As shown below, each participant then launched shoulder surfing and offline training attacks. In the robot simulation, the participant was given two victims for each attack type. The first 16 users served as the targets of attack for the second

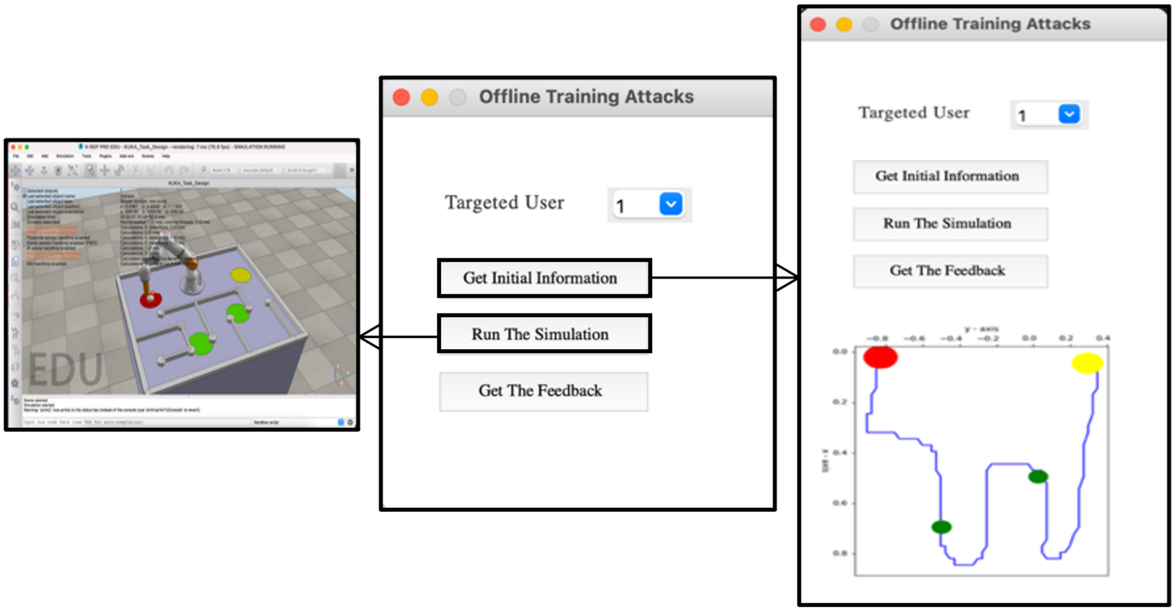


Figure 5.3: Main interface

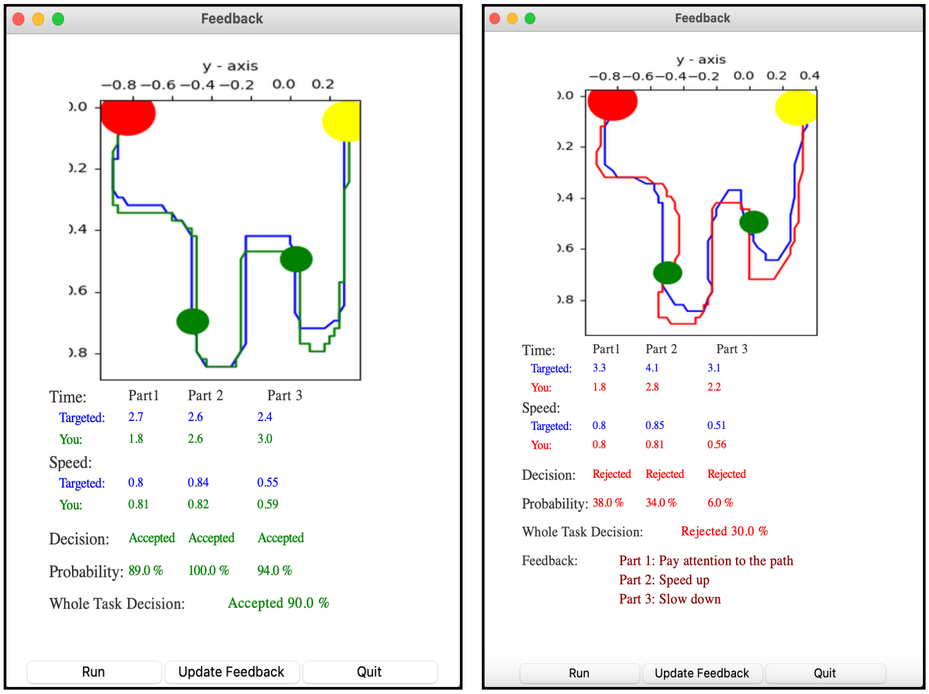
16 users. Each of users 1–16 is attacked by two of users 17–32. Each of users 17–32 attacks two of users 1–16.

The *shoulder surfing attack* consisted of two components: viewing videos of the target and attacking by imitating the victim's execution of the maze task. The attackers were allowed to re-watch the videos as many times as they wanted. Once the participant confirmed that they were ready, the video was closed, and the simulation was launched, allowing them to emulate the victim's execution of the task. The participants were informed that they could re-watch the video if their attempt failed before trying to imitate the victim's behaviour.

The *offline training attack* consisted of two components: training using the mimicker software and attacking by imitating the victim's behaviour on the task. Before the first training attempt, the attackers obtained initial information, which is the trajectory of their victims, as we can see in Figure 5.3. The participants were told that they would be required to overcome the authentication mechanism at least once (one whole task) during the training phase before conducting the actual attack. If they could not defeat the authentication mechanism during the training phase, they were required to carry out at least 20 training tasks before moving on to the real attack. No feedback was given throughout the actual attack (see Fig. 5.5), and the participants only had six attempts.

5.6 Results and Discussion

The study included 32 participants (16 victims and 16 attackers). There were a total of 384 logged attacks (192 for each attack type).



		Part1	Part 2	Part 3
Time:				
	Targeted:	2.7	2.6	2.4
	You:	1.8	2.6	3.0
Speed:				
	Targeted:	0.8	0.84	0.55
	You:	0.81	0.82	0.59
Decision:		Accepted	Accepted	Accepted
Probability:		89.0 %	100.0 %	94.0 %

Whole Task Decision: Accepted 90.0 %

(a) Accepted.

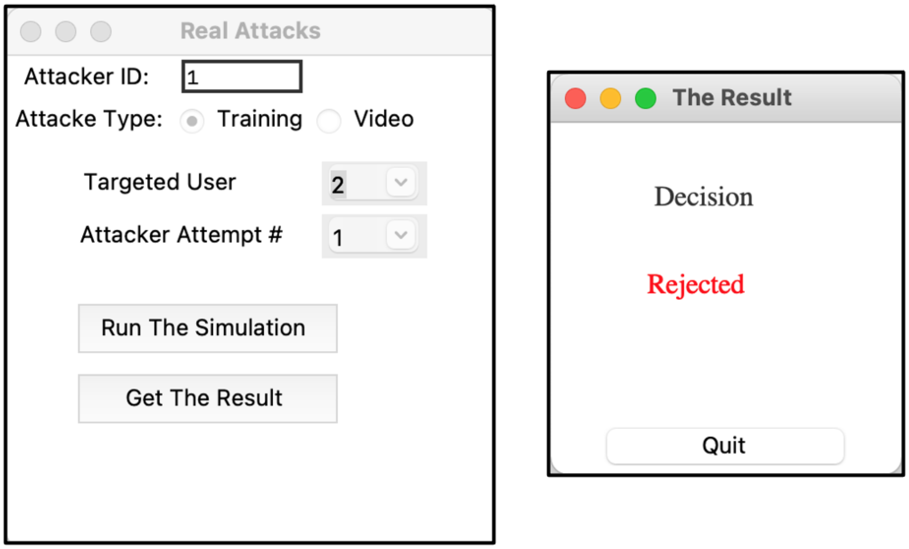
		Part1	Part 2	Part 3
Time:				
	Targeted:	3.3	4.1	3.1
	You:	1.8	2.8	2.2
Speed:				
	Targeted:	0.8	0.85	0.51
	You:	0.8	0.81	0.56
Decision:		Rejected	Rejected	Rejected
Probability:		38.0 %	34.0 %	6.0 %

Whole Task Decision: Rejected 30.0 %

Feedback: Part 1: Pay attention to the path
Part 2: Speed up
Part 3: Slow down

(b) Rejected.

Figure 5.4: Feedback interface.



Attacker ID: 1

Attacke Type: ● Training ○ Video

Targeted User 2

Attacker Attempt # 1

Decision

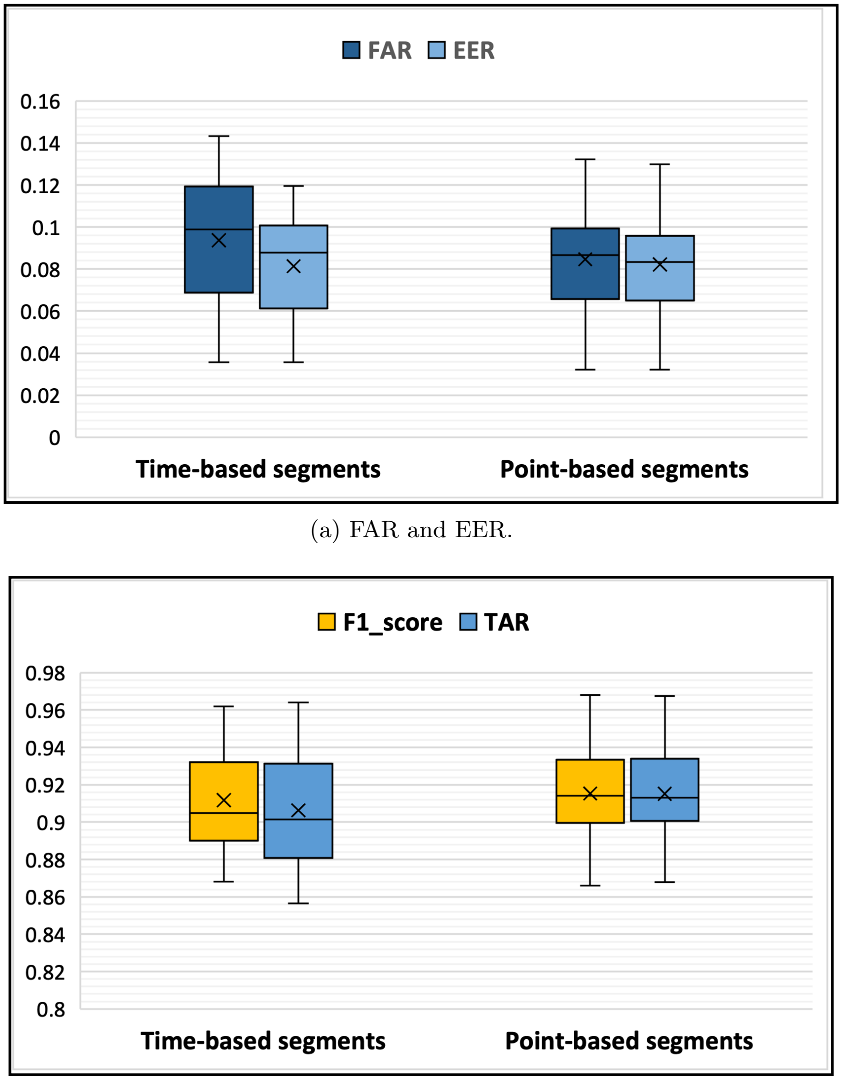
Rejected

Figure 5.5: Actual attack interface

5.6.1 Baseline Evaluation

To assess the efficacy of the zero-effort attack, we studied four typical metrics: F1 score, TAR, FAR and EER. The F1 score provides a weighted average of precision and recall. The TAR denotes the likelihood that the system will match a genuine user to a system-stored template for that user. The FAR denotes the likelihood that the system will erroneously match a behavioural template from an impostor to the behavioural template stored by the system of a targeted genuine user. We also calculate the false reject rate $(FRR) = (1 - TAR)$, which allows the pairs (FAR, FRR) to be calculated for the various parameter values (see Section 5.4.5) of the particular ML technique being used. The EER indicates the point at which the FAR and FRR are equal. The lower the system's performance, the higher the EER value and vice versa. We utilised five-fold cross-validation to determine the prediction efficiency. Cross-validation protects against over-fitting by dividing the dataset into folds and assessing the accuracy of each fold. As a result, this technique yields an accurate evaluation of the prediction accuracy of the final trained model on the dataset.

Figure 5.6 shows the results of the two experiments when using the RF classifier. We found that the average F1 score is 91.2% and 91.5% for the time-based segments experiment and point-based segments experiment, respectively (see Fig. 5.6b). The average of the EER was 8.1% and 8.2% for the time-based and point-based distributions, respectively (see Fig. 5.6a).

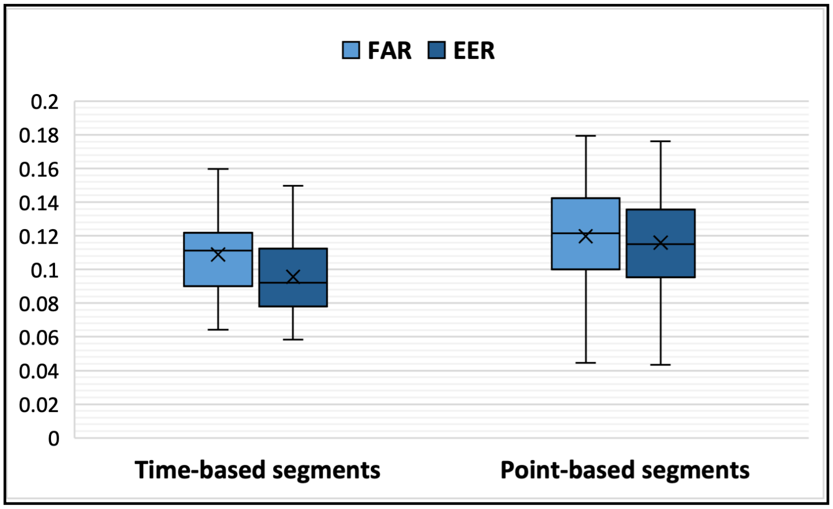


(a) FAR and EER.

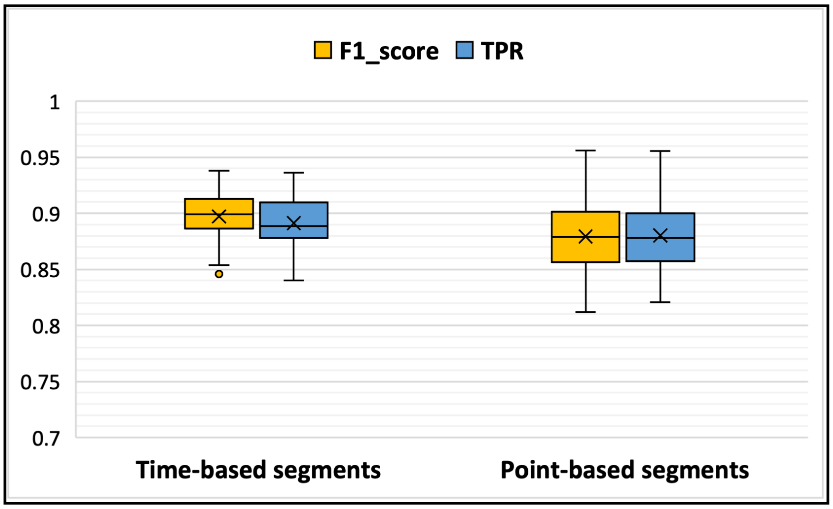
(b) F1 score and TAR.

Figure 5.6: Evaluation of the RF classifier for 32 users.

The findings obtained with the SVM classifier differed slightly from those obtained with the RF classifier (see Fig. 5.7), as the average F1 score was 90% for the time-based segments experiments and 88% for the point-based segments experiments. The average EER was 9.3% and 11.6 % for the time-based and point-based segments, respectively.



(a) FAR and EER.

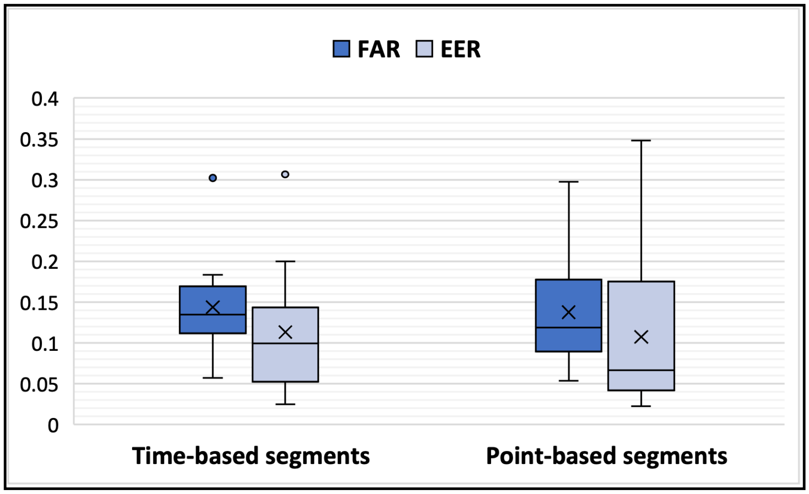


(b) F1 score and TAR.

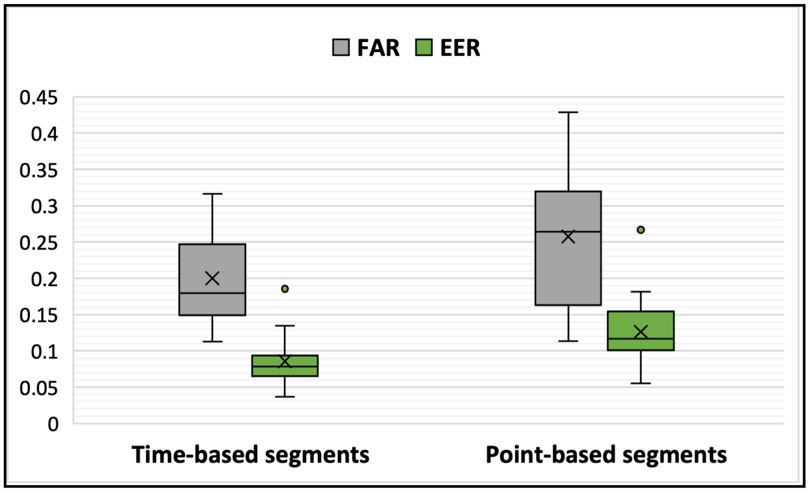
Figure 5.7: Evaluation of SVM classifier for 32 users.

5.6.2 Evaluation of Offline Training Attacks

In this section, we measure the performance of an attacker who has been trained to mimic the targeted victim. As described in Section 5.5, the attackers received three types of feedback to help them in mimicking genuine users. To measure the efficacy of the attack, we calculated the EER and FAR. As presented in Figure 5.8, in both experiments, the mean of the EER was less than 0.15 regardless of whether we used the RF or SVM classifier. However, for the SVM, the FAR in both experiments was greater than 0.15, as shown in Figure 5.8b.



(a) RF classifier.

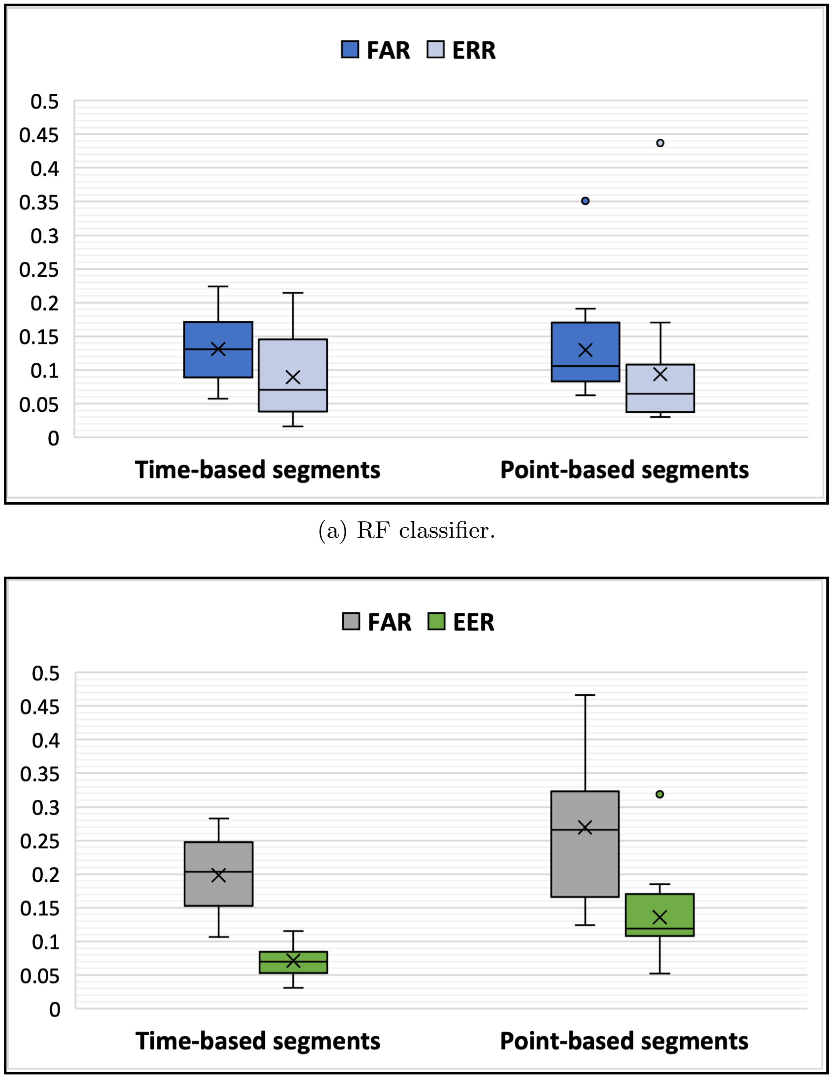


(b) SVM classifier.

Figure 5.8: Evaluation of offline training attacks

5.6.3 Evaluation of Shoulder Surfing Attacks

In this part, we measure the performance of an impersonating attacker who is aware of the present system's authentication process. The attacker is considered to be monitoring their victim from a nearby location or attempting to mimic the victim's behaviour by viewing a previously captured video of the victim. To reproduce this impersonation attack scenario, we captured a video of a genuine user doing a task and presented it to an attacker who was also a participant in our research. The attacker attempted to imitate the legitimate user by watching the video several times, as provided in the experiments. Similar to offline training attacks, we calculated the EER, FAR and attacker acceptance rate. As presented in Figure 5.9, in both experiments, the mean of the EER was less than 0.15 regardless of whether we used the RF or SVM classifier.



(a) RF classifier.

(b) SVM classifier.

Figure 5.9: Evaluation of shoulder surfing attacks

5.6.4 Attacker Acceptance Rate

In this section, we measure the attacker acceptance rate, which indicates how many attacker samples pass the authentication mechanism. Table 5.2 shows that the highest attacker acceptance rate in offline training attacks was 29.2%, in time-based segments when we used the RF classifier. Conversely, the lowest attacker acceptance rate was 13.3%, for time-based segments when we used the SVM classifier.

The highest attacker acceptance rate in shoulder surfing attacks was 28.6%, for time-based segments when we used the RF classifier. However, the lowest attacker acceptance rate was 12.5%, for time-based segments when we used the SVM classifier.

As shown in Table 5.2, We observe that, for the RF-based classifier, the false acceptance rates for both offline and shoulder surfing attacks are greater for the time-based authentication than for point-based authentication. However, the opposite is the case for the SVM classifier.

It is hard to determine, or even speculate with any confidence, why this should be the case. It is useful to consider how conservative the training assumptions are. Witnessing three authentication attempts by the target user (i.e. shoulder surfing) seems a plausible threat, though the witness adversary would likely see these spread over a period of time (which imposes a potentially significant cognitive load). Seeing three attempts in short succession (as per the training in our experiments) would seem an implausible and hence highly conservative assumption.

For offline training, we should remember that the information availability assumption is highly conservative: the adversary needs to be able to develop a simulation capability with access to the target users' behavioural template data. In this context, false acceptance rates of 12.5 or 13.3 percent (achieved by the SVM time-based approach) should not be considered particularly high. The conservative data availability assumptions were a deliberate attempt to stress test the authentication systems. It might also be observed that a more intensive training regime, i.e. where the users have unlimited training opportunities, would increase these false acceptance rates. Furthermore, the task attempted by users in this chapter (i.e. maze following) is actually rather simple. It might be expected for users to be able to masquerade to some extent. This might not be the case for more sophisticated tasks, where user "micro-movements", imperceptible to an adversary, might be distinguishing characteristics of the attacked users. Investigating this is left as future work.

Table 5.2: The attacker acceptance rate for two classifiers.

Classifier	Experiment	Offline training	Shoulder surfing
RF	time-based	29.2%	28.6%
	point-based	26.3%	25.7%
SVM	time-based	13.3%	12.5%
	point-based	14.8%	19.5%

5.7 Limitations

In an offline training attack, we used simple-to-understand features in the feedback module. Our experimental setup reveals that these techniques are not vulnerable to very simple attacks. We do caution, however, that skilled attackers may enhance their chances of success by practising on the excluded features.

A limitation of the experiments in this chapter is that they were carried out using a simulation-based system rather than a physical robot. Furthermore, control of the working simulation system is entirely by mouse and the feedback is entirely visual. A real application might involve more sophisticated control and feedback, e.g.using a joystick for control and receiving sound and haptic feedback. Increasing the complexity of the system in such a manner may affect the applicability of the results presented here. However, we also note that a wider range of information may lend itself to the very approaches exemplified here. This remains a future work avenue.

5.8 Summary

A behavioural-based biometric continuous authentication system was developed for a (simulation-based) human–robot interaction task. The task is representative of the type of activity performed in remote operation, in which a user is physically involved in guiding the behaviour of a robot. Our method provides a way to ensure that humans programming robots by demonstration or remotely operating robots are always authenticated. This is especially important in industrial and high-risk settings, where only a limited number of authorised users are allowed to control or reprogram robots. We evaluated this mechanism under the behavioural biometric attack known as a mimicry attack under different regimes of knowledge of the attacker. The results show that biometric approaches can be used to deliver effective continuous authentication and that mimicry attacks may be quite difficult. However, the difficulty level may vary significantly depending on the specific tasks attempted. Investigating this issue over further test types is an important area for future work.

Chapter 6

Conclusions and Future Work

6.1 Summary of the Thesis

Collaborative robots and other HRI systems, such as exoskeletons and teleoperation, have excellent potential for enhancing manufacturing processes. Increasing the security for these types of robotics technologies is crucial to realise their potential. Biometric authentication of users can increase the security of robotics technologies by stopping unauthorised individuals from controlling and manipulating them and guaranteeing that authorised users operate within their authorised boundaries.

This thesis illustrates how user authentication may be used in three different contexts: a direct physical manipulation application, a sensor glove application and a remote access application. We focused on CA rather than one-off authentication. The research hypothesis we identified earlier was as follows:

Continuous biometrics can form the basis for the effective and practical authentication of users operating in close collaboration with robots.

Furthermore, all three investigations sought to use data that would be collected by the system *as part of normal operations*. Authentication in our investigated schemes did not require any specific actions on behalf of the user; the user simply goes about their work. This *unobtrusiveness* is of major importance in manufacturing and other critical environments.

Specifically, we investigated *behavioural* biometrics as a means of user authentication, focusing on the behaviour of human co-workers as they operate in close collaboration with robots. An in-depth literature review (Chapter 2) was carried out. Chapter 2 investigated extant user authentication methods and briefly examined the role of robots in industry. It emphasised the concept of authentication in general. There are three basic approaches to user authentication: knowledge-, object- and biometric-based authentication. Although knowledge- and object-based authentication methods have many security weaknesses, they are the most commonly used methods for verifying a user's identity. However, both knowledge- and object-based access can easily be compromised. Passwords and other special pieces of knowledge can be shared and/or forgotten, and tokens, such as smart cards, can also be lost or stolen.

Biometric-based forms of authentication can overcome the problems in other approaches. Biometric markers can be used for recognising an individual based on their biometric features. New authentication systems require a balance between simplicity, cost, accuracy, performance and acceptability, in addition to security. One of the problems identified with traditional forms of authentication, including some biometric forms, is that they are very intrusive. For a manufacturing setting, they may be overly intrusive, e.g. requiring interruption of work processes. In Chapter 3, we propose a system that uses internal sensor data collected automatically as the basis for CA and **imposes no additional requirements on the user**.

Compared with conventional authentication methods, biometric authentication can be highly secure. Recently, various application areas, such as airport security, mobile access and authentication, banking and building access, have come to rely on biometrics. Although biometric systems have limitations, they are becoming increasingly common security technologies, most obviously biometrics have seen a very high footprint in smartphone security particularly fingerprint and facial recognition. Despite their emergence as solutions to avoid the defects and problems associated with traditional authentication systems, biometric systems can still be vulnerable to attacks. Several types of attacks can threaten biometric systems, either directly or indirectly. Direct attacks include DoS, fake biometrics and latent print reactivation. Indirect attacks include modifying a biometric system's template, using Trojan horses and intercepting communication channels between modules of a biometric system. Several techniques can improve the defence of biometrics against these attacks, such as liveness detection, soft biometrics, challenge–response systems, watermarking, continuous biometric authentication, multimodal biometric systems and MFA.

In Chapter 3, we proposed an original approach to the CA of users to a collaborative robot. More precisely, we discussed how data from the internal sensors of a collaborative robot can be used to characterise a user's physical contact with it and serve as a reference template for authentication. We leveraged ML-based classification to continuously authenticate actual user behaviours against these distinctive templates. Our approach, which uses a recognised trust model, can provide a reasonable and practical solution for continuously authenticating users who engage physically with a collaborative robot in terms of rejecting imposters (i.e. low ANIA) and approving legitimate users (i.e. high ANGA). Additionally, it uses data that the collaborative robot *already maintains as part of its normal operations.* The major experimental findings proved the usability of the biometric authentication in collaborative robots.

Chapter 4 showed how CA can be performed using wearable sensors, such as those included in exoskeletons or haptic interfaces. We demonstrated authentication specifically using the perceived physical manipulations of a user via an e-glove. In general, the way a user touches, squeezes, and interacts with the glove is unique. Even when the same operation is executed, a user's sensor traces differ from those of another authorised user or an invader. An ML approach was used to match dynamic behaviour feature vectors to users in the reference database. The matching was obtained through training with a random forest technique, and it demonstrated highly promising results in terms of rejecting imposters (i.e. low ANIA) and approving legitimate users (i.e. high ANGA). The e-glove delivers a multi-channel stream of pressure data as part of its regular functioning. The gathered data may be used for a number of applications, including robot control, teleoperation, robot training and ergonomic assessment. Our method demonstrates that such data may also be used for a secondary purpose: the foundation for efficient CA. *No further data collection is required.* As a result, the method is very cost effective in terms of implementation and is generally **unobtrusive to the user**.

In Chapter 5, we demonstrated our approach for ensuring that humans remotely operating robots are always authenticated. This is critical in industrial and high-risk environments, where only small numbers of approved people are permitted to control or reprogramme robots. We assessed this method using a behavioural biometric attack known as a mimicry attack with varying levels of attacker awareness (i.e. able to access different levels of user information). The findings indicate that biometric techniques are capable of providing effective CA and that launching mimicking attacks may be quite challenging. However, the difficulty level will vary substantially based on the tasks attempted. We also stressed that teleoperation is a primary control mode for robots operating in hazardous environments, and authentication for remote operation must be developed to secure this. In the long term, this is likely to be a key application for approaches of the kind reported here.

In summary, the experiments presented in this thesis all propose user authentication for robotic technologies. We used an application for direct physical manipulation in chapter 3, sensor gloves in chapter 4, and remote access in chapter 5. All experiments share the fact that authentication relies on data acquired or created as a result of a coworker's normal work activities. No further action is required. We may conclude that the difference between the experiments is related to the employed ML method. In chapters 3 and 4, we use multi-class classification, whereas in chapter 5, we use binary classification.

6.2 Discussion

The following observations are made:

- In general, we believe that we have advanced the state of the art by developing a CA system for robots, particularly those that require close user interaction, such as collaborative robots, exoskeletons and teleoperation.

- In a continuous biometric system, a recovery cycle must be invoked when the user is locked out. This will most likely involve a one-time authentication approach, such as a password, but it *could* also be any of the traditional authentication methods or even another biometric. This aspect is not the focus of this thesis. An assessment should be made of possible methods with respect to identifying those with reduced intrusiveness and clear feasibility.

- Continuous biometrics can be used with a variety of threat models. We used several of them, including zero-effort attacks, statistical attacks and imitation attacks. In particular, we believe that we have pushed the state of the art in developing a very conservative threat model in Chapter 5. We developed a user interface that assists the attacker in improving their ability to impersonate the authorised user by providing text and visual feedback.

- We have made methodological contribution. We evaluated the authentication system in several ways of data segmentation (whole task and task multi-segment). Additionally, we used the TSFEL library, which we believe is the first time this or a similar library has been used to extract features for use in a biometric authentication system.

- There are several technological contributions made by this thesis. Authenticating the user requires no additional effort, as the user is not required to make any specific effort other than perform their routine job tasks. External sensing equipment is not required in Chapter 3. The system is entirely dependent on the robot's internal sensors. The experiment in Chapter 4 provides continuous user authentication in the context of industrial tasks, but we believe that it may also be useful in other fields, such as healthcare.

- The three technical chapters have addressed different aspects of continuous biometric authentication for manufacturing collaborative robot systems. The outcomes suggest that the overall approach is quite versatile. Some aspects of the approaches taken can clearly find ready application in other collaborative robotic authentication systems, e.g. the trust model used in Chapter 3. The TSFEL used in Chapters 3 and 4 to automatically synthesise some features will also find application in many future continuous biometric authentication time series analyses for collaborative robots.

- In Chapter 4, we used the *lfilter* function to apply the digital low-pass Butterworth filter to obtain a smoother version of the original data. We did, however, evaluate our system without the filter and discovered that the difference is not significant. For instance, in zero-effort attacks, the average F1 score using WSF is 99.4%, whereas the average F1 score without the filter is 98.96% (see appendix A.5.)

- In Chapter 3, to evaluate the variability of a user's behaviour over time, we requested participants repeat the experiment after around 40 days, and found that the majority of users (16 users) can complete most tasks without being rejected by the system (see appendix A.3). However, further work on such properties is desirable.

6.3 Limitations and Future Work

Below we summarise limitations of the work presented in this thesis. These can serve as areas for useful future investigation.

- A limitation of most behavioural-based biometrics is that individuals' behaviours may fluctuate slightly because of changes in physical or mental condition. One of the effects of these factors on the authentication system is that an authorised user may be rejected from the system because of fatigue or mood swings. Here, because in relevant applications, there are often policies that prevent a user from operating equipment when they are not sufficiently capable and alert, the detection of behaviour variance due to tiredness and mood will actually be desirable. However, a full investigation of this issue in general could be important future work.

- In Chapter 4, our analysis has limitations, as described in Section 4.5, which lead to interesting future research directions. Briefly, we propose an ML-based biometrics authentication using hand pressure and flexion data measured by an e-glove during industrial-oriented activities, distinguishing imposters and legitimate users via the usual operational movements. More precisely, we authenticate users after a series of brief activities, as described in Section 4.3.1. As future work, it would be interesting to test our system's capability of authenticating users based on a single activity, such as walking, carrying an item or turning a screw, instead of a sequence of activities. Furthermore, using additional and important machine learning techniques (e.g., deep learning) for classification could enhance results.

- In this thesis, we use a classification approach. If the dynamic profile presented by the user matches the claimed user profile in the database, the user is authenticated. As a future study, it would be interesting to evaluate our system's capability of authenticating users based on the anomaly detection approach. This approach can distinguish between normal and abnormal patterns. This is usually the case with research that focuses on intrusion detection or other application areas that necessitate user comparisons or normal/abnormal behaviour comparisons. Anomaly detection detects a deviation from an established pattern of behaviour. This can be used for biometric authentication purposes by training a behavioural model for each user in the system. Once the identity of a user has been supplied (e.g. by provision of a user id and an initial password) that user's run time behaviour can be tested against the stored profile or model for that user.

- A consequence of the recent COVID-19 pandemic has been an intensification of interest in remote operation. In advanced manufacturing approaches such as those that leverage virtual reality (VR) and more recently augmented reality (AR) are emerging as highly promising, and interfacing means are advancing rapidly, with the use of, for example, Microsoft's Kinect and Hololens being trialled for manufacturing applications [37, 94]. The data collected (or easily collectable) by such systems could form the basis for another promising and unobtrusive means of CA of users to manufacturing systems.

  We purchased several such types of equipment: Emotiv EPOC+ for brainwave sensing, Shimmer IMU3 accelerometry and HoloLens 2. Unfortunately, because of the pandemic, we were unable to conduct user experiments with these; rather, we used an existing public dataset in Chapter 4 and investigated remote operations in Chapter 5. There is clear potential for further research into unobtrusive, no-extra-cost sensing as a means to deliver CA.

- In section 5.7 it was identified that experiments were carried out using a simulation-based system rather than a physical robot. It was further noted that control was entirely by mouse and the feedback was entirely visual. Further work with a real system and more diverse control and feedback remains as future work.

- In Chapter 5, one might even consider how an automated intelligent adversary would perform given the same degree of training assistance. An automated approach can be absolutely reliable and can likely be trained to hone in on the desired acceptable behaviour. If such a scenario becomes a significant threat then one would have to investigate means to detect such 'authentication bots'. This raises intriguing possibilities. For example, could we develop a CAPTCHA angle on the authentication protocol? Of course, this merely starts a war! An AI-enabled attacker could be trained to interact in a manner sufficiently *similar* to a target user (and so pass authentication) but not repeatedly exhibit *identical* behaviours (because such ultra-reliable repetition would indicate a bot). Evaluating resilience to such attacker developments has not been attempted. It would require the development of a taxonomy of AI-enabled attacks for authentication systems and an experimental methodology to ensure rigorous evaluation across its categories. Furthermore, such attacks are, at heart, mimicry attacks, and mimicry is an established collaborative robot concept. For example, training by (human) use is an active research area in the collaborative robot field. So, enhanced authentication mimicry may well take advantage of ideas in mimicry from more general collaborative robotic research. AI-enabled attacks are likely to assume increasing importance and their exploration is left as future work.

6.4 The Future of Behaviour-based User Authentication for Physical Human–Robot Interaction (HRI)

This thesis has shown three aspects of how continuous user authentication can be deployed in robotic and remote operations. First, the techniques we have investigated are promising. Second, these techniques can form the basis for reliable, unobtrusive and continuous authentication. We believe that approaches such as presented herein have a significant potential to play a part in enhancing robot security. Finally, we believe that this is the first thesis focused on continuous user authentication to robotic technology, and we recommend this field to the research community.

Bibliography

[1] Abo-Zahhad, M., Ahmed, S. M., and Abbas, S. N. Biometric authentication based on pcg and ecg signals: present status and future directions. *Signal, Image and Video Processing 8*, 4 (2014), 739–751.

[2] Acar, A., Aksu, H., Uluagac, A. S., and Akkaya, K. Waca: Wearable-assisted continuous authentication. *arXiv preprint arXiv:1802.10417* (2018).

[3] Agatonovic-Kustrin, S., and Beresford, R. Basic concepts of artificial neural network (ann) modeling and its application in pharmaceutical research. *Journal of pharmaceutical and biomedical analysis 22*, 5 (2000), 717–727.

[4] Agrawal, R., Srikant, R., et al. Fast algorithms for mining association rules. In *Proc. 20th int. conf. very large data bases, VLDB* (1994), vol. 1215, Citeseer, pp. 487–499.

[5] Alemzadeh, H., Raman, J., Leveson, N., Kalbarczyk, Z., and Iyer, R. K. Adverse events in robotic surgery: a retrospective study of 14 years of fda data. *PloS one 11*, 4 (2016), e0151470.

[6] Alotaibi, S., Alruban, A., Furnell, S., and Clarke, N. L. A novel behaviour profiling approach to continuous authentication for mobile applications. In *ICISSP* (2019), pp. 246–251.

[7] Alqarni, M. A., Chauhdary, S. H., Malik, M. N., Ehatisham-ul Haq, M., and Azam, M. A. Identifying smartphone users based on how they interact with their phones. *Human-centric Computing and Information Sciences 10*, 1 (2020), 1–14.

[8] Amin, R., Gaber, T., ElTaweel, G., and Hassanien, A. E. Biometric and traditional mobile authentication techniques: Overviews and open issues. In *Bio-inspiring cyber security and cloud services: trends and innovations*. Springer, 2014, pp. 423–446.

[9] Anderson, G., and Anderson, G. *The economic impact of technology infrastructure for advanced robotics*. US Department of Commerce, National Institute of Standards and Technology, 2016.

[10] Aschenbrenner, D., Fritscher, M., Sittner, F., Krauss, M., and Schilling, K. Teleoperation of an industrial robot in an active production line. *IFAC-PapersOnLine 48*, 10 (2015), 159–164.

[11] Ashibani, Y., and Mahmoud, Q. H. A behavior profiling model for user authentication in iot networks based on app usage patterns. In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society* (2018), IEEE, pp. 2841–2846.

[12] Aslam, M. U., Derhab, A., Saleem, K., Abbas, H., Orgun, M., Iqbal, W., and Aslam, B. A survey of authentication schemes in telecare medicine information systems. *Journal of medical systems 41*, 1 (2017), 14.

[13] Aumi, M. T. I., and Kratz, S. Airauth: evaluating in-air hand gestures for authentication. In *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services* (2014), ACM, pp. 309–318.

[14] Avgousti, S., Christoforou, E. G., Panayides, A. S., Voskarides, S., Novales, C., Nouaille, L., Pattichis, C. S., and Vieyres, P. Medical telerobotic systems: current status and future trends. *Biomedical engineering online 15*, 1 (2016), 1–44.

[15] Aviv, A. J., Gibson, K. L., Mossop, E., Blaze, M., and Smith, J. M. Smudge attacks on smartphone touch screens. *Woot 10* (2010), 1–7.

[16] Bača, M., Grd, P., and Fotak, T. *Basic principles and trends in hand geometry and hand shape biometrics.* INTECH Open Access Publisher, 2012.

[17] Banala, S. K., Kim, S. H., Agrawal, S. K., and Scholz, J. P. Robot assisted gait training with active leg exoskeleton (alex). *IEEE transactions on neural systems and rehabilitation engineering 17*, 1 (2008), 2–8.

[18] Bao, G., Pan, L., Fang, H., Wu, X., Yu, H., Cai, S., Yu, B., and Wan, Y. Academic review and perspectives on robotic exoskeletons. *IEEE Transactions on Neural Systems and Rehabilitation Engineering 27*, 11 (2019), 2294–2304.

[19] Barandas, M., Folgado, D., Fernandes, L., Santos, S., Abreu, M., Bota, P., Liu, H., Schultz, T., and Gamboa, H. Tsfel: Time series feature extraction library. *SoftwareX 11* (2020), 100456.

[20] Bauer, W., Bender, M., Braun, M., Rally, P., and Scholtz, O. Lightweight robots in manual assembly—best to start simply. *Examining companies' initial experiences with lightweight robots, Stuttgart* (2016), 1–32.

[21] Bensid, K., Samai, D., Laallam, F. Z., and Meraoumia, A. Deep learning feature extraction for multispectral palmprint identification. *Journal of Electronic Imaging 27*, 3 (2018), 033018.

[22] Bergstra, J., and Bengio, Y. Random search for hyper-parameter optimization. *Journal of machine learning research 13*, 2 (2012).

[23] Berrar, D. Cross-validation. In *Encyclopedia of Bioinformatics and Computational Biology*, S. Ranganathan, M. Gribskov, K. Nakai, and C. Schönbach, Eds. Academic Press, Oxford, 2019, pp. 542–545.

[24] Bhatt, S., and Santhanam, T. Keystroke dynamics for biometric authentication—a survey. In *Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on* (2013), IEEE, pp. 17–23.

[25] Bhattacharyya, D., Ranjan, R., Alisherov, F., Choi, M., et al. Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology 2*, 3 (2009), 13–28.

[26] Blum, A., and Mitchell, T. Combining labeled and unlabeled data with co-training. In *Proceedings of the eleventh annual conference on Computational learning theory* (1998), ACM, pp. 92–100.

[27] Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T., and Chizeck, H. J. To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. *arXiv preprint arXiv:1504.04339* (2015).

[28] Bonaci, T., Yan, J., Herron, J., Kohno, T., and Chizeck, H. J. Experimental analysis of denial-of-service attacks on teleoperated robotic systems. In *Proceedings of the ACM/IEEE sixth international conference on cyber-physical systems* (2015), pp. 11–20.

[29] Bonneau, J., Herley, C., Oorschot, P. C. v., and Stajano, F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Tech. rep., University of Cambridge, Computer Laboratory, 2012.

[30] Bonneau, J., and Preibusch, S. The password thicket: Technical and market failures in human authentication on the web. In *WEIS* (2010).

[31] Bošnjak, L., and Brumen, B. Shoulder surfing: From an experimental study to a comparative framework. *International Journal of Human-Computer Studies 130* (2019), 1–20.

[32] Bours, P. Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report 17*, 1-2 (2012), 36–43.

[33] Bours, P., and Mondal, S. Performance evaluation of continuous authentication systems. *IET Biometrics 4*, 4 (2015), 220–226.

[34] Burge, M. J., and Bowyer, K. *Handbook of iris recognition.* Springer Science & Business Media, 2013.

[35] Buriro, A., Crispo, B., Delfrari, F., and Wrona, K. Hold and sign: A novel behavioral biometrics for smartphone user authentication. In *2016 IEEE Security and Privacy Workshops (SPW)* (2016), IEEE, p. 276–285.

[36] Cai, J., Luo, J., Wang, S., and Yang, S. Feature selection in machine learning: A new perspective. *Neurocomputing 300* (2018), 70–79.

[37] Caruso, L., Russo, R., and Savino, S. Microsoft kinect v2 vision system in a manufacturing application. *Robotics and Computer-Integrated Manufacturing 48* (2017), 174–181.

[38] Centeno, M. P., van Moorsel, A., and Castruccio, S. Smartphone continuous authentication using deep learning autoencoders. In *2017 15th Annual Conference on Privacy, Security and Trust (PST)* (2017), IEEE, p. 147–1478.

[39] Cerrudo, C., and Apa, L. Hacking robots before skynet1. *IOActive Website* (2017).

[40] Chen, R.-C., Dewi, C., Huang, S.-W., and Caraka, R. E. Selecting critical features for data classification based on machine learning methods. *Journal of Big Data 7* (2020), 1–26.

[41] Cheng, L., and Tavakoli, M. Covid-19 pandemic spurs medical telerobotic systems: A survey of applications requiring physiological organ motion compensation. *Frontiers in Robotics and AI 7* (2020).

[42] Choi, P. J., Oskouian, R. J., and Tubbs, R. S. Telesurgery: past, present, and future. *Cureus 10*, 5 (2018).

[43] Claesen, M., and De Moor, B. Hyperparameter search in machine learning. *arXiv preprint arXiv:1502.02127* (2015).

[44] Clarke, N. *Transparent user authentication: biometrics, RFID and behavioural profiling.* Springer Science & Business Media, 2011.

[45] Cobot Sales Will Reach $5.6bn by 2027, Driven by Growth in Non-Manufacturing Applications , `https://www.interactanalysis.com/cobot-sales-will-reach-5-6bn-by-2027-driven-by-growth`, Accessed 2022-9-20.

[46] Colgate, J. E., Edward, J., Peshkin, M. A., and Wannasuphoprasit, W. Cobots: Robots for collaboration with human operators, 1996.

[47] Collaborative Robot Market by Component, Payload (Up to 5 Kg, 5-10 Kg, and Above 10 Kg), Application (Handling, Processing), Industry (Automotive, Furniture & Equipment), and Region (2021-2027), `https://www.marketsandmarkets.com/market-reports/collaborative-robot-market-194541294.html`, accessed: 2022-09-10.

[48] Collaborative Robot Market is Charging at 40 % CAGR, https://statzon.com/insights/global-collaborative-robot-market-is-forecasted-to-reach-2-3bn-by-2025, accessed: 2022-09-20.

[49] Collaborative Robot Market Analysis, https://www.coherentmarketinsights.com/market-insight/collaborative-robot-market-4667, accessed 2022-9-10.

[50] Collaborative Robots Market Size, Share & Trends Analysis Report By Payload Capacity, By Application (Assembly, Handling, Packaging, Quality Testing), By Vertical, By Region, And Segment Forecasts, 2022 - 2030, https://www.grandviewresearch.com/industry-analysis/collaborative-robots-market, accessed: 2022-09-11.

[51] Connor, P., and Ross, A. Biometric recognition by gait: A survey of modalities and features. *Computer Vision and Image Understanding 167* (2018), 1–27.

[52] Craig, J., and Petterson, V. Introduction to the practice of telemedicine. *Journal of telemedicine and telecare 11*, 1 (2005), 3–9.

[53] Dahia, G., Jesus, L., and Pamplona Segundo, M. Continuous authentication using biometrics: An advanced review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 10*, 4 (2020), e1365.

[54] Das, K., and Behera, R. N. A survey on machine learning: concept, algorithms and applications. *International Journal of Innovative Research in Computer and Communication Engineering 5*, 2 (2017), 1301–1309.

[55] DeCann, B., and Ross, A. Relating roc and cmc curves via the biometric menagerie. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on* (2013), IEEE, pp. 1–8.

[56] IFR Positioning Paper demystifying collaborative industrial robots. https://ifr.org/papers/demystifying-collaborative-industrial-robots-updated-version, accessed: 2021-12-8.

[57] Dennis, S. A., Goodson, B. M., and Pearson, C. A. Online worker fraud and evolving threats to the integrity of mturk data: A discussion of virtual private servers and the limitations of ip-based screening procedures. *Behavioral Research in Accounting 32*, 1 (2020), 119–134.

[58] Doroz, R., Porwik, P., and Orczyk, T. Dynamic signature verification method based on association of features with similarity measures. *Neurocomputing 171* (2016), 921–931.

[59] Dravenstott, R. E., Krzeminski, B., and Martinez, L. Pin creation system and method, Apr. 26 2016. US Patent 9,324,076.

[60] Drummond, C., and Holte, R. C. Cost curves: An improved method for visualizing classifier performance. *Machine learning 65*, 1 (2006), 95–130.

[61] Eberz, S., Lovisotto, G., Rasmussen, K. B., Lenders, V., and Martinovic, I. 28 blinks later: Tackling practical challenges of eye movement biometrics. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (2019), pp. 1187–1199.

[62] Eberz, S., Rasmussen, K. B., Lenders, V., and Martinovic, I. Looks like eve: Exposing insider threats using eye movement biometrics. *ACM Transactions on Privacy and Security (TOPS) 19*, 1 (2016), 1–31.

[63] Ekso bionics. `https://eksobionics.com/`, accessed 2021-12-01.

[64] El-Bendary, N., Al-Qaheri, H., Zawbaa, H. M., Hamed, M., Hassanien, A. E., Zhao, Q., and Abraham, A. Hsas: Heart sound authentication system. In *Nature and Biologically Inspired Computing (NaBIC), 2010 Second World Congress on* (2010), IEEE, pp. 351–356.

[65] Exoskeleton market with covid-19 impact by type (powered, passive), component (hardware, software), mobility, body part (lower extremities, upper extremities, full body), vertical (healthcare, defense, industrial) and region - global forecast to 2026, 2021. `https://www.marketsandmarkets.com/Market-Reports/exoskeleton-market-40697797.html`, accessed 2021-12-01.

[66] Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., and Schclar, A. User identity verification via mouse dynamics. *Information Sciences 201* (2012), 19–36.

[67] Feldhofer, M. An authentication protocol in a security layer for rfid smart tags. In *Electrotechnical Conference, 2004. MELECON 2004. Proceedings of the 12th IEEE Mediterranean* (2004), vol. 2, IEEE, pp. 759–762.

[68] Feng, H., Fawaz, K., and Shin, K. G. Continuous authentication for voice assistants. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking* (2017), pp. 343–355.

[69] Fiddy, H. O. Method and system for defeat of replay attacks against biometric authentication systems, Aug. 13 2013. US Patent 8,508,338.

[70] Föll, S., Maritsch, M., Spinola, F., Mishra, V., Barata, F., Kowatsch, T., Fleisch, E., and Wortmann, F. Flirt: A feature generation toolkit for wearable data. *Computer Methods and Programs in Biomedicine 212* (2021), 106461.

[71] IFR forecast ifr presents world robotics 2021 reports. `https://https://https://ifr.org/ifr-press-releases/news/robot-sales-rise-again`, accessed 2021-12-01.

[72] Frank, M., Biedert, R., Ma, E., Martinovic, I., and Song, D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security 8*, 1 (2012), 136–148.

[73] Freese, M., Singh, S., Ozaki, F., and Matsuhira, N. Virtual robot experimentation platform v-rep: a versatile 3d robot simulator. In *International Conference on Simulation, Modeling, and Programming for Autonomous Robots* (2010), Springer, pp. 51–62.

[74] Fridman, L., Stolerman, A., Acharya, S., Brennan, P., Juola, P., Greenstadt, R., and Kam, M. Multi-modal decision fusion for continuous authentication. *Computers & Electrical Engineering 41* (2015), 142–156.

[75] Fridman, L., Weber, S., Greenstadt, R., and Kam, M. Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location. *IEEE Systems Journal 11*, 2 (2016), 513–521.

[76] Gafurov, D. A survey of biometric gait recognition: Approaches, security and challenges. In *Annual Norwegian computer science conference* (2007), Annual Norwegian Computer Science Conference Norway, pp. 19–21.

[77] Genuer, R., Poggi, J.-M., and Tuleau-Malot, C. Variable selection using random forests. *Pattern recognition letters 31*, 14 (2010), 2225–2236.

[78] Géron, A. *Hands-on machine learning with Scikit-Learn and TensorFlow: concepts, tools, and techniques to build intelligent systems.* " O'Reilly Media, Inc.", 2017.

[79] Gleirscher, M., Johnson, N., Karachristou, P., Calinescu, R., Law, J., and Clark, J. Challenges in the safety-security co-assurance of collaborative industrial robots. *arXiv preprint arXiv:2007.11099* (2020).

[80] Gonzalez-Manzano, L., Fuentes, J. M. D., and Ribagorda, A. Leveraging user-related internet of things for continuous authentication: A survey. *ACM Computing Surveys (CSUR) 52*, 3 (2019), 1–38.

[81] Goodrich, M. A., and Schultz, A. C. *Human-robot interaction: a survey.* Now Publishers Inc, 2008.

[82] Gopura, R., Bandara, D., Kiguchi, K., and Mann, G. K. Developments in hardware systems of active upper-limb exoskeleton robots: A review. *Robotics and Autonomous Systems 75* (2016), 203–220.

[83] Gopura, R., Kiguchi, K., and Bandara, D. A brief review on upper extremity robotic exoskeleton systems. In *2011 6th international Conference on Industrial and Information Systems* (2011), IEEE, pp. 346–351.

[84] Granitto, P. M., Furlanello, C., Biasioli, F., and Gasperi, F. Recursive feature elimination with random forest for ptr-ms analysis of agroindustrial products. *Chemometrics and Intelligent Laboratory Systems 83*, 2 (2006), 83–90.

[85] Grau Saldes, A., Indri, M., Lo Bello, L., and Sauter, T. Industrial robotics in factory automation: From the early stage to the internet of things. In *IECON 2017: 43rd IEEE Annual Conference of the IEEE Industrial Electronics Society: China National Convention Center, Beijing, China, 29, October-01 November, 2017: proceedings* (2018), Institute of Electrical and Electronics Engineers (IEEE), pp. 6159–6164.

[86] Guest, R. Age dependency in handwritten dynamic signature verification systems. *Pattern Recognition Letters 27*, 10 (2006), 1098–1104.

[87] MEET THE COBOTS "human-safe" collaborative robots. `https://cobotsguide.com/cobots/`. accessed: 2021-09-18.

[88] Gupta, B., Tewari, A., Jain, A. K., and Agrawal, D. P. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications 28*, 12 (2017), 3629–3654.

[89] Haas, S., Ulz, T., and Steger, C. Secured offline authentication on industrial mobile robots using biometric data. In *Proceedings of the RoboCup International Symposium 2017* (2017).

[90] Hadid, A., Evans, N., Marcel, S., and Fierrez, J. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. *IEEE Signal Processing Magazine 32*, 5 (2015), 20–30.

[91] Halonen, T. Authentication and authorization in mobile environment. In *Tik-110.501 Seminar on Network Security* (2000), Citeseer.

[92] Hamdan, M. M., and Mahmoud, M. S. Control of teleoperation systems in the presence of cyber attacks: A survey. *IAES International Journal of Robotics and Automation 10*, 3 (2021), 235.

[93] Hentout, A., Aouache, M., Maoudj, A., and Akli, I. Human–robot interaction in industrial collaborative robotics: a literature review of the decade 2008–2017. *Advanced Robotics 33*, 15-16 (2019), 764–799.

[94] Hietanen, A., Pieters, R., Lanz, M., Latokartano, J., and Kämäräinen, J.-K. Ar-based interaction for human-robot collaborative manufacturing. *Robotics and Computer-Integrated Manufacturing 63* (2020), 101891.

[95] Hirakawa, Y., Kogure, Y., and Ohzeki, K. A password authentication method tolerant to video-recording attacks analyzing multiple authentication operations. *International Journal of Computer Science and Electronic Engineering (IJCSEE) 3* (2015), 356–360.

[96] Huang, L., Meng, Z., Deng, Z., Wang, C., Li, L., and Zhao, G. Robot behavior-based user authentication for motion-controlled robotic systems. In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (2021), IEEE, pp. 1–6.

[97] Idrus, S. Z. S., Cherrier, E., Rosenberger, C., and Bours, P. Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords. *Computers & Security 45* (2014), 147–155.

[98] Idrus, S. Z. S., Cherrier, E., Rosenberger, C., and Schwartzmann, J.-J. A review on authentication methods. *Australian Journal of Basic and Applied Sciences 7*, 5 (2013), 95–107.

[99] Jain, A., Maltoni, D., Maio, D., and Wayman, J. Biometric systems technology, design and performance evaluation. *Springer-Verlag London limited, 2005* (2005).

[100] Jain, A. K., Duin, R. P. W., and Mao, J. Statistical pattern recognition: A review. *IEEE Transactions on pattern analysis and machine intelligence 22*, 1 (2000), 4–37.

[101] Jain, A. K., Nandakumar, K., and Nagar, A. Biometric template security. *EURASIP Journal on advances in signal processing 2008* (2008), 1–17.

[102] Jain, A. K., Ross, A., and Prabhakar, S. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology 14*, 1 (2004), 4–20.

[103] Kaczmarek, T., Ozturk, E., and Tsudik, G. Assentication: user de-authentication and lunchtime attack mitigation with seated posture biometric. In *International Conference on Applied Cryptography and Network Security* (2018), Springer, pp. 616–633.

[104] Kaiser, J., and Reed, W. Data smoothing using low-pass digital filters. *Review of Scientific Instruments 48*, 11 (1977), 1447–1457.

[105] Kataria, A. N., Adhyaru, D. M., Sharma, A. K., and Zaveri, T. H. A survey of automated biometric authentication techniques. In *2013 Nirma university international conference on engineering (NUiCONE)* (2013), IEEE, pp. 1–6.

[106] Khalid, A., Kirisci, P., Ghrairi, Z., Thoben, K., and Pannek, J. Towards implementing safety and security concepts for human-robot collaboration in the context of industry 4.0. In *39th International MATADOR Conference on Advanced Manufacturing (Manchester, UK)* (2017), pp. 0–7.

[107] Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K.-D., and Pannek, J. Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry 97* (2018), 132–145.

[108] Khan, A. A. Preventing phishing attacks using one time password and user machine identification. *arXiv preprint arXiv:1305.2704* (2013).

[109] Khan, H., Hengartner, U., and Vogel, D. Targeted mimicry attacks on touch input based implicit authentication schemes. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services* (2016), pp. 387–398.

[110] Khan, H., Hengartner, U., and Vogel, D. Mimicry attacks on smartphone keystroke authentication. *ACM Transactions on Privacy and Security (TOPS) 23*, 1 (2020), 1–34.

[111] Khan, M. A., Arya, Y., and Agarwal, G. Security enhancement of recall based graphical authentication system by using biometric features. *International Journal of Computer Applications 128*, 7 (2015).

[112] Kim, D., Lee, J., Yoon, H.-S., and Cha, E.-Y. A non-cooperative user authentication system in robot environments. *IEEE Transactions on Consumer electronics 53*, 2 (2007).

[113] Kim, J., Kim, H., and Kang, P. Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection. *Applied Soft Computing 62* (2018), 1077–1087.

[114] Kinnunen, T., and Li, H. An overview of text-independent speaker recognition: From features to supervectors. *Speech communication 52*, 1 (2010), 12–40.

[115] Knapik, J. J., Reynolds, K. L., and Harman, E. Soldier load carriage: historical, physiological, biomechanical, and medical aspects. *Military medicine 169*, 1 (2004), 45–56.

[116] Kot, T., and Novák, P. Application of virtual reality in teleoperation of the military mobile robotic system taros. *International journal of advanced robotic systems 15*, 1 (2018), 1729881417751545.

[117] Kumar, R., Phoha, V. V., and Jain, A. Treadmill attack on gait-based authentication systems. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)* (2015), IEEE, pp. 1–7.

[118] Kumari, P., and Vaish, A. Brainwave based user identification system: A pilot study in robotics environment. *Robotics and Autonomous Systems 65* (2015), 15–23.

[119] Lal, N. A., Prasad, S., and Farik, M. A review of authentication methods. *International Journal of Scientific & Technology Research 4*, 8 (2015), 246–249.

[120] Lammi, H.-K. Ear biometrics. *Lappeenranta University of Technology* (2004).

[121] Latha, U., and Rameshkumar, K. A study on attacks and security against fingerprint template database. *International Journal of Emerging Trends & Technology in Computer Science 2*, 5 (2013).

[122] Lee, H., Kim, W., Han, J., and Han, C. The technical trend of the exoskeleton robot system for human power assistance. *International Journal of Precision Engineering and Manufacturing 13*, 8 (2012), 1491–1497.

[123] Li, Y., Hu, H., and Zhou, G. Using data augmentation in continuous authentication on smartphones. *IEEE Internet of Things Journal 6*, 1 (2018), 628–640.

[124] Liang, J., Yu, G., and Guo, L. Human-robot collaborative semi-autonomous teleoperation with force feedback. In *2018 5th International Conference on Soft Computing & Machine Intelligence (ISCMI)* (2018), IEEE, pp. 129–134.

[125] Liang, Y., Samtani, S., Guo, B., and Yu, Z. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. *IEEE Internet of Things Journal 7*, 9 (2020), 9128–9143.

[126] Lichiardopol, S. A survey on teleoperation. *Technische Universitat Eindhoven, DCT report 20* (2007), 40–60.

[127] Lin, P.-L., Weng, L.-T., and Huang, P.-W. Graphical passwords using images with random tracks of geometric shapes. In *Image and Signal Processing, 2008. CISP'08. Congress on* (2008), vol. 3, IEEE, pp. 27–31.

[128] Maggi, F., Quarta, D., Pogliani, M., Polino, M., Zanchettin, A. M., and Zanero, S. Rogue robots: Testing the limits of an industrial robot's security. *Trend Micro, Politecnico di Milano, Tech. Rep* (2017).

[129] Mahfouz, A., Mahmoud, T. M., and Eldin, A. S. A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications 37* (2017), 28–37.

[130] Maier, J., et al. Made smarter—review 2017. *Department for Business EIS. The Stationery Office. London* (2017).

[131] Mansfield, A., Wayman, J., for Mathematics, N. P. L. C., and Kingdom);, S. C. G. B. Best practices in testing and reporting performance of biometric devices. *NPL Report CMSC 14(02)* (2002).

[132] Marsland, S. *Machine learning: an algorithmic perspective.* Chapman and Hall/CRC, 2011.

[133] Mason, J. E., Traoré, I., and Woungang, I. Gait biometric recognition. In *Machine Learning Techniques for Gait Biometric Recognition.* Springer, 2016, pp. 9–35.

[134] Mason, J. E., Traoré, I., and Woungang, I. *Machine Learning Techniques for Gait Biometric Recognition.* Springer, 2016.

[135] Masupha, L., Zuva, T., and Ngwira, S. A review of gait recognition techniques and their challenges. In *Third international conference on digital information processing, e-business and cloud computing* (2015), pp. 63–69.

[136] Maurice, P., Malaisé, A., Amiot, C., Paris, N., Richard, G.-J., Rochel, O., and Ivaldi, S. Human movement and ergonomics: An industry-oriented dataset for collaborative robotics. *The International Journal of Robotics Research 38*, 14 (2019), 1529–1537.

[137] Mawashi. `https://mawashi.net/en/fraco-exoskeleton-by-mawashi-alias`, accessed 2021-12-01.

[138] Mjaaland, B. B., Bours, P., and Gligoroski, D. Walk the walk: Attacking gait biometrics by imitation. In *International Conference on Information Security* (2010), Springer, pp. 361–380.

[139] Mokaram, S., Aitken, J. M., Martinez-Hernandez, U., Eimontaite, I., Cameron, D., Rolph, J., Gwilt, I., McAree, O., and Law, J. A ros-integrated api for the kuka lbr iiwa collaborative robot. *IFAC-PapersOnLine 50*, 1 (2017), 15859–15864.

[140] Mondal, S., and Bours, P. Continuous authentication using mouse dynamics. In *Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the* (2013), IEEE, pp. 1–12.

[141] Mondal, S., and Bours, P. Continuous authentication in a real world settings. In *2015 eighth international conference on advances in pattern recognition (ICAPR)* (2015), IEEE, pp. 1–6.

[142] Muaaz, M., and Mayrhofer, R. Smartphone-based gait recognition: From authentication to imitation. *IEEE Transactions on Mobile Computing 16*, 11 (2017), 3209–3221.

[143] Murphy, A. Intro: Robotics outlook 2025. `https://loupventures.com/intro-robotics-outlook-2025/`, accessed 2021-12-01.

[144] Musale, P., Baek, D., Werellagama, N., Woo, S. S., and Choi, B. J. You walk, we authenticate: lightweight seamless authentication based on gait in wearable iot systems. *IEEE Access 7* (2019), 37883–37895.

[145] Nickel, C., Wirtl, T., and Busch, C. Authentication of smartphone users based on the way they walk using k-nn algorithm. In *2012 Eighth international conference on intelligent information hiding and multimedia signal processing* (2012), IEEE, pp. 16–20.

[146] Nikose, S., and Meena, H. K. Ear-biometrics for human identification. In *2020 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)* (2020), IEEE, pp. 8–13.

[147] Noonee. `https://www.noonee.com/?lang=en`, accessed 2021-12-01.

[148] of Robotics, I. F. Robots and the workplace of the future. *International Federation of Robotics, Frankfurt, Germany* (2018).

[149] O'Gorman, L. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE 91*, 12 (2003), 2021–2040.

[150] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., and Koucheryavy, Y. Multi-factor authentication: A survey. *Cryptography 2*, 1 (2018), 1.

[151] Papavasileiou, I., Qiao, Z., Zhang, C., Zhang, W., Bi, J., and Han, S. Gaitcode: Gait-based continuous authentication using multimodal learning and wearable sensors. *Smart Health 19* (2021), 100162.

[152] Park, A. J., and Kazman, R. N. Augmented reality for mining teleoperation. In *Telemanipulator and Telepresence Technologies* (1995), vol. 2351, International Society for Optics and Photonics, pp. 119–129.

[153] Patel, S., Paul, I., Astekar, M. S., Ramesh, G., and Sowmya, G. A study of lip prints in relation to gender, family and blood group. *International journal of oral and maxillofacial pathology 1*, 1 (2010), 4–7.

[154] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos, A., Cournapeau, D., Brucher, M., Perrot, M., and Duchesnay, E. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research 12* (2011), 2825–2830.

[155] Peshkin, M., and Colgate, J. E. Cobots. *Industrial Robot: An International Journal 26*, 5 (1999), 335–341.

[156] Petsas, T., Tsirantonakis, G., Athanasopoulos, E., and Ioannidis, S. Two-factor authentication: is the world ready?: quantifying 2fa adoption. In *Proceedings of the eighth european workshop on system security* (2015), ACM, p. 4.

[157] Phan, D.-T., Dam, N. N.-T., Nguyen, M.-P., Tran, M.-T., and Truong, T.-T. Smart kiosk with gait-based continuous authentication. In *International Conference on Distributed, Ambient, and Pervasive Interactions* (2015), Springer, pp. 188–200.

[158] Phillips, P. J., Martin, A., Wilson, C. L., and Przybocki, M. An introduction evaluating biometric systems. *Computer 33*, 2 (2000), 56–63.

[159] Quarta, D., Pogliani, M., Polino, M., Maggi, F., Zanchettin, A. M., and Zanero, S. An experimental security analysis of an industrial robot controller. In *2017 38th IEEE Symposium on Security and Privacy (SP)* (2017), IEEE, pp. 268–286.

[160] Rabkin, A. Personal knowledge questions for fallback authentication: Security questions in the era of facebook. In *Proceedings of the 4th symposium on Usable privacy and security* (2008), ACM, pp. 13–23.

[161] Raza, M., Iqbal, M., Sharif, M., and Haider, W. A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal 19*, 4 (2012), 439–444.

[162] Redd, L. V. K. Lip prints: An overview in forensic dentistry. *Journal of Advanced Oral Research 2*, 1 (2011), 17–20.

[163] Rehmat, N., Zuo, J., Meng, W., Liu, Q., Xie, S. Q., and Liang, H. Upper limb rehabilitation using robotic exoskeleton systems: a systematic review. *International Journal of Intelligent Robotics and Applications 2*, 3 (2018), 283–295.

[164] Riel, A., Kreiner, C., Macher, G., and Messnarz, R. Integrated design for tackling safety and security challenges of smart products and digital manufacturing. *CIRP annals 66*, 1 (2017), 177–180.

[165] Roberts, C. Biometric attack vectors and defences. *Computers & Security 26*, 1 (2007), 14–25.

[166] Robla-Gómez, S., Becerra, V. M., Llata, J. R., Gonzalez-Sarabia, E., Torre-Ferrero, C., and Perez-Oria, J. Working together: A review on safe human-robot collaboration in industrial environments. *IEEE Access 5* (2017), 26754–26773.

[167] Robot simulator coppeliasim: create, compose, simulate, any robot coppelia robotics. `https://www.coppeliarobotics.com/`, accessed 2021-12-01.

[168] Rognon, C., Mintchev, S., Dell'Agnola, F., Cherpillod, A., Atienza, D., and Floreano, D. Flyjacket: An upper body soft exoskeleton for immersive drone control. *IEEE Robotics and Automation Letters 3*, 3 (2018), 2362–2369.

[169] Rosenberg, C., Hebert, M., and Schneiderman, H. Semi-supervised self-training of object detection models. In *WACV/MOTION* (2005), pp. 29–36.

[170] Ross, A., and Jain, A. K. Multimodal biometrics: An overview. In *Signal Processing Conference, 2004 12th European* (2004), IEEE, pp. 1221–1224.

[171] Sabhanayagam, T., Venkatesan, V. P., and Senthamaraikannan, K. A comprehensive survey on various biometric systems. *International Journal of Applied Engineering Research 13*, 5 (2018), 2276–2297.

[172] Sahoo, S. K., Choubisa, T., and Prasanna, S. M. Multimodal biometric person authentication: A review. *IETE Technical Review 29*, 1 (2012), 54–75.

[173] Saltzer, J. H. Protection and the control of information sharing in multics. *Communications of the ACM 17*, 7 (1974), 388–402.

[174] Sánchez, P. M. S., Celdrán, A. H., Maimó, L. F., Pérez, G. M., and Wang, G. Securing smart offices through an intelligent and multi-device continuous authentication system. In *International Conference on Smart City and Informatization* (2019), Springer, pp. 73–85.

[175] Santhosh, N., Mathew, D., and Thomas, A. Person verification using multimodal biometric system. In *Computer Communication and Informatics (ICCCI), 2017 International Conference on* (2017), IEEE, pp. 1–5.

[176] Saraswathi, T., Mishra, G., Ranganathan, K., et al. Study of lip prints. *Journal of forensic dental sciences 1*, 1 (2009), 28.

[177] Sarohi, H. K., and Khan, F. U. Graphical password authentication schemes: current status and key issues. *Int. j. eng. innovative technol.(ijeit) 10*, 2 (2013).

[178] Seha, S., Papangelakis, G., Hatzinakos, D., Zandi, A. S., and Comeau, F. J. Improving eye movement biometrics using remote registration of eye blinking patterns. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (2019), IEEE, pp. 2562–2566.

[179] Serwadda, A., and Phoha, V. V. When kids' toys breach mobile phone security. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (2013), pp. 599–610.

[180] Sharma, A., Belwal, R. C., Ojha, V., and Agarwal, G. Password based authentication: Philosophical survey. In *Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on* (2010), vol. 3, IEEE, pp. 619–622.

[181] Shen, C., Cai, Z., and Guan, X. Continuous authentication for mouse dynamics: A pattern-growth approach. In *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012)* (2012), IEEE, pp. 1–12.

[182] Sherman, M., Clark, G., Yang, Y., Sugrim, S., Modig, A., Lindqvist, J., Oulasvirta, A., and Roos, T. User-generated free-form gestures for authentication: Security and memorability. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services* (2014), ACM, pp. 176–189.

[183] Sherwani, F., Asad, M. M., and Ibrahim, B. Collaborative robots and industrial revolution 4.0 (ir 4.0). In *2020 International Conference on Emerging Trends in Smart Technologies (ICETST)* (2020), IEEE, pp. 1–5.

[184] Singh, N., Agrawal, A., and Khan, R. Voice biometric: A technology for voice based authentication. *Adv. Sci 10* (2018), 1–6.

[185] Srivastava, H. A comparison based study on biometrics for human recognition. *IOSR Journal of Computer Engineering (IOSR-JCE) Volume 15* (2013), 22–29.

[186] Stanciu, V.-D., Spolaor, R., Conti, M., and Giuffrida, C. On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks. In *proceedings of the sixth ACM conference on data and application security and privacy* (2016), pp. 105–112.

[187] Stylios, I., Kokolakis, S., Thanou, O., and Chatzis, S. Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Information Fusion 66* (2021), 76–99.

[188] Suitx. https://www.suitx.com, accessed 2021-12-01.

[189] Sujatha, E., and Chilambuchelvan, A. Multimodal biometric authentication algorithm using iris, palm print, face and signature with encoded dwt. *Wireless Personal Communications 99*, 1 (2018), 23–34.

[190] Sun, H.-M., Chen, S.-T., Yeh, J.-H., and Cheng, C.-Y. A shoulder surfing resistant graphical authentication system. *IEEE Transactions on Dependable and Secure Computing 15*, 2 (2016), 180–193.

[191] Suo, X., Zhu, Y., and Owen, G. S. Graphical passwords: A survey. In *Computer security applications conference, 21st annual* (2005), IEEE, pp. 10–pp.

[192] Szepesvári, C. Algorithms for reinforcement learning. *Synthesis lectures on artificial intelligence and machine learning 4*, 1 (2010), 1–103.

[193] Tabassi, E., Watson, C., Fiumara, G., Salamon, W., Flanagan, P., and Cheng, S. L. Performance evaluation of fingerprint open-set identification algorithms. In *Biometrics (IJCB), 2014 IEEE International Joint Conference on* (2014), IEEE, pp. 1–8.

[194] Teresko, J. Here come the cobots. https://www.industryweek.com/technology-and-iiot/automation/article/21938640/here-come-the-cobots, accessed 2021-12-01.

[195] Tey, C. M., Gupta, P., and Gao, D. I can be you: Questioning the use of keystroke dynamics as biometrics. In *Annual Network and Distributed System Security Symposium 20th NDSS 2013, 24-27 February* (2013).

[196] The e-glove basic. https://www.emphasisnet.gr/e-glove/, accessed 2021-09-18.

[197] Towhidi, F., and Masrom, M. A survey on recognition based graphical user authentication algorithms. *arXiv preprint arXiv:0912.0942* (2009).

[198] Tripathi, K. A comparative study of biometric technologies with reference to human interface. *International Journal of Computer Applications 14*, 5 (2011), 10–15.

[199] Tuscano, A., and Koshy, T. S. Types of keyloggers technologies–survey. In *ICCCE 2020*. Springer, 2021, pp. 11–22.

[200] Uludag, U., and Jain, A. K. Attacks on biometric systems: a case study in fingerprints. In *Security, Steganography, and Watermarking of Multimedia Contents VI* (2004), vol. 5306, International Society for Optics and Photonics, pp. 622–634.

[201] van der Vorm, J., Nugent, R., and O'Sullivan, L. Safety and risk management in designing for the lifecycle of an exoskeleton: a novel process developed in the robo-mate project. *Procedia Manufacturing 3* (2015), 1410–1417.

[202] Van Tilborg, H. C., and Jajodia, S. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.

[203] Velásquez, I., Caro, A., and Rodríguez, A. Kontun: A framework for recommendation of authentication schemes and methods. *Information and Software Technology* (2017).

[204] Villani, V., Pini, F., Leali, F., and Secchi, C. Survey on human–robot collaboration in industrial settings: Safety, intuitive interfaces and applications. *Mechatronics* (2018).

[205] Villani, V., Pini, F., Leali, F., and Secchi, C. Survey on human–robot collaboration in industrial settings: Safety, intuitive interfaces and applications. *Mechatronics 55* (2018), 248–266.

[206] Virtanen, P., Gommers, R., Oliphant, T. E., Haberland, M., Reddy, T., Cournapeau, D., Burovski, E., Peterson, P., Weckesser, W., Bright, J., van der Walt, S. J., Brett, M., Wilson, J., Millman, K. J., Mayorov, N., Nelson, A. R. J., Jones, E., Kern, R., Larson, E., Carey, C. J., Polat, İ., Feng, Y., Moore, E. W., VanderPlas, J., Laxalde, D., Perktold, J., Cimrman, R., Henriksen, I., Quintero, E. A., Harris, C. R., Archibald, A. M., Ribeiro, A. H., Pedregosa, F., van Mulbregt, P., and SciPy 1.0 Contributors. SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python. *Nature Methods 17* (2020), 261–272.

[207] Vojić, S. Applications of collaborative industrial robots. *Machines. Technologies. Materials. 14*, 3 (2020), 96–99.

[208] Walsh, C. J., Endo, K., and Herr, H. A quasi-passive leg exoskeleton for load-carrying augmentation. *International Journal of Humanoid Robotics 4*, 03 (2007), 487–506.

[209] Xu, W., Shen, Y., Luo, C., Li, J., Li, W., and Zomaya, A. Y. Gait-watch: A gait-based context-aware authentication system for smart watch via sparse coding. *Ad Hoc Networks 107* (2020), 102218.

[210] Yaacoub, J.-P., Noura, H., Salman, O., and Chehab, A. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things 11* (2020), 100218.

[211] Yaacoub, J.-P. A., Noura, H. N., Salman, O., and Chehab, A. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security* (2021), 1–44.

[212] Yampolskiy, R. V. Human computer interaction based intrusion detection. In *Fourth International Conference on Information Technology (ITNG'07)* (2007), IEEE, pp. 837–842.

[213] Yang, Y., Guo, B., Wang, Z., Li, M., Yu, Z., and Zhou, X. Behavesense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. *Ad Hoc Networks 84* (2019), 9–18.

[214] Yfantis, E. A., and Fayed, A. Authentication and secure robot communication. *International Journal of Advanced Robotic Systems 11*, 2 (2014), 10.

[215] Zaki, M. J. Scalable algorithms for association mining. *IEEE transactions on knowledge and data engineering 12*, 3 (2000), 372–390.

[216] Zhang, C., Zhou, Y., Guo, J., Wang, G., and Wang, X. Research on classification method of high-dimensional class-imbalanced datasets based on svm. *International Journal of Machine Learning and Cybernetics 10*, 7 (2019), 1765–1778.

[217] Zhang, Y., Hu, W., Xu, W., Chou, C. T., and Hu, J. Continuous authentication using eye movement response of implicit visual stimuli. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 1*, 4 (2018), 177.

[218] Zhao, X., Feng, T., and Shi, W. Continuous mobile authentication using a novel graphic touch gesture feature. In *2013 IEEE sixth international conference on biometrics: theory, applications and systems (BTAS)* (2013), IEEE, pp. 1–6.

[219] Zhong, Y., Deng, Y., and Meltzner, G. Pace independent mobile gait biometrics. In *2015 IEEE 7th international conference on biometrics theory, applications and systems (BTAS)* (2015), IEEE, pp. 1–8.

[220] Zhu, X., and Goldberg, A. B. Introduction to semi-supervised learning. *Synthesis lectures on artificial intelligence and machine learning 3*, 1 (2009), 1–130.

Appendices

Appendix A

More Results

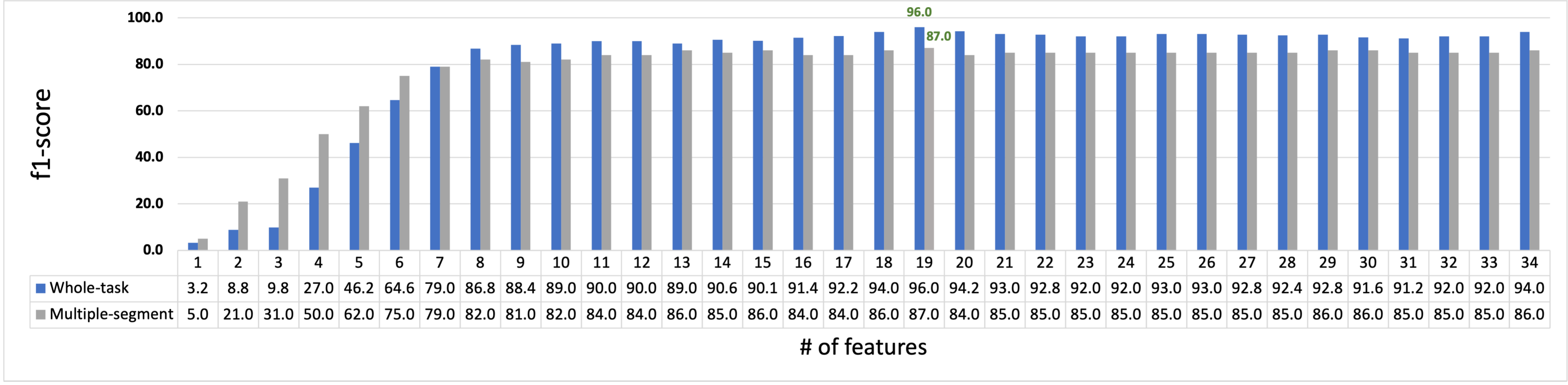
A.1 Chapter 3: User Authentication for Collaborative Robots

Table A.1 shows the features that were used in the experiment. Figure A.1 shows the results for a various number of features (i.e. from 1 to 34). In Chapter 3, the best average f1-score was obtained using 19 features.

Several ML techniques results (using Time Series Feature Extraction Library TSFEL) are reported in tableA.2.

Table A.1: List of features ordered from most important to least important using the RFE selection approach.

Feature NO	Feature	Feature NO	Feature
1	Time	18	ToolTorque_M_Mean
2	ToolForce_x_STD	19	ToolTorque_M_STD
3	ToolForce_x_SKEW	20	ToolForce_M_KURTOSIS
4	ToolForce_y_STD	21	ToolForce_z_SKEW
5	ToolForce_z_Mean	22	ToolForce_y_SKEW
6	ToolForce_z_STD	23	ToolForce_x_KURTOSIS
7	ToolForce_z_KURTOSIS	24	ToolTorque_y_STD
8	ToolForce_M_Mean	25	ToolForce_M_STD
9	ToolForce_M_SKEW	26	ToolTorque_M_KURTOSIS
10	ToolTorque_x_Mean	27	ToolForce_y_KURTOSIS
11	ToolTorque_y_Mean	28	ToolTorque_x_SKEW
12	ToolTorque_y_SKEW	29	ToolForce_x_Mean
13	ToolTorque_y_KURTOSIS	30	ToolTorque_x_STD
14	ToolTorque_z_Mean	31	ToolForce_y_Mean
15	ToolTorque_z_STD	32	ToolTorque_M_SKEW
16	ToolTorque_z_SKEW	33	ToolTorque_x_KURTOSIS
17	ToolTorque_z_KURTOSIS	34	Task_No



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
■ Whole-task	3.2	8.8	9.8	27.0	46.2	64.6	79.0	86.8	88.4	89.0	90.0	90.0	89.0	90.6	90.1	91.4	92.2	94.0	96.0	94.2	93.0	92.8	92.0	92.0	93.0	93.0	92.8	92.4	92.8	91.6	91.2	92.0	92.0	94.0
■ Multiple-segment	5.0	21.0	31.0	50.0	62.0	75.0	79.0	82.0	81.0	82.0	84.0	84.0	86.0	85.0	86.0	84.0	84.0	86.0	87.0	84.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	85.0	86.0	86.0	85.0	85.0	85.0	86.0

Figure A.1: The optimal number of features.

Table A.2: Results using several ML techniques: using Time Series Feature Extraction Library TSFEL.

Classifier	Experiment	Statistical features				Temporal features				Spectral features				All features			
		f1_score	TAR	FAR	EER	f1_score	TAR	FAR	EER	f1_score	TAR	FAR	EER	f1_score	TAR	FAR	EER
SVM	whole-task	82.67%	83.51%	0.57%	1.10%	76.67%	76.44%	0.81%	1.57%	33.49%	31.77%	2.35%	4.55%	29.51%	27.55%	2.49%	4.82%
	Multiple-segment	68.26%	67.14%	1.13%	2.19%	38.28%	38.81%	2.11%	4.08%	45.68%	44.33%	1.92%	3.71%	60.26%	58.71%	1.42%	2.75%
KNN	whole-task	74.06%	73.69%	0.91%	1.75%	65.54%	63.77%	1.25%	2.41%	33.89%	32.44%	2.32%	4.50%	34.14%	30.44%	2.40%	4.64%
	Multiple-segment	61.61%	61.85%	1.32%	2.54%	22.19%	22.71%	2.67%	5.15%	43.72%	44.87%	1.90%	3.67%	54.63%	55.40%	1.53%	2.97%
LR	whole-task	83.46%	83.51%	0.56%	1.10%	77.42%	78.44%	0.74%	1.44%	44.22%	43.11%	1.96%	3.79%	39.32%	38.66%	2.11%	4.09%
	Multiple-segment	64.77%	65.59%	1.19%	2.29%	41.99%	43.00%	1.97%	3.80%	54.95%	56.56%	1.49%	2.89%	71.71%	72.07%	0.96%	1.86%
LDA	whole-task	89.40%	89.74%	0.36%	0.68%	90.76%	91.11%	0.31%	0.59%	35.23%	35.11%	2.23%	4.32%	35.91%	36.22%	2.19%	4.25%
	Multiple-segment	75.13%	75.31%	0.85%	1.65%	64.65%	65.05%	1.21%	2.33%	67.35%	67.36%	1.13%	2.17%	69.51%	69.54%	1.05%	2.03%

Table A.3: Results for 16 users performing 15 tasks after 40 days.

User Id	# of Accepted tasks	# of Rejected tasks
1	14	1
2	8	7
3	15	0
6	8	7
11	15	0
12	15	0
14	15	0
16	14	1
17	12	3
19	13	2
20	15	0
21	15	0
23	15	0
24	15	0
25	10	5
27	15	0

A.2 Chapter 4: User Authentication in a Wearable Sensor System

Table A.4: Results using several ML techniques.

Classifier	Experiment	f1_score	TAR	FAR	EER
SVM	WSF	74.57%	70.24%	2.48%	4.56%
	WST	54.16%	52.33%	3.96%	7.33%
KNN	WSF	85.44%	85.64%	1.22%	2.24%
	WST	50.34%	50.66%	4.12%	7.58%
LR	WSF	90.76%	91.28%	0.74%	1.36%
	WST	70.00%	70.26%	2.48%	4.56%
LDA	WSF	92.04%	92.28%	0.66%	1.20%
	WST	70.55%	70.76%	2.46%	4.47%

Table A.5: Evaluation of RF classifier before and after using Lfilter over each experiment.

Experiment	Method	f1_score	TAR	FAR	EER
WSF	No filter	98.96%	98.96%	0.08%	0.16%
	Lfilter	99.40%	99.5%	0.04%	0.08%
WST	No filter	88.12%	88.32%	0.98%	1.78%
	Lfilter	88.40%	88.38%	0.96%	1.8%

A.3 Chapter 5 User Authentication in Human-Robot Tele-operation Systems

Table A.6: Results using several ML techniques

Classifier	Experiment	f1_score	TAR	FAR	EER
KNN	time-based	72.57%	73.06%	26.93%	24.16%
	point-based	76.63%	77.23%	22.77%	22.13%
LR	time-based	89.64%	89.11%	10.89%	9.68%
	point-based	87.80%	87.86%	12.14%	11.78%
LDA	time-based	87.35%	87.42%	12.58%	12.31%
	point-based	87.51%	87.11%	12.88%	11.75%