DEPARTMENT OF INFORMATION ENGINEERING AND COMPUTER SCIENCE

ICT International Doctoral School

Next-Generation User Authentication Schemes For IoT Applications

Sandeep Gupta

SUBMITTED TO THE DEPARTMENT OF INFORMATION ENGINEERING AND COMPUTER SCIENCE (DISI) IN THE PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

Advisor
Prof. Bruno Crispo,
Università degli Studi di Trento, Italy.

Examiners
Prof. Simone Fischer-Hübner,
Karlstads University, Sweden.

Dr. Kimmo Halunen,
VTT Technical Research Centre, Finland.

27 October 2020

Abstract

The unprecedented rise of IoT has revolutionized every business vertical enthralling people to embrace IoT applications in their day-to-day lives to accrue multifaceted benefits. It is absolutely fair to say that a day without connected IoT systems, such as smart devices, smart enterprises, smart homes or offices, etc., would hamper our conveniences, drastically. Many IoT applications for these connected systems are safety-critical, and any unauthorized access could have severe consequences to their consumers and society.

In the overall IoT security spectrum, human-to-machine authentication for IoT applications is a critical and foremost challenge owing to highly prescriptive characteristics of conventional user authentication schemes, i.e., knowledge-based or token-based authentication schemes, currently used in them. Furthermore, studies have reported numerous users' concerns, from both the security and usability perspectives, that users are facing in using available authentication schemes for IoT applications. Therefore, an impetus is required to upgrade user authentication schemes for new IoT age applications to address any unforeseen incidents or unintended consequences.

This dissertation aims at designing next-generation user authentication schemes for IoT applications to secure connected systems, namely, smart devices, smart enterprises, smart homes, or offices. To accomplish my research objectives, I perform a thorough study of ways and types of user authentication mechanisms emphasizing their security and usability ramifications. Subsequently, based on the substantive findings of my studies, I design, prototype, and validate our proposed user authentication schemes. I exploit both physiological and behavioral biometrics to design novel schemes that provide implicit (*frictionless*), continuous (*active*) or risk-based (*non-static*) authentication for multi-user scenarios. Afterward, I present a comparative analysis of the proposed schemes in terms of accuracy against the available state-of-the-art user authentication solutions. Also, I conduct SUS surveys to evaluate the usability of user authentication schemes.

Keywords
IoT, User Authentication Schemes, Biometrics, Security, Usability

Acknowledgement

Undertaking this research work proved to be an apt experience of learning and understanding the latest cybersecurity trends and landscapes. Without the uninterrupted guidance and unfailing support of many wonderful people, this would not have been doable. I am highly indebted to all of them for being a part of my Ph.D. journey and contributing to making it realizable.

First and foremost, I express my sincere gratitude to my thesis advisor *Prof. Bruno Crispo* for the research advice, continuous guidance, and encouragement throughout my Ph.D. studies and other research-related activities. I would also like to thank my thesis reviewers, *Prof. Simone Fischer-Hübner* and *Dr. Kimmo Halunen*, for their precise and constructive feedback with unstinting support in improving my thesis.

My special thanks to the European Union's Horizon 2020 research and innovation programme to sponsor this excellent innovative training network for early-stage researchers (ESR) under NeCS ETN H2020 – Marie Sklodowska Curie actions. I heartily, convey my thanks to *Prof. Fabio Martinelli*, all the consortium members, and other ESRs to establish a competitive nexus and conducive environment for the research activities.

I would like to equally thank the volunteers for testing our prototype applications and the co-authors of our publications for their honest efforts and stimulating discussions to make our collaborative research possible. I am also grateful to friends, colleagues, professors, and staff at the University of Trento, for imparting their knowledge and support.

Finally, my heartfelt gratitude, appreciation, and thanks to my family for their unswerving support and continuous motivation throughout my years of studies. The love and blessings of my parents have been a privilege that inspired me to move forward in life. I profoundly, thanks to my beloved wife *Neha*, and my adorable daughter *Aanya* for their unconditional trust and endless patience lead to this remarkable accomplishment.

Sandeep Gupta
Trento, Italy
October 28, 2020

To
my lovely family
and my wonderful teachers.

Contents

List of Tables

List of Figures

List of Acronyms

BSIF	Binarized Statistical Image Features
DTW	Dynamic Time Warping
EBT	Ensemble Bagged Tree
EER	Equal Error Rate
FAR	False Acceptance Rate
FISHERC	Fisher's Least Square Linear Discriminant
FRR	False Rejection Rate
HPF	High Pass Filter
IGAE	Information Gain Attribute Evaluator
IoT	Internet of Things
LDC	Linear Discriminant Classifier
LPF	Low Pass Filter
KBA	Knowledge-based Authentication
KNN	K-Nearest Neighbors
MITM	Man-in-the-Middle
MITPC/Phone	Man-in-the-PC/Phone
MFCC	Mel Frequency Cepstral Coefficients
NB	Naive Bayes
NN	NeuralNet
OTP	One Time Passcode
PbD	Privacy-by-Design
PCA	Principal Component Analysis
RBFS	Relief-based feature selection
RF	Random Forest
ROC	Receiver Operating Characteristics
ROI	Region of Interest
SSO	Single Sign-on
STATSVC	Stats support vector classifier
SUS	System Usability Scale
SVM	Support Vector Machine
TAR	True Acceptance Rate
TBA	Token-based Authentication
TRR	True Rejection Rate

Chapter 1

Introduction

> *"User authentication for IoT (Internet of Things) applications is not a trifle. Without any stupefaction, user authentication is a primary defense mechanism to secure IoT applications. Nonetheless, it is a fundamental building block for most types of Human-to-Machine accountability principles and access-control methods."*

IoT applications for smart devices, smart homes or offices, smart enterprises, etc., have become an epicenter of our lives. From online banking or shopping to door access, taxi ride-bookings, and so on, everything literally revolves around IoT applications to accomplish our day-to-day activities. It sounds fascinating but yet unnerving owing to highly prescriptive characteristics of conventional user authentication schemes that foster wanton disconcert for security among the users of IoT applications [92].

Biometrics, naturally, come as a first choice to instigate sophisticated security solutions capable of overcoming drawbacks present in conventional user authentication schemes [132]. Our next-generation user authentication schemes exploit biometrics to leverage novel solutions that profoundly bring the balance between the security and usability requirements for IoT applications.

1.1 The Problem

A threat to IoT applications in any circumstances or events with the potential to adversely impact their end-users is blatantly perturbing. Undeniably, usable security for IoT applications is today's unprecedented demand, and an impetus is required to design next-generation user authentication schemes for them.

- IoT applications touch on nearly every aspect of our lives, offering: 1) sensitive activities such as online banking and shopping, 2) business operations such as the on-demand ride and share applications, or 3) security management of smart homes or offices. Any cyber-threat will bring unfavorable consequences to their users lacking robust user authentication schemes.

- User authentication schemes that are widely provided by smart devices (e.g., smartphones, tablets, smart-watches, etc.), smart homes and offices (e.g., door access system, etc.), or smart enterprises (e.g., driverless, on-demand ride and ride-sharing taxis, etc.), require an upgrade. As studies have shown that user authentication mechanisms deployed in them have several security issues, and they can be easily exploitable by attacks such as random-, mimicry-, insider-, social-engineering-, and spoofing-attacks.

- Typically, IoT applications are used by both experts and non-experts (negligible information technology knowledge) people. Therefore, usability must be incorporated into user authentication mechanisms.

- Also, the form factor and usage pattern are equally responsible for making knowledge- or token-based user authentication schemes unsuitable to deploy them for IoT applications.

1.2 The Solutions

Our next-generation user authentication schemes exploit biometrics by leveraging both physiological and behavioral human traits to achieve usable security solutions for IoT applications. The schemes are designed for multi-user authentication scenarios incorporating a risk-based or continuous verification approach that can be easily deployed for client-server infrastructures. We also perform a security and usability assessment for our proposed user authentication schemes.

Hold & Tap is a risk-driven one-shot-cum-continuous for IoT applications that strengthens the widely used PIN/password-based authentication technology by giving flexibility to users to enter any random 8-digit alphanumeric text, instead of pre-configured PIN/Passwords. Our scheme authenticates users based on their invisible tap-timings and hand-movements during the application sign-in process and then *continuously* monitors risk to safeguard the entire user session of sensitive applications.

Step & Turn offers a secure and usable user authentication scheme for smart homes or offices to secure door access to the authorized users. The scheme exploits users' single footsteps and hand-movements by taking the benefit of their implicit body actions.

DriverAuth and RiderAuth are risk-based user authentication schemes for smart enterprises such as on-demand rides and driverless taxis, respectively, strengthening the security and safety of their customers. DriverAuth utilizes three biometric modalities, i.e., swipe, *text-independent* voice, and face, in a multi-modal fashion to verify the identity of driver-partners at the time of ride-booking to minimize the threat(s) posed by illegitimate, fake or malicious drivers. RiderAuth is a proposal for a real-time rider authentication system to verify the customers before allowing them the rides to foster safety and security to their customers and the general public.

1.3 Innovative Aspects

1.3.1 Motivation

Biometrics involves measuring individual body characteristics, such as a face, fingerprints, and behavioral patterns, such as voice-prints, hand-movements, touch-strokes that can be used to identify a legitimate person more intricately in contrast to the conventional authentication schemes. Motivations for this research work are as follows:
(i) To design next-generation user authentication schemes for IoT applications by using multi-modal biometrics that can address the safety and security of their users, unerringly.
(ii) To design a risk-based and/or continuous authentication approaches that can protect the entire user-session while users can execute their desired activities, confidently.
(iii) To assert the usability, performance, scalability, maintainability, and robustness against the attacks such as random-, mimicry-, insider-attacks, etc, of our user authentication schemes.
By doing so, the motivation is to cultivate the knowledge that can be applied to similar problem IoT applications for improving user authentication schemes.

1.3.2 Challenges

The important research challenges that we tackled in designing authentication schemes for IoT applications are as follows:

- Identification of suitable biometric modalities that can be collected easily and efficiently fulfilling criterion as covered in Section 2.4.2.

- Availability of inexpensive biometric sensors that can accurately and efficiently acquire and recognize biometric patterns sustainable over a long period.
- User authentication schemes design to be compliant with the CIA triad, i.e., Confidentiality, Integrity, and Availability, to ensure the physical, logical, and perceptual security of users' biometric data.
- User authentication schemes minimize the ominous presence of risk and offer continuous authentication that can improve the security and usability paradigm.
- To bridge gaps in quality attributes such as usability, security, performance, and reliability, etc., to achieve robust user authentication systems.

1.3.3 Contributions

The recent explosive growth of IoT applications as a result of technological advances such as connected IoT systems availability, information processing capabilities, and widespread data connectivity is noteworthy.

Numerous IoT applications for smart devices allow users to access sensitive systems and confidential data anytime, anywhere. PINs and passwords are still widely used user authentication mechanism in a large number of security-sensitive IoT applications, despite the inherent weaknesses [19].

HOLD & TAP provides an enjoyable and satisfying experience by giving the flexibility to enter random alphanumeric text to access security-sensitive applications. Although, behind the scene, users' invisible tap-timings and hand-movements are exploited to secure access to IoT applications.

STEP & TURN can contribute to simplifying access to authorized persons for smart homes, and offices smart by providing on-the-go next-generation user authentication system. We introduce these conveniences by amalgamating three technologies: biometrics, IoT devices, and machine learning.

The meteoric rise of IoT-driven smart enterprises has revolutionized the transportation market rapidly, with their on-demand ride or ride-sharing services and driverless taxis. Alone, Uber, Lyft, and Ola are providing approximately, 20 million rides per day worldwide [56, 57, 58]. Unfortunately, rider's assault or abuse incidents by fake or malicious drivers are surfacing every now and again [22, 274]. DRIVERAUTH can contribute to curbing unforeseen incidents by deploying risk-based multi-modal biometric-based user authentication in on-demand ride and ride-sharing services for proactive verification of driver-partners before allocating the new ride assignments to them.

Similarly, driverless vehicles (e.g., Waymo) as Transportation-As-A-Service is inevitable in the coming years. However, unsupervised physical access to riders in driverless taxis may lead to unexpected safety and security risks. RIDERAUTH - a proposal for rider authentication can address potential risks that may materialize as a consequence customers' diversified motivations like curiosity, monetary benefits, malicious intentions, or terrorism [50].

1.4 Thesis Structure

The structure of the thesis is as follows:

1.4.1 Chapter 2

The chapter put forward relevant information to understand the need for next-generation user authentication schemes for IoT applications. It discusses the different ways and types of authentication mechanisms. Authentication ways refer to the common modalities used to authenticate humans, while authentication types refer to different authentication mechanisms, e.g., one-shot, multi-factor, continuous, multimodal, etc., utilizing these modalities. It presents design goals for usable security and usability evaluation methods. Eventually, describe the biometric recognition system and performance metrics for reporting validation results for our authentication schemes.

1.4.2 Chapter 3

This chapter apprises readers with IoT fact sheet, IoT architecture, and challenges in user authentication available for them, to understand the need for next-generation user authentication schemes for IoT applications.

1.4.3 Chapter 4

The chapter presents HOLD & TAP that is a risk-driven one-shot-cum-continuous behavioral biometric-based user authentication scheme for IoT applications. The scheme can be seamlessly integrated into the existing PIN/password-based authentication schemes to enhance their usability and security. It discusses the threat model, proposed scheme, architecture, validation, and usability assessment of our proposed system.

1.4.4 Chapter 5

The chapter presents STEP & TURN that is a novel bimodal behavioral biometric-based authentication system based on two natural human actions, i.e., single footstep and hand-movement. This scheme can be easily deployed to secure smart homes or offices access to their authorized users. It describes the experimental setup and hardware details of the

STEP & TURN user authentication system. It covers the methodology for system validation including data collection, features extraction, and features selection and the usability assessment of STEP & TURN user authentication system.

1.4.5 Chapter 6

The chapter presents DRIVERAUTH - a novel risk-based multi-modal authentication scheme that exploits three biometric modalities, i.e., swipe gestures, *text-independent* voice and face, to make the on-demand ride and ride-sharing services secure and safer for riders. It covers the problems in the existing driver registration process and the risk involved in on-demand ride and ride-sharing services and it explains the need for risk-based user verification method along with the considered threat model.

1.4.6 Chapter 7

The chapter presents a study for RIDERAUTH - a proposal for biometric-based secure and usable riders authentication schemes for driverless taxis. It discusses the motivation for the need for rider authentication for driverless taxis. Subsequently, the survey results are analyzed to study rider authentication requirements followed by the proposal for a rider authentication framework that uses physiological and behavioral biometric traits.

1.4.7 Chapter 8

The chapter concludes the thesis and covers the possible future work emerging from this work.

1.5 Summary

This chapter is an introduction to our research work on next-generation user authentication schemes for IoT applications. We briefly familiarised readers with the user authentication problems for IoT applications and presented the synopses of our solutions followed by a discussion on the innovative aspects of our research work.

In the next chapter, we give an overview of user authentication schemes and biometric-based authentication system design.

Chapter 2

Background

This chapter familiarizes readers with user authentication schemes, usable security concepts, biometric recognition system design, and performance metrics for their evaluation.

Some sections of this chapter are published in [92]: *Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. "Demystifying authentication concepts in smartphones: Ways and types to secure access." Mobile Information Systems, Volume 2018, Article ID 2649598, 16 pages, Hindawi, 2018*.

2.1 Introduction

In recent years, a large number of IoT applications for smart devices, smart homes or offices, on-demand rides, and driverless taxis, etc., have boomed for the benefit of our lives. With such an unprecedented rise of IoT applications, our work towards next-generation user authentication schemes is of utmost significance in the interest of their users.

2.1.1 Chapter Organization

The rest of the chapter is organized as follows: Section 2.2 presents the possible Ways and Types of user authentication mechanisms. The Ways refers to the common modalities used to authenticate humans, while the Types refers to different authentication mechanisms, e.g., one-shot, multi-factor, continuous, multimodal, etc., utilizing these modalities. Section 2.2 discusses design goals for usable security, and usability evaluation methods. Section 2.4 and 2.5 describe biometric recognition system and performance metrics for reporting validation results for our authentication schemes.

2.2 User Authentication Schemes

By and large, authentication schemes for IoT applications can be envisaged in multitudinous *Ways* and *Types* to authenticate their users [92]. Section 2.2.1 and 2.2.2 cover *Ways* and *Types* of user authentication respectively, with their compendious security and usability analysis.

2.2.1 Ways of User Authentication

The Ways, in which, humans can be authenticated are broadly categorized into three groups, i.e., “Something You Know”, “Something You Have”, and “Something You Are”, as depicted in Figure 2.1.

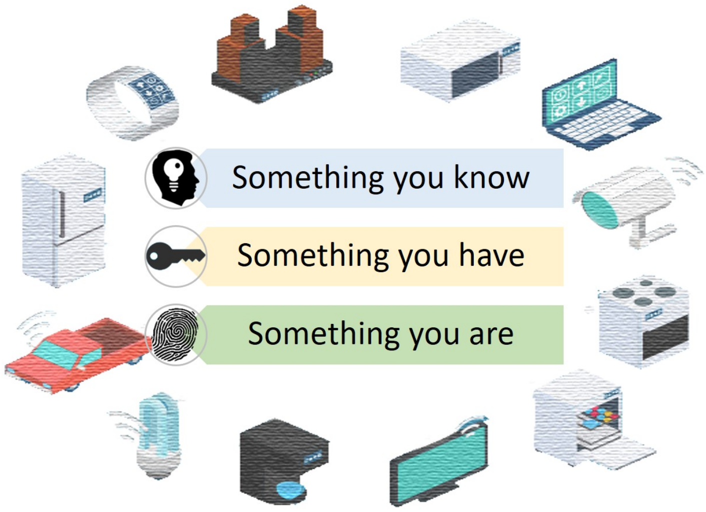


Figure 2.1: Ways to authenticate humans.

2.2.1.1 Something You Know

Something You Know or *Knowledge-based Authentication* (KBA) schemes are based on some sort of secret that users enter at the time of registration and they need to re-enter the same to sign-in the system later. PINs (Figure 2.2a), graphical passwords (Figure 2.2b), and password (Figure 2.2c), are among the most widely used KBA schemes.

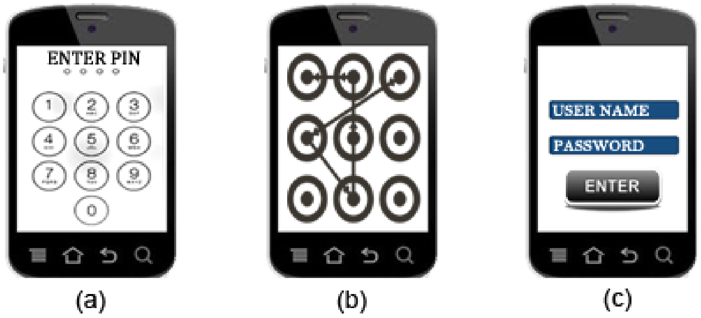


Figure 2.2: (a) PIN, (b) Graphical pattern, and (c) Password.

According to a web-report [275], average smart devices users get themselves engaged in 76 separate sessions, while heavy users (the top 10%) peaked to 132 sessions per day. PIN/passwords, and graphical patterns, require users to memorize their text, they had set earlier, to unlock their devices, every time they need to initiate the session (76 times a day). The capacity of the human brain to process information varies from person to person [46]. Zhang et al. [283] found that users faced problems in remembering their passwords and more especially, to memorize and correctly recall numerous passwords. This encouraged users to go for an easy or simple password which is quick to remember [1] but this opens plenty of opportunities for attackers to guess or crack their passwords, easily [8]. When the system enforces stringent password policies, users due to memorability issues [147, 21], allow their browsers or password managers to save their `username/password` information to make future logins easier. However, users trusting their browsers or password managers are more likely to be a victim of a wide variety of attacks [20, 232]. Overall, 82% of end-users are frustrated with managing passwords [15]. Clearly, this indicates the lack of usability, and a result, nearly, 75 million smartphones users in the US do not use any of PIN, pattern, or passwords, because they consider them annoying and an obstacle in quick access to their smartphones [192]

From security perspective, PINs, passwords, are vulnerable to various attacks, e.g., guessing [140], because users choose date of births [20], easier digits (1111, 2222, etc.) [251], to set up their PIN. Alternatively, Android users (40% of them) prefer graphical patterns for device unlocking. But this approach also requires users to remember them, hence users choose simple and less secure patterns, i.e., if a user connects at least four dots without repeating any of them in their patterns, the maximum number of combinations are 389,112 which could be easily cracked by brute-force [227]. Ye at al. [281] managed to crack 95% of 120 unique patterns collected from 215 independent users within just five attempts by recording their smartphone screen, remotely, while they were unlocking their devices. Also, these schemes are more vulnerable to shoulder surfing than textual passwords [247].

Knowledge based authentication schemes are generally used as one-shot, static, or unimodal authentication types (refer Table 2.1), they are prone to several attacks, such as smudge attacks [7], shoulder surfing or observation attacks [140, 244], or dictionary based attacks or rainbow table password attacks [35]. Recently, Mehrnezhad et al. [174] demonstrated the recovery of entered PIN or password from the sensory data collected, while the users were entering their secrets. They installed PINlogger.js - a JavaScript-based side-channel attack, capable of recording motion and orientation sensor streams without requiring any user permission from the user. The attack resulted in 94% accuracy in recovering the correct

PIN in just three rounds of tries. Similarly, Sarkisyan et al. [223] demonstrated an approach to exploit smartwatch motions sensors to recover the entered PINs. They infested smartwatches with malware to get access to the smartwatch's motion sensors and inferred user activities and PINs. In a controlled scenario, authors obtained PINs within 5 guesses with an accuracy of at least 41% using the Random Forest classifier over a dataset of 21 users.

Table 2.1: Synopsis of knowledge-based schemes.

Modalities	Authentication Types	Usability pros and cons indicated	Security solutions or concerns reported
PIN [20, 192, 251], Password [192, 283], Pattern [192, 281]	One-shot, Static, Periodic, Single sign-on, Unimodal	[1, 8, 20, 26, 46, 104, 147, 173, 192, 251, 283]	[7, 35, 140, 174, 223, 227, 232, 244, 247, 251, 281]

2.2.1.2 Something You Have

Something You Have is also referred as *token-based authentication*. Many service providers and financial institutions are offering sensitive services, such as net-banking, e-wallet, and e-commerce, adopting 2-factors authentication, i.e., one-time-passcodes (OTP) along with usual `username/password` for authentication purpose. Service providers usually supply a small security device to each of their users for generating the one-time passcodes.

OTP schemes can be easily implemented on smartphones (Figure 2.3a) which could be sent either via SMS on the registered number or user could generate this OTP offline (Figure 2.3b) on the mobile apps provided by service providers [37, 40, 243]. Additionally, wearable devices (Figure 2.3c) could be used for receiving the OTPs via SMS [229].

As defined in the section 2.2.1.2, smart devices are being utilized for authentication purposes in several sensitive operations by the means of OTP

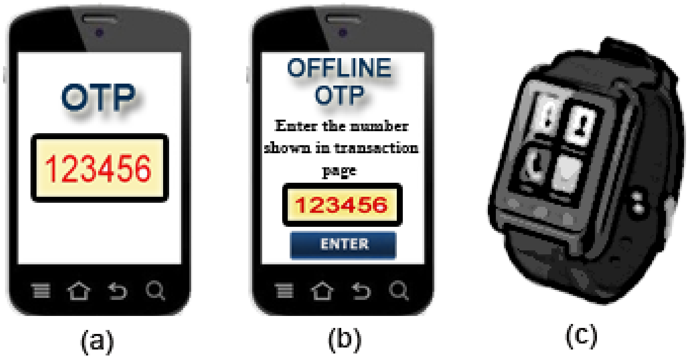


Figure 2.3: (a) One-time passcode (OTP) via SMS, (b) Offline OTP using App, and (c) Paired devices.

via SMS, offline OTP using Apps, or pairing the wearable devices, e.g., smart-watches, smart-glasses, smart-cards, etc. However, this idea of enhancing security with multi-factor authentication, i.e., topping *knowledge based authentication* with *token based authentication* (one-time-passcode), eventually perishes too due to side-channel attacks, e.g., MITM (Man-in-the-Middle), and MITPC/Phone (Man-in-the-PC/Phone) [40]. Software-based OTP solutions also do not guarantee the confidentiality of the generated passwords or the seeds as the mobile OS could be compromised, at the same time, could also suffer from denial-of-service attacks on the account of mobile OS crashes [243].

The adversaries by the means of real-time phishing or intercept attacks could reveal the users' secret information and valid OTP by breaking into their smartphones [37]. Verizon's Data Breach Investigation Report [269] published that the National Institute of Standards and Technology (NIST) listed scenarios involving banking Trojans and malicious code on mobile endpoints as reasons to rule out recommending the users for two-factor authentication via SMS[1]. Seemingly, adversaries can surreptitiously capture second factors delivered by SMS or offline-OTP gen-

[1] https://pages.nist.gov/800-63-3/sp800-63b.html

erated using apps and can reuse them. Secure device pairing schemes allow access to smartphones by pairing it with a trusted Bluetooth device like a smartwatch and use the same to unlock the phone. This concept from the usability point of view is a very elegant solution but not safe from insider attacks or sniffing attacks [2, 77].

Table 2.2: Synopsis of token-based schemes.

Modalities	Authentication Types	Usability pros and cons indicated	Security solutions or concerns reported
OTP [37], Device pairing [2, 11]	Multi-factor, Adaptive, Dynamic, Risk-based	[23, 11, 41, 151, 292]	[2, 40, 77, 37, 243, 269]

Token based authentication (TBA) schemes are used in multi-factor, adaptive, dynamic, and risk-based authentication types (see Table 2.2). Unfortunately, they could not add too much to the usability because the users are required to manage always an additional hardware for the sole purpose of authentication. As a result, Braz [23] gave usability rating 3 (out of 5) to one-time generator acquisition devices. Additionally, Belk mentioned token-based authentication mechanism incurred more cost to users and are comparatively slower [11]. According to a study by Zink and Waldvogel [292], 83.3% of users considered SMS based Transaction Authentication Number is not a usable solution. Another in-depth usability study by Krol et al. [151] evaluated 2-factor authentication on 21 online banking customers (16 among 21 were having multiple accounts with more than one bank). A total of 90 separate login sessions of all the participants were collected meticulously, over a period of 11 days. Their analysis showed that approximately 13.3% faced problems due to mistyped credentials, misplaced token, forgotten credentials, etc.

Another way to authenticate humans under *Something You Have*, i.e., *Insertable Tokens* [109, 240, 137] (see Table 2.3) includes implantable medical devices (IMDs) [108] and emerging technologies such as Bespoke devices [248, 91], Neodymium Magnets [74], NFC or RFID chips [264, 79], smart-piercings [107, 49], smart-tattoos [49] are the newer addition to biometrics that potentially can be used to provide increased usability over the existing solutions [110]. Researches are exploring the further possibilities of insertable tokens as a go-to solution for improving digital security and usability in IoT applications.

Table 2.3: Synopsis of insertable/implantable tokens.

Modalities	Authenti-cation Types	Usability pros and cons indicated	Security solutions or concerns reported
Bespoke devices [248, 91], Neodymium magnet's [74], NFC or RFID chips [264, 79], smart-piercings [107, 49], smart-tattoos [49]	Continuous, Multimodal, Transparent	[110]	Data not available

2.2.1.3 Something You Are

Authentication schemes under *Something You Are* rely on the measurement of users' biometric characteristics and they can be further classified as physiological and behavioral biometrics. Figure 2.4 illustrates the commonly available authentication ways for smartphone users under this category.

Physical traits, i.e., ear, face, fingerprint, and iris, can be collected by hardware like a camera. Similarly, behavioral biometric modalities, such as gait, grip, swipe, pick-up, touch, and voice can be profiled unobtrusively, using various built-in sensors [78], namely, accelerometer, gyroscope, magnetometer, proximity sensor, touch-screens, and microphone.

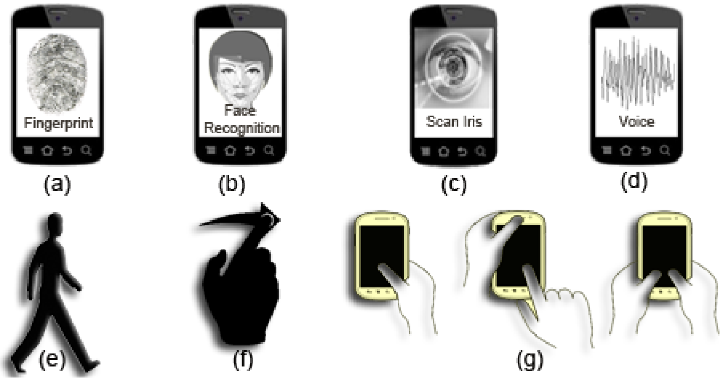


Figure 2.4: (a) Fingerprint, (b) Face, (c) Iris, (d) Voice, (e) Gait, (f) Swipe, and (g) Touch.

Smart devices manufacturers have started embedding sensors in their flagship smartphones for reliable and convenient user authentication with the intuition that biometric approaches are better than their conventional authentication schemes. For example, Apple, Huawei, Lenovo (Motorola), Microsoft (Nokia), Samsung, and many other leading manufacturers have integrated fingerprint sensors, iris scanners, and face recognition algorithms, in some of their high-end devices.

Physiological biometrics e.g., face, fingerprint, iris, eyes, etc., are commonly used modalities for user authentication. Behavioral biometrics, e.g., voice, handwritten signature, keystroke/touch dynamics, gait, and hand-movements are considered as the future of user authentication [121]. According to Jain et al. [132], biometric-based authentication schemes are more secure than other authentication schemes because biometrics cannot be lost or stolen (if used securely) and is harder to be forged. Table 2.4 and 2.5 present the synopsis of existing physiological and behavioral biometric-based schemes.

Evidently, conventional authentication schemes, i.e., PIN, passwords, graphical patterns, are no more considered secure and convenient [104], because they are not able to distinguish between the users, rather they

Table 2.4: Synopsis of physiological biometrics.

Modalities	Authentication Types	Usability pros and cons indicated	Security solutions or concerns reported
Face [150, 252], Eyes [47, 221], Iris [112], Fingerprint [38, 172]	One-shot, Multi-factor, Multimodal	[14, 130, 152, 52, 241, 279]	[38, 18, 112, 132, 150, 172, 175, 209, 235, 252]

Table 2.5: Synopsis of behavioral biometrics.

Modalities	Authentication Types	Usability pros and cons indicated	Security solutions or concerns reported
Touch [33], Keystroke [287], Signature [254], Gait [183, 113, 185], Behavior Profiling [242]	Adaptive, Continuous, Multimodal, Risk-based, Transparent	[33, 47, 48, 142, 194, 199, 242]	[32, 29, 30, 113, 170, 183, 184, 146, 220, 246, 255, 256, 287]

authorize everyone (regardless of whether that person is the legitimate owner of the device or not) who enter the correct credentials. Biometric-based solutions are considered more secure because it is assumed human body traits cannot be shared, copied, lost, or stolen. Moreover, they genuinely authenticate their users by forcing them to present themselves physically to the system. However, studies suggest that no single biometric trait can ideally fit all the scenarios [29, 146, 199].

In our research, we focus to combine biometrics modalities that can be deployed as implicit, continuous or risk-driven authentication schemes to address users' security, safety, and usability concerns for IoT applications [95, 93, 94]. Furthermore, we stitched our schemes to the knowledge-based user authentication schemes as an additional transparent authentication layer that enhances the reliability and usability of the whole authentication process, significantly [32, 33].

2.2.2 Types of User Authentication

Researchers have been investigating the utilization of different ways, i.e., PIN, passwords, OTP, face, touch, voice, etc., to design and develop the different types of authentication schemes. Different authentication types are concisely described as follows:

2.2.2.1 One-shot Authentication

One-shot authentication is a type of authentication mechanism in which a user credentials are verified at the beginning of the session [33, 175, 215]. It is a simple process, where users claim their identity by entering correct credentials or fulfilling the challenges to access a smart device or ecosystem. The session remains valid until the user signs-off or closes the session. For example, PINs, passwords, graphical patterns, fingerprints, face, and voice, are some of the commonly used modalities on smart devices to authenticate users.

Roth et al. [215] discussed the limitations of one-shot authentication, such as short sensing time, inability to rectify decisions, and enabling the access for potentially unlimited periods. Meng et al. [175] introduced the term one-off authentication for one-shot authentication and they concluded that authenticating just once leaves the possibilities for impostors to gain access to the current session and retrieve sensitive information from smart devices.

2.2.2.2 Periodic Authentication

Periodic authentication is simply the variant of "one-shot authentication" in which idle-timeout-duration is set, for closing the session, automatically [13, 72]. If a User remains inactive for more than the idle-timeout-duration, the device locks itself. Bertino et al. [13] defined *periodic authorization* with a mathematical expression "$\{$[begin, end], P, auth$\}$" holding of 3 prime attributes, where 'begin' is authorization-start-date, 'end' is either the constant ∞, or a deauthorization date after the start-date, 'P' is the duration of a session, and 'auth' is an authorization function.

Feng et al. [72] determined that periodic authentication or automatic logouts are more detrimental while one-shot authentication solutions are prone to a wide variety of attacks. Typing an error-free `username and/or password` on a smartphone's keyboard is a tedious task, especially when an average user initiates 76 phone sessions a day [275]. *Single Sign-On* (SSO) has been seen as the solution to the problem.

2.2.2.3 Single Sign-On (SSO) Authentication

Single sign-on (SSO) is a type of long-term or persistent authentication in which users remain signed-on till the time they revoke or terminates the session. In case, the system observes any discrepancy with respect to some fixed attributes, e.g., change in location, network connection, an anomaly in usage pattern, the session is terminated or the user is asked for re-authentication [71, 119, 222].

In an SSO system, users are authenticated to a single Identity Provider (IDP) that acts as a trusted party between the users and multiple service providers (SPs). When a user demand for their authentication, IDP generates a token for that SP asserting the user's identity, and in turn, SP allows the user to access the services [71]. Users can access as many different applications, using SSO, as they what to access, once they are authenticated to the system [222]. SSO can be further divided into the Enterprise Single Sign-On (ESSO) and Reduced Sign-On (RSSO) [119]. ESSO enables users to enter the same id and password to sign into multiple applications within an enterprise domain. RSSO tends to reduce the frequency with which users are prompted to provide credentials after their authentication into a system. Many organizations are willing to reduce the burden of repeated login prompts for users. However, these systems are considered less secure because there could be a curious adversary who can spoof easily, which may result in identity theft.

VMware identity manager provides APIs to implement mobile sign-on authentication for Airwatch-Managed Android devices [270]. Similarly, Google offers G Suite apps for single sign-on for Android devices which can be done by pairing smartphones with smartwatches [89]. *Single Sign-On* (SSO) enables users to sign-in to an app using a single or federated identity, e.g., Facebook, Twitter, Google+, etc., however, misplacing or sharing smart devices or ecosystems inadvertently, could make this concept risky for their users.

2.2.2.4 Multi-Factor Authentication

Multi-factor authentication introduces a concept that combines two or more authentication ways, i.e., email verification, OTP via SMS, phone-call to the predefined numbers, push notification to the paired device, smart-tokens, etc., to the conventional authentication schemes [212, 237, 272]. A common practice is to register a mobile number with service providers and whenever the user accesses that service for sensitive operation, e.g., online-banking, the service provider sends the one-time-passcodes (OTP) via SMS, getting assured that a legitimate user has requested access to that service.

Generally, security experts suggest the use of multi-factor authentication by processing multiple factors, simultaneously, for verification purposes [272]. In multi-factor authentication, commonly a PIN or password is the baseline authentication standard, while more factors can be augmented from a wide variety of available modalities to verify users. Readers can observe in Figure 2.5 that as the number of authentication factors increases the authentication levels are also get added. For in-

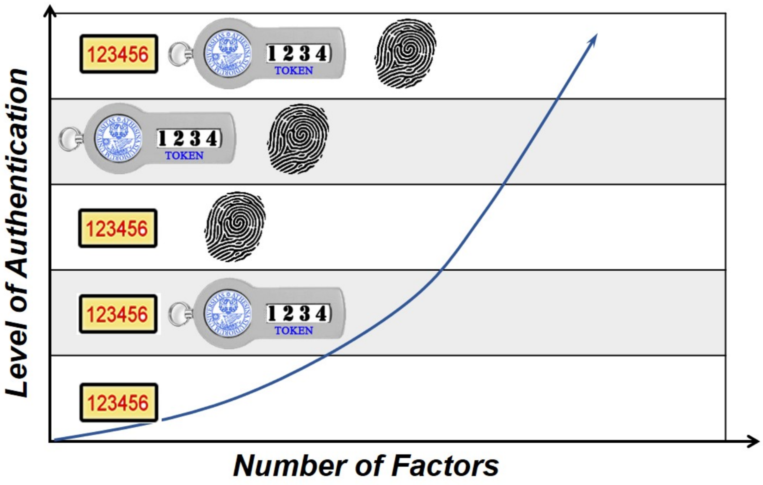


Figure 2.5: Authentication factors [272].

stance, if only PIN is used the authentication level is minimum, but when other factors like tokens and fingerprints are added, the authentication level tends to increase proportionally.

The common mechanism for the secondary authentication can be delivered either by sending SMS to the registered mobile number or can be obtained directly from a secure authenticator mobile app. Other forms of multi-factor authentication involve the use of a smart-card or smart-token entitled to the user, biometrics like the face or fingerprint scans, or a dedicated code generator linked to user's account [212]. This concept is mainly influenced by the notion that not all the authentication factors could be hacked at the same time. Stanislav [237] explained the various technical methods by which two-factor authentication can be implemented.

2.2.2.5 Static and Dynamic Authentication

Static authentication scheme works with a fixed set of challenges, whereas dynamic authentication mechanism capitalizes on a diverse set of pre-stored challenges, every time users unlock their smart devices [211, 255].

Furthermore, static authentication schemes verify the user's identity only at the start of the session like a one-shot authentication scheme, while in case of dynamic authentication users are presented with a variable set of challenges to enable the dynamic scaling of access controls. According to Ren and Wu [211], dynamic authentication utilizes a one-time password derived from the user's password, the authenticating time, and a unique attribute only known to the user.

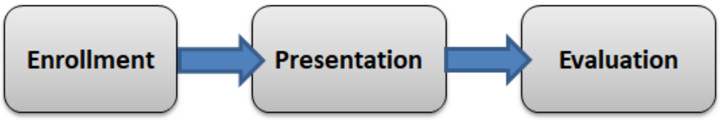


Figure 2.6: Static authentication process [255].

As illustrated in Figure 2.6, a static authentication process like any other authentication types, mainly consists of three steps: enrollment, presentation, and evaluation and the outcome of the evaluation is a binary decision [255]. In the enrollment step, the system generates a feature template by processing the information gathered from the user, profile the feature vectors with the label of the user, and save it for the evaluation or matching. During the presentation step, the system asks the user to confirm her credentials. In the final step, i.e., evaluation, the information was given by the user is compared with the stored templates of the claimed identity. Subsequently, the access is granted or denied as per the match result.

2.2.2.6 Continuous Authentication

Continuous authentication is a mechanism that repeatedly verifies the identity of users for the entire duration of the authorized session [255]. The continuous authentication process dynamically iterates over the three steps throughout the session as illustrated in Figure 2.7. However, these iterations can be event-based or can be adjusted at fixed intervals (pe-

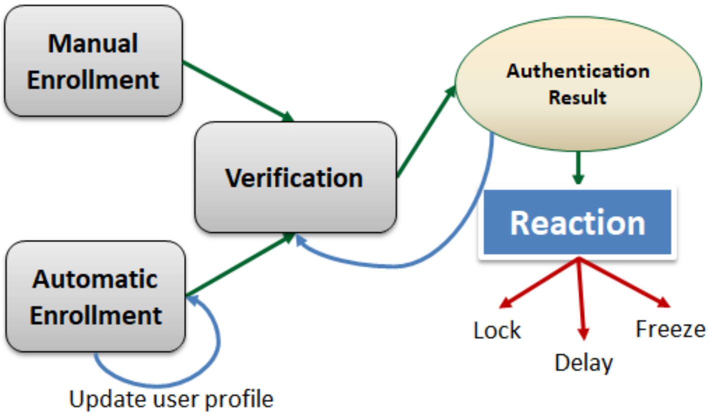


Figure 2.7: Continuous authentication process [255].

riodically) or randomly. If any anomaly is detected by the device, the access to the device is disabled, immediately, and the device asks for explicit re-authentication [72, 80]. In other words, the users are passively and periodically monitored throughout their interactive session with any device or system [194].

This concept seems to promise higher security as compared to the other type of authentication mechanisms, such as *one-shot* authentication, *one-time* authentication, and *periodic* authentication, but at the same time much more complex to implement. Thus, overcoming the limitations of one-shot authentication, where authentication happens only at the time of login and any future changes in user identity goes undetected [65]. However, it is desirable that a *continuous* authentication system should not interrupt the user's normal activity and be light-weight, i.e., on battery consumption. Biometric-based continuous authentication solutions have shown to be more viable because biometric modalities can be collected with minimal effort from the users [80].

Evidently, continuous authentication, active authentication, implicit authentication, and transparent authentication have been interchangeably used in many papers [47, 142, 165, 239]. Patel et al. [194] considered continuous authentication and active authentication systems as similar and explained it as continuous monitoring of the user activities after the initial access to the mobile device. Active authentication, as defined by Stolerman [239], is the process of continuously verifying users based on their on-going interaction with the device. The Defense Advanced Research Projects Agency (DARPA) started Active Authentication program [90] to seek solutions by shifting the focus during authentication from the password to people themselves. The first phase of their Active Authentication program focused on the behavioral traits, i.e., cognitive fingerprint, which could be processed without the need for additional sensors.

According to Fridman et al. [81], active authentication is the problem of continuously verifying the identity of an individual. They experimented using Android mobile devices and collected both behavioral and contextual modalities, namely, text entered via the soft keyboard, applications used, websites visited, the physical location of the device as determined from GPS (when outdoors) or WiFi (when indoors), and stylometry, of 200 volunteers approximately for a period of at least 30 days. Their authentication system achieved an ERR of 0.05 (5%) after 1 minute of user interaction with the device, and an EER of 0.01 (1%) after 30 minutes in identifying a legitimate user. In another stylometric based continuous authentication, an EER of 12.42% for message blocks of 500 characters is achieved using Support Vector Machine (SVM) for classification [27]. However, stylometry based authentication schemes must improve accuracy, delays, and forgery. Khan et al. [142] mentioned that *implicit authentication* employs behavioral biometrics continuously and transparently to recognize and validate smartphone users' identity and conducted a field study on implicit authentication usability and security perceptions with 37 participants. Their experiment indicated that 91%

of participants found implicit authentication to be convenient and 81% perceived defined protection level to be satisfactory.

2.2.2.7 Transparent Authentication

Transparent authentication is an authentication mechanism with minimal or no noticeable involvement of users [47]. Transparent authentication implicitly authenticates the users based on their unique interactions with the device and create logic for authentication decisions. However, this concept stresses more on the procedure of collecting and analyzing user-authentication-identifiers [47, 72].

If systems perform users' authentication in the background (without requiring explicit user cooperation) [47, 33], they can be termed as *implicit, transparent, or unobtrusive* authentication systems. However, various authentication types (one-shot, risk-based, or continuous) could collect input transparently. Feng et al. [72] utilized the term transparent and continuous for their Finger-gestures Authentication System using Touchscreen (FAST) to secure mobile systems. The approach transparently captures the touch data without intervening in the user's normal activities. After the successful login, the FAST continues to authenticate the user in the background by transparently acquiring touch data that is generated as a result of normal activities with the device.

2.2.2.8 Risk-based Authentication

Generally, risk-based authentication schemes contain a non-static authentication decision engine that accepts or denies users access by comparing their real-time risk-score with their stored risk-profiles, and accordingly, the system challenges the users to authenticate themselves. For instance, if a user is checking a bank account balance from a verified secure location (home or workplace), verification of identity should not be required.

Otherwise, in case of a non-verified location, the service requires additional evidence about the identity of the user thus asking for the authentication credentials. Nowadays, risk-based authentication schemes tend to offer frictionless authentication providing user experience, that could be tailored as per threats observed by the service providers [36, 105, 189, 256]. Google proposed a BeyondCorp security framework [191] based on the *zero trust model*. The *zero-trust model* advises that all resources are accessed securely regardless of their location, inspects and logs all traffic, and adopts a least-privileged strategy and strictly enforces access control [98]. Consequently, the BeyondCorp security framework considers both internal- and external networks completely unreliable and enables access to IoT applications by dynamically asserting and enforcing access levels or tiers based on behavioral perception strategy.

ClearLogin [42] defines *risk-based user authentication* as a method which adapts authentication levels based on the apparent risks, to mitigate the potential intrusion, before they happen. Existing *risk-based user authentication* schemes generate a risk-profile to determine the complexity of challenge to authenticate a user during a session, i.e., higher-risk profiles lead to stronger authentication, whereas usual authentication scheme should be sufficient in normal scenarios [226]. Identity Automation [123] consider *risk-based user authentication* similar to *adaptive authentication* because they adapt to the stringency of authentication processes based on the likelihood that access to a given system could result in its compromise.

Earlier risk-based user authentication mechanisms were mainly based on contextual or historical user information or both [114]. Furthermore, these systems rely on ad-hoc or simplistic risk management models with some rule-based techniques, which proved to be ineffective due to human factors [99]. However, nowadays as NuData Security [189] mentioned risk-based authentication schemes are getting fueled by behavior piercing technology that gives maximum security with minimal interruption to the user experience. Risk-based user authentication can be applied from two different perspectives, i.e., proactive or reactive [256]. Authors explained the main benefits of applying a proactive risk-based authentication is that the genesis of potential attacks, failures, or any kind of security issues can be anticipated for administrating prompt actions. On the contrary, reactive risk-based authentication accepts some of the risks until the risk-score goes beyond the permissible threshold level to prompt for the reauthentication.

2.2.2.9 Adaptive Authentication

Adaptive user authentication boasts the concept of having the ability to change and to prepare for different conditions and situations, while securing any unauthorized access [9, 117, 216]. It entails multi-factor user authentication mechanisms that should be readily configurable and deployable by performing risk-assessment [124]. Thus, it is a method for selecting the appropriate authentication factors accustomed to the situation accordingly to the user's risk profile and tendencies. It can be deployed as follows:

- By setting static policies based on risk levels for different factors, such as user role, resource importance, location, time of day, or day of the week.
- By learning day-to-day activities of users based on their habits to generate dynamic policies.
- Lastly, by combing both static and dynamic policies.

Hulsebosch et al. [117] exploited the ability to sense and use context information to augment or replace the traditional static security measures

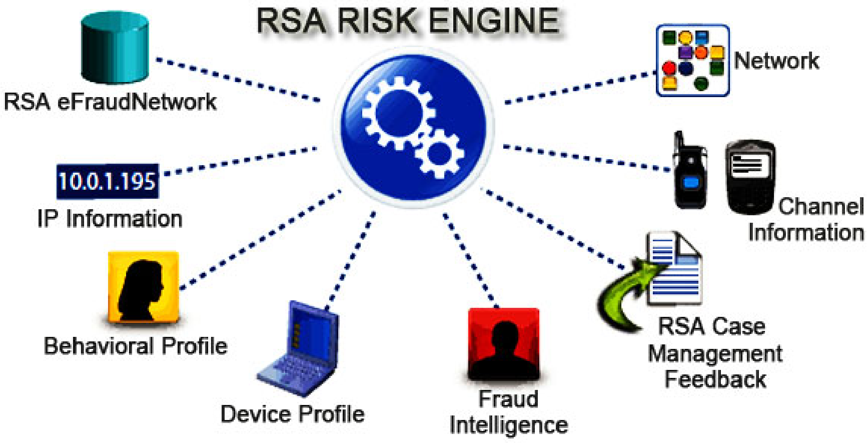


Figure 2.8: RSA adaptive authentication [216]. The RSA *Risk Engine* measures over one hundred indicators and assigns a unique risk-score to each activity.

by making them more adaptable to a given context and thereby less intrusive to derive Context-Sensitive Adaptive Authentication. RSA Risk Engine [216] used the self-learning risk model and adapts itself based on received feedback. The feedback loop includes case resolution and genuine or failed authentication results as well as chargeback files for *adaptive authentication* for eCommerce (see Figure 2.8).

2.2.2.10 Unimodal and Multi-modal Authentication

Typically, this terminology is used for biometric authentication schemes based on the number of modalities or traits used in authentication systems [133, 131, 214]. The literal meaning of modality[2] is a particular way of doing or experiencing something.

Unimodal authentication systems leverage only a single biometric modality or trait, whereas multi-modal systems, are developed by combining two or more modalities (sources of information). Multi-modal authentication systems demonstrate several advantages, such as higher recognition rate, accuracy, and universality [214]. Jain et al. [131] showed

[2] https://dictionary.cambridge.org/dictionary/english/modality

that multi-modal biometric systems driven by multiple biometric sources perform, generally, better recognition performance as compared to uni-modal systems. As per the type of multiple modalities being used, multi-modal biometric systems can be further divided into three categories: 1) Multi-physiological, 2) Multi-behavioral, and 3) Hybrid Multi-modal systems [132]. The multi-physiological category includes multi-modal biometric systems, where only physiological traits, such as the face, fingerprint, iris, etc., are fused at different levels, whereas a multi-behavioral system combines data from keyboard, mouse, and graphical user interface interactions. Hybrid multi-modal system [196] fused face, ear, and signature with social network analysis at the decision level to enhance the biometric recognition performance.

Researchers have been actively working on combining different modalities to design multi-modal user authentication schemes, however, usable security schemes for emerging IoT applications are yet to be studied, and evolved thoroughly.

2.3 Usable Security

This section explores the design goals and evaluation methods for usable security. Unarguably, the usability of a security system is emerged out as a critical factor that influences users to use security for their IoT applications.

2.3.1 Why Usability Matters?

The ISO standard:13407 defines usability as "*the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction, in a specified context of use* [126]." We present some important considerations that account for the growing significance of usability.

- Usage easiness is an intrinsic characteristic that impacts end-users' decision to go for a security mechanism. Usability helps in determining the effort required by users to interact with a particular user authentication scheme.

- Many critical sectors, e.g., banking and finance, transport, smart-offices, etc., enforce user authentication to maintaining and safeguarding themselves from adversaries. And, at the same time, consolidate the security, privacy, and safety of their legitimate users. Usable security can aid to overcome the inadvertent (or even deliberate) undermining of security by end-users.

- Usability evaluation aid to determine user experience, challenges, skills, and attitudes in using authentication schemes, thus, achieving usable security goals.

2.3.2 Usable Security Design Goals

We present some important design goals that address valid and non-trivial concerns specific to usable security [282]. The design goals include some terminologies such as Actor, Action, and Boundaries. An actor can be defined as an application, service, or system that interacts with end-users. Actions are the various task performed by actors. And, boundaries can be specified as conditions or circumstances that are important for end-users.

- **Appropriate boundaries:** Systems must acknowledge to the users about the actions demanded by the actors along the boundaries that are matter to them. This goal is based on *the principle of boundaries* [179].

- **Clarity:** Notify the consequences of any security-relevant decisions precisely that the user is most likely to perform.

- **Explicit authorization:** Any authorization to other actors must only be granted in accordance with user actions which should be well understood by a user while acknowledging the consent.

- **Expressiveness:** Enable the user to express safe security policies in terms that fit the user's goals.

- **Identifiability:** Any specific actors or specific actions must be clearly identifiable and transparent to the user.

- **Path of least resistance:** Selection of the natural methods to grant permissions to the actors without compromising security processes.

- **Revocability:** A user should be able to revoke others' authority to access the system.

- **Self-awareness:** Maintain accurate awareness of the user's own authority to control the system.

- **Trusted path:** Protect the user's channels to any entity that manipulates authority on the user's behalf.

- **Visibility:** A user should be aware of others' active authority affecting any security-relevant decisions.

2.3.3 Usability Evaluation Methods

Usability evaluation can be performed during the design and development phase of a system, i.e., formative evaluation, or based on users' assessment after they use the system, i.e., summative evaluation. Typically, usability evaluation methods incorporate techniques, such as inspection, testing, or survey, to assess the extent to which usability objectives are achieved for a system.

2.3.3.1 Usability Inspection Methods

In the usability inspection method, experienced practitioners like usability specialists and security professionals examine the usability aspects of a system. The goal is to gather some useful insights by testing designs and systems. The popular usability inspection methods are Pluralistic Walkthrough [16], Heuristic Evaluation [111], Cognitive Walkthrough [236], Heuristic Walkthrough [31], Metaphors of Human Thinking (MOT) [82], and Persona Based Inspection [59].

2.3.3.2 Usability Testing with Users

Usability testing approaches involve representative users to work on typical tasks using the system. The task execution result of each user is analyzed to assess the system's friendliness. Testing methods for usability evaluation include Think Aloud Testing, Wizard of Oz, Coaching Method, Co-discovery Learning, Question asking protocol, Benchmark Testing, and Retrospective testing [120, 207].

2.3.3.3 Questionnaire and Survey Methods

Questionnaire and survey methods analyze the usability of a system by assessing 1) users' satisfaction to accomplish their objectives with the system and, 2) the mental model perceived by users after using the system for some time. In this category, Rating Scales, Satisfaction Questionnaire, and System Usability Scale (SUS) are some commonly used methodologies [75].

To evaluate the usability of our prototypes, we employed the System Usability Scale (SUS) as it is a reliable tool for the subjective assessments of a system's usability [28, 257, 188]. The SUS questionnaire consists of 10 questions or statements. The response to each question/statement is measured on a 5-point Likert scale that ranges from "Strongly Disagree" to “Strongly Agree”. The final SUS score ranges between 0 and 100, where a higher value indicates a more usable system. The System Usability Scale (SUS) template for questionnaire and scoring is available online [265].

2.4 Biometric Recognition System

The ISO standard:24741 defines the term biometrics, or biometric recognition as “*the automated recognition of individuals based on their biological and behavioral characteristics* [128].” Typically, a biometric recognition system can utilize for either or both authentication (verification) and identification purposes [132].

2.4.1 Authentication vs. Identification Process

- The biometric authentication process is a *one-to-one comparison* between a claimed identity and the biometric templates of that individual stored securely, in the system database. Authentication is also known as verification.

  Generally, a biometric-based authentication system requires a labeled claimant identity as an input to be matched with the stored biometrics templates corresponding to the given label, to assert the individual's claim. Often, authentication systems are deployed for positive identification to prevent systems from impostors and illegitimate persons.

- The biometric identification process is a *one-to-many comparison* to recognize an individual by searching the templates of all available persons in the system database for a match. The system asserts the claim if the individual is already enrolled in the system database.

  Biometric-based identification can be employed for both negative recognition preventing a single person from using multiple identities or positive recognition for authentication purposes.

2.4.2 Biometric Trait Selection

Simple, convenient, and user-friendly biometrics traits are the first requirement for flawless security systems. The selection of a biometric trait for a particular security application usually depends on the degree to which the following attributes are satisfied [282].

- **Universality:** Is specific biometric trait presence in each person?
- **Distinctiveness:** How efficiently biometric traits can differentiate one person from another?
- **Permanence:** Is biometric trait sufficiently invariant (with respect to the matching criterion) over a period of time?
- **Collectability:** How easily biometric traits can be acquired from a person?
- **Performance:** How accurate and robust is the biometric trait?
- **Acceptability:** Indicates the extent to which people are willing to accept a particular biometric.
- **Circumvention:** How difficult is it to tamper with the biometric trait?

2.4.3 Biometric Recognition System Building Blocks

As shown in Figure 2.9, a biometric recognition system primarily consists of five modules: 1) Data Acquisition Module, 2) Data Processing Module, 3) Features Processing Module, 4) Database Module, and 5) Classification Module. It operates in two modes, namely, the enrollment mode and the recognition mode. Each module is described as follows.

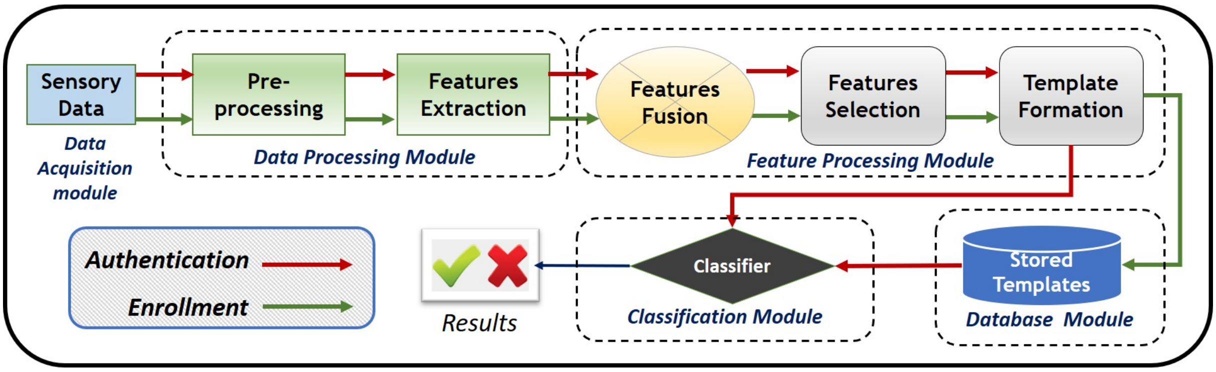


Figure 2.9: Buildings blocks of a biometric system.

1. **Data Acquisition Module:** This module consists of sensors that acquire the biometric traits of an individual. It is desired that the measured biometric modalities are both distinctive between individuals and repeatable over time for the same individual. This module is also referred to as a data collection module.

2. **Data Processing Module:** This module preprocesses the acquired data and subsequently, extracts the features from the processed data.

3. **Features Processing Module:** In this module, the extracted features are fused and selected for the generation of a user biometric template. Biometric traits may be acquired separately or simultaneously and they are processed as per the fusion model used.

4. **Database Module:** Database module stores the users' biometric template generated during the enrollment process.

5. **Classification Module:** Classification module compares between the input query and stored biometric template of an individual to accept or reject the claimed identity.

During the *enrollment process*, a biometric system acquires the various biometric trait of an individual. The features are processed and extracted from the raw sensor data. Then, the extracted features are selected and fused to create an individual biometric template to be stored in the system database.

During the *recognition process*, the system once again acquires the biometric trait of an individual. Subsequently, features from the raw sensor data are processed, extracted, selected, and fused to form a query template. The query template is then compared with the stored template present in the database to determine a match or to verify a claimed identity.

2.4.4 Classification Model Design

The machine-learning based classification model designing is a systematic approach to derive a precise mapping function that learns from the labeled dataset (training data) to predict labels of new data. Typically, classification models can be divided as multi-class classification and one-class classification to address user authentication scenarios.

2.4.4.1 Multi-class Classification Model

Smart homes or offices and applications such as online banking, online shopping, ride-booking, are used by multiple users. For multiple user authentication scenarios, multi-class classification models are best suited. The multi-class classification model classifies more than two classes (users). Classes are mutually exclusive and each new instance belongs to a single class.

2.4.4.2 One-class Classification Model

One-class classification model suffices for scenarios such as user authentication for accessing smart devices. The main goal of one-class classification is to detect an anomaly or a state other than the one for the target class (legitimate user). Therefore, information regarding other classes (illegitimate users) is not required to build a one-class classification model.

The one-class classification model is trained only with the target class samples. And, no information about outlier objects is available during the training of the model. This model is often called outlier (or novelty) detection.

2.4.5 Privacy Issues for Biometrics

While designing a user authentication scheme, the attributes - *security*, *privacy*, and *usability* emerged out to be orthogonal to each other. Studies have shown that none of the available authentication schemes can satisfy these three attributes, simultaneously [101]. For instance, PIN/password or smart-token based schemes do not affect users' privacy, but they have several security and usability issues. Whereas, biometric-based schemes can fulfill security and usability criteria, but affect the privacy of a user. Thus, a trade-off between security, privacy, and usability is a viable option for designing biometric-based authentication schemes.

Concerning users' privacy, cross-matching, and the inability to revoke a biometric are two major issues. Although, a number of privacy-preserving techniques [253], such as *Template Protection Schemes*, *Biometric Crypto-Systems*, and *Pseudonymous Biometric Identities* are available to safeguard user's biometric data complying with criteria like irreversibility, revocability, and unlinkability, published in ISO24745:2011 [129].

- Template protection schemes exploit *features transformation mechanisms*, in which users' biometric templates are stored after bio-hashing, biometric salting, or non-invertible transformation of extracted features from the freshly acquired biometric data. *Cancelable Biometrics* is another type of template protection scheme that leverages noninvertible geometric transformations (e.g., cartesian-, polar-, or functional transformation), random projections (e.g., a random subspace used for projection of biometric templates), random convolution (e.g., random user-specific convolution kernels applied for encryption of biometric templates), BioConvolving (e.g., applicable to biometric templates comprises of sequential feature-set), or Bloom filters (e.g., utilizes a space-efficient probabilistic data structure) [195].

- Biometric crypto-systems involves key-binding (e.g., fuzzy vault, fuzzy commitment, etc.), and key generation (e.g., fuzzy extractor, secure sketches, etc.) [15].
- Pseudonymous Biometric Identities exploit non-invertible functions to create pseudo-identities based on the references of biometric data [39].

According to kindt [145], *the most effective and advanced techniques for guaranteeing irreversibility, unlinkability, and renewability of biometric identities shall be used, if the implementation of such techniques under economically and technically viable conditions is possible* enabling design requirements into regulation, such as Privacy-by-Design (PbD). Technically, it is computationally exhaustive to recover the original biometric from a transformed one by incorporating privacy-preserving techniques. Also, they are capable of preventing cross-matching between databases since each application uses a different transformation.

2.5 Performance Metrics

The performance metrics to report validation results for our authentication schemes are described below.

- **True Acceptance Rate (TAR):** It is a ratio of correctly accepted legitimate user's attempts to all the attempts made [128]. Higher TAR indicates that the system performs better in recognizing a legitimate user.

- **False Rejection Rate (FRR):** It is a ratio of wrongly rejected attempts of a legitimate user to all the attempts made [128]. It is calculated as `FRR = 1 - TAR`.
- **False Acceptance Rate (FAR):** It is a ratio of wrongly accepted impostor attempts to all the attempts made [128]. Lower FAR means the system is robust to impostor attempts.
- **True Rejection Rate (TRR):** The ratio of correctly rejected attempts of impostors to all the attempts made. It is calculated as `TRR = 1 - FAR`.
- **Receiver- or Relative-Operating Characteristic (ROC):** ROC plot is a visual characterization of trade-off between `FAR` and `TAR` [70]. In simple words, it is a plot between true alarms vs. false alarm. The curve is generated by plotting the `FAR` versus the `TAR` for varying thresholds to assess the classifier's performance.

We reported our results mostly in terms of TAR and FAR, and ROCs to avoid redundancy, as TAR is a complement of FRR and FAR is a complement of TRR.

2.6 Summary

We are plainly dependable on IoT applications to sort-out our day-to-day activities. User authentication for IoT applications is the basic requirement to secure Human-to-Machine interaction. This chapter covered the topics in the realm of next-generation user authentication for IoT applications.

- We covered various ways and types of user authentication schemes with their security and usability analysis.

- We presented design goals and evaluation methods for usable security.
- We described biometric recognition system and performance metrics to report validation results for our authentication schemes.

The next chapter describes the problem domain to understand the need for next-generation user authentication schemes for IoT applications.

Chapter 3

The Problem

This chapter apprises readers with relevant information to understand the need for next-generation user authentication schemes for IoT applications.

3.1 Introduction

In the IoT age, smart devices, smart homes/offices, and smart enterprises have brought omnipotent experiences to their users.

Figure 3.1: Smart Devices, smart homes/offices and smart Enterprises.

The smart devices, smart homes/offices, and smart enterprises illustrated in Figure 3.1 are consistently improving the quality of their users' life. Typically, they offer numerous IoT applications that can be used for many personalized activities like (i) to store sensitive data, e.g., photos, emails, documents, etc., (ii) to perform sensitive operations, e.g., online banking, online shopping, GPS navigation, etc., and (iii) to offer or access sensitive services, e.g., on-demand ride and ride-sharing taxi services, driverless taxis, etc. Any unauthorized access to these IoT applications raises security and safety concerns for their users. Thus, it becomes imperative to design usable authentication schemes for them that can safeguard users' interests against potential risks, cyber-attacks, or inherent vulnerabilities, unerringly.

3.2 Problem Description

We present the fact sheet followed by an overview of IoT architecture and the challenges related to available authentication schemes for IoT applications.

3.2.1 The Fact Sheet

1. *Harvard Technology Fact Sheet* [106] stated that by 2030 more than 500 billion devices are expected to be IoT powered. Each device will be capable of interacting with the surrounding, collecting data, and communicating over a network with humans.

2. *IoT Analytics*[1], a leading provider of market insights and strategic business intelligence for Industry 4.0 and the Internet of Things (IoT), published in their report for the period 2017 to 2022 that authentication/authorization is one of the biggest issues for IoT applications.

[1] https://iot-analytics.com/new-iot-security-report/

3. The *2019 State of Password and Authentication Security Behaviors Report* published by Ponemon Institute [200], reported that 57% of respondents expressed a preference for passwordless logins. 51% of respondents stated that managing passwords is too difficult and the same percentage of respondents have faced a number of phishing attacks, regularly. 67% of respondents do not use any form of two-factor authentication. On average, respondents have spent approximately 10.9 hours per year entering and/or resetting their passwords. This analysis is based on inputs from 1761 IT security practitioners.

4. According to Gartner[2], by 2020, 20% of organizations will use IoT Applications in place of traditional physical access cards to enable access to offices and other premises.

5. The *Safety Report* released by Uber[3] revealed that there were 5,981 incidents of sexual assault were reported against their driver-partners in 2017 and 2018.

6. Table 3.1 categories the most targeted IoT applications based on *Verizon Data Breach Report* [269].

Table 3.1: Most targeted IoT applications.

Category	**Description**
Smart Devices	Digital devices for communication, navigation, entertainment, or any personal use.
Smart Home/Offices	Devices for lighting, heating and air conditioning, security, or sanitation.
Smart Enterprises	Public transportation, driverless vehicles.

[2] https://www.gartner.com/document/3515618

[3] https://www.uber.com/newsroom/2019-us-safety-report/

3.2.2 IoT Architecture

IoT enables Human-to-Machine (H2M) and Machine-to-Machine (M2M) nexus by introducing intelligence to sense, collect, react, and communicate, to enrich our lives. Figure 3.2 illustrates the simplified three-layer IoT architecture [291] consisting of perception, network and application layers.

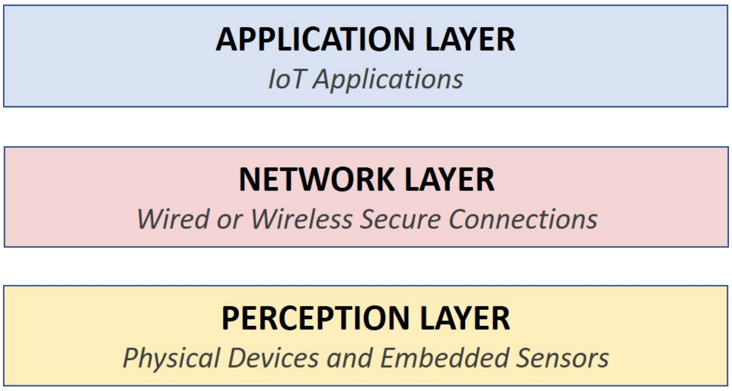

APPLICATION LAYER
IoT Applications
NETWORK LAYER
Wired or Wireless Secure Connections
PERCEPTION LAYER
Physical Devices and Embedded Sensors

Figure 3.2: A 3-layer IoT architecture.

- **Perception layer:** The perception layer is the lowest-most layer in three-layer IoT architecture. It is also known as *physical layer* and contained all the physical devices and embedded sensors. It collects, processes, and sends the physical data to the network layer. It also receives commands from the network layer to execute the tasks.

- **Network layer:** The network layer interfaces the perception and application layers. It is also known as *transmission layer* consists of wired or wireless communication networks, e.g., Wi-Fi, LAN, WAN, etc., and sensor networks, e.g., Ad-hoc, Mesh, Zigbee, industrial bus, etc.

- **Application layer:** The application layer houses various IoT applications that must ensure confidentiality, integrity, and authenticity to their consumers, i.e., humans or machines.

3.2.3 User Authentication Challenges

Studies have shown that application-layer attacks are much more complex to detect and deflect [245]. Considering the ubiquity of IoT applications and their fast adoption by almost everyone and every domain, user authentication (*i.e., Human-to-Machine authentication*) can play a pivotal role in the overall IoT security spectrum [159, 258].

Conventional (*knowledge-based and token-based*) authentication schemes are the most widely used methods for IoT devices, platforms, services, and application [67, 73]. However, there are many drawbacks in the conventional user authentication scheme [118, 84, 158]. According to Antonakakis et al. [5], weaker passwords were the main cause of bot-attacks like Mirai on various IoT applications. Lack of robust authentication mechanisms resulted in an easy hacking of IoT applications for smart devices, smart homes, and offices [160, 55]. Likewise, smart enterprises lack real-time authentication systems that can ensure the safety and security of their consumers [93, 97].

Chapter 2, Section 2.2 presented a detailed security and usability analysis of conventional authentication schemes suggesting their unsuitability for IoT applications. Taking all of those factors into consideration, we see both opportunities and challenges to design next-generation user authentication schemes for IoT applications.

3.3 Summary

The IoT applications' users are experiencing numerous security issues such as brute-force, presentation, shoulder-surfing, social engineering, etc., and usability issues such as cognitive load, form-factor, application interfaces, etc., in using convectional user authentication schemes[92, 62]. The challenges described above have led to a realization that user authentication schemes need upgrading for these new IoT age applications, Chapter 4 to 7 present our novel user authentication schemes for most targeted IoT applications as indicated in Table 3.1.

Chapter 4 presents HOLD & TAP a risk-driven one-shot-cum-continuous user authentication solution for smart devices' IoT applications based on users' invisible tap-timings and hand-movements. Chapter 5 presents STEP & TURN that offers a secure and usable authentication solution for smart homes and offices by exploiting users' single footstep and hand-movement to secure physical access only to their authorized users. Chapter 6 and 7 present DRIVERAUTH and RIDERAUTH offer risk-based authentication schemes for smart enterprises strengthening the security and safety of their consumers.

Chapter 4

Hold & Tap: A Risk-driven One-Shot-Cum-Continuous Behavioral Biometric-based User Authentication Scheme For Smart Devices

The chapter presents a risk-driven one-shot-cum-continuous behavioral biometric-based user authentication scheme for smart devices. HOLD & TAP strengthens the widely used PIN/password-based authentication technology by giving flexibility to users to enter any random 8-digit alphanumeric text and authenticates users based on their invisible tap-timings and hand-movements, instead of pre-configured PIN or Passwords. Moreover, the entire user session is *continuously* safeguarded by assessing risk. Thus, HOLD & TAP, not only authenticates users during the application sign-in process but also, throughout the entire active user session.

Partially, this work is published in [33]: *Attaullah Buriro, Sandeep Gupta, and Bruno Crispo. "Evaluation of motion-based touch-typing biometrics in online financial environments. BIOSIG 2017 (2017).*

4.1 Introduction

Smart devices provide a large number of IoT applications, such as banking app, m-commerce app, social networking app, etc., enabling users to access them anytime, anywhere. Many of these applications rely on PIN or password-based user authentication schemes despite numerous security and usability issues present in these schemes [238, 92]. Some of these IoT applications also deploy 2-factor authentication schemes by introducing smart-tokens, one-time-passcodes (OTP), verification over-the-call, etc., to enhance security, however, on the contrary, they degrade usability without providing any continuous risk assessment of the active user session.

From the security perspective, PIN/password-based schemes are vulnerable to guessing [140], smudge [7], shoulder-surfing [140, 281], dictionary [35] attacks. Similarly, from the usability perspective, users face difficulty to manage numerous PINs/passwords [15] and complex passwords add cognitive load on users [286, 147]. Additionally, it is not easy to employ PIN/password-based schemes for continuous user authentication without affecting the user experience [231]. Further, it is worth mentioning that these schemes do not necessarily authenticate the users, but authorize anyone who enters the correct PIN/password [92]. Thus, it becomes requisite to redesign the PIN/password-based authentication mechanism to overcome their inherent shortcomings.

Hold & Tap supplements the existing PIN/password-based authentication schemes with two behavioral biometric traits to enhance their usability and security, i.e., users do not require to remember their PINs, or passwords and authentication decision is not simply a binary comparison. Internally, the scheme exploits two behavioral biometric traits, i.e., tap-timings and hand-movement gesture recorded during the *ran-*

dom text entry, to authenticate users. Then, throughout the active user session, the scheme continuously performs risk-assessment. If the risk-score is higher than the predefined threshold, the current user session terminates. Afterward, the scheme requests the user to re-authenticate. Thus, the dependency on any dedicated devices (e.g., smart token) that are required to generate *One Time Password* (OTP) to finish critical operations is eliminated.

The results obtained on $11,400$ user-samples (collected by 3 days *in-the-wild* testing) and user-experience responses (received from the *Software Usability Scale*[1] survey) of 95 testers demonstrate HOLD & TAP as an accurate and acceptable user authentication scheme.

4.1.1 Contributions

In brief, the main contributions are:

- The proposal of a bimodal behavioral biometric-based one-shot-cum-continuous user authentication scheme that authenticates users based on *how* they enter the text instead of *what* they enter, thus strengthen `username/password`-based schemes.
- The introduction of a novel risk-assessment mechanism that *continuously* determines the need of user re-authentication during the active user session, by computing cumulative deviation of client-attributes.
- The validation of our proposed scheme on a dataset collected *in-the-wild* from 95 testers in three different activities, i.e., *sitting, standing, and walking*.
- The security evaluation of HOLD & TAP to assess its robustness against the most common (random and mimic) attacks
- The usability evaluation of HOLD & TAP by conducting a *System Usabil-*

ity Scale[1] survey.

4.1.2 Chapter Organization

The rest of the chapter is organized as follows: Section 4.2 surveys the related behavioral biometric-based user authentication and risk assessment approaches. Section 4.3 discusses the assumed threat model, working of our proposed scheme, and architecture of our system. In Section 4.4, we discuss the methodology used to design our one-shot-cum-continuous authentication scheme. Section 4.5 presents the obtained results. In Section 4.7, we assess the usability of our proposed system.

4.2 Related Work

This section presents some of the behavioral biometric-based user authentication schemes, and risk assessment approaches relevant to HOLD & TAP. Behavioral biometrics offers a simple way to implement a frictionless user authentication schemes that can be suited for implicit or continuous authentication [92]. This is possible due to the advantages associated with behavioral biometrics: 1) transparent collection, 2) no special hardware requirements, and 3) cost-effective deployment [212].

4.2.1 Behavioral Biometric-based User Authentication

Behavioral data, such as gait, grip, swipe, pick-up, tap, and voice can be collected, unobtrusively, due to the availability of sensors, particularly accelerometer, gyroscope, magnetometer, proximity sensor, soft keyboards, touch-screens and microphone in smartphones and have become widely researched subject these days.

We survey various behavioral authentication schemes proposed for user authentication over the years with the emphasis on: (i) novel behaviors,

[1] https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

(ii) use of smart devices sensory data and/or (iii) focus on user effort minimization.

4.2.1.1 Keystroke/Touch based Authentication

The concept of augmenting keystroke/touch-based behavioral biometrics to PIN or password is predicated on the understanding that users need a better way to prove their identities. The musculoskeletal structure in human produces unique finger movements resulting in distinguishable keystrokes or touch-points which can be utilized in anchoring an extra layer of security for user authentication.

Touch dynamics refers to user profiling based on touch patterns (i.e., touch duration and direction, etc.) on the touchscreen. The touchscreen allows the user to interact with the smartphone by taping at different locations on the screen. Touch-biometrics have been proposed for both one-shot and continuous user authentication on smartphones.

The touch-based scheme [51] leverages different touch features: X and Y coordinates, touch-pressure, the size of touch, and the time offset, generated from different slide operations to identify a user. Authors report 77% accuracy (with 19% FRR and 21% FAR) using Dynamic Time Warping (DTW) as the classifier over a dataset of 48 participants. Feng et al. [72] presented a finger-gesture based authentication system (called as FAST) in addition to the digital gloves. Every touch gestures include 53 features: X & Y coordinates, the direction of finger motion, the pressure at each sample touch-point, and the distance between multi-touch points. Digital gloves add angular values from X, Y and Z direction in addition to roll, pitch, and yaw values. FAST achieved a FAR of 4.66% and FRR of 0.13% on a dataset of 40 users using Gesture Sequence-Based Authentication.

A study by Frank et al. [80] also explores the touchscreen gestures for continuous smartphone user authentication. This mechanism exploits the very common navigational movements (e.g., horizontal/vertical strokes) and shows their efficacy to authenticate the real user. This study achieves an EER of 0%, $2-3\%$ and <4%, respectively, in intra-session, inter-session and authentication tests after one week of enrollment using KNN classifier and SVM - with Gaussian Radial Basis Function (RBF) kernel, on a dataset of 41 testers.

Sae-Bae et al. [219] exploit single and multitouch gestures for user authentication on touch-sensitive devices, i.e., smartphones and tablets. On a dataset of 34 participants, they report an average EER of 7.88% using a single instance of multi-touch gesture and an EER of 1.58% with a combination of three gestures (static counter-clockwise rotation, closed and opened, with all five fingertips). Authentication solution [278] profiles simple touch actions, i.e., keystroke, sliding, pinch, and handwriting, and continuously authenticates the smartphone user. The scheme leverages multiple features related to coordinates, pressure, size, etc, and achieves the lowest EER of 0.75% for sliding gesture and all other action types, lower than 10% with SVM classifier using RBF kernel.

4.2.1.2 Sensors/motion based Authentication

In addition to the touch-based solutions, researchers have also exploited smartphone's built-in physical 3-dimensional sensors, such as accelerometer, gyroscope, orientation, etc., to profile phone movements, for smartphone user authentication. The data from these sensors is used to identify users from their walking patterns [166], general hand-movement [157, 289, 230], special hand-movement (while entering PIN, password) [33, 233], and hand-movement (how a user moves the phone to place or answer a call [45] and profiled gesture models [289], etc.

The study by Shi et al. [230] presents a multi-sensor-based approach to passively identify a real user. Their system incorporates the accelerometer, touch screen, voice, and location data for user authentication. They achieve around 97% TPR, using the Naive Bayes as the classifier, from their dataset of 7 users (three females and four males). The study [157] explores the role of three sensors: accelerometer, orientation, and compass in addition to the touch gestures towards continuous user authentication. This transparent mechanism profiles finger movements with classical touch-based features and interprets the sensed data as different gestures. It then trains the SVM classifier on those gestures and performs authentication tasks. The paper reports as high as 95.78% accuracy on a dataset of 75 users.

The study by Zhu et al. [289] proposes a mobile framework model *Sensec* based on the accelerometer, orientation, gyroscope, and magnetometer, to construct a user gesture profile. The model then continuously computes the sureness score and keep the user sign-in. By concatenating X, Y, Z values from these sensors, they identify a valid user with 75% accuracy and an adversary with an accuracy of 71.3% (with 13.1% FAR) on their collected dataset of 20 users. However, the study required a user to follow a script and collect the sensory data for the entire duration of that interaction.

4.2.1.3 Sensor-enhanced Touch-typing based Authentication

Our scheme is a bimodal system that leverages the timing-differences from the entered 8-digit "text-independent" secret and the hand-movements while the user enters the text to sign-in to the security-sensitive apps, we compare our work with the closely related works proposed in the literature, i.e., [87, 33].

Giuffrida et al., [87], proposed sensor enhanced fix-text scheme for user authentication on Android smartphones. They reported 4.97% EER on fixed-text passwords and 0.08% on sensor data on a dataset of 20 users.

The papers discussed here implemented a behavioral biometric-based authentication scheme performed in in-the-lab supervised settings, and their analysis was based on a small number of users. We evaluated our scheme on a comparatively larger dataset of 95 users collected in-the-wild. Since the number of users in previous studies was less and data was collected in in-lab settings, it is difficult to examine how their achieved error would have varied if the number of users was more and data was collected in-the-wild. Also, we evaluated our data by applying multi-class classification to replicate a server-based remote client authentication with the risk-based authentication mechanism. However, the papers discussed here evaluated their data either using one class or binary class classification approaches - replicating authentication only on smartphones [233].

4.2.2 Risk-based Authentication Schemes

Most of the systems deploying risk-based authentication approaches typically generate a risk profile for each of the users. Based on the risk-score, the complexity of the challenge is determined to authenticate the user, i.e., a higher risk-score leads to stronger authentication, whereas a risk-score below the threshold means minimal or no authentication requirement [226].

Risk-based authentication approaches based on basic communication information [34], such as the source-destination IP addresses, or frequency of transactions, performed by a user on her devices to determine risk, are easily exploitable. According to Traore [255], such systems could be exploited by polling or cloning users' devices. Then, the same settings can be replicated on different machines to access their systems by attackers.

The cognitive fraud detection system by IBM Trusteer [122] is designed for PCs and laptops. Whereas, IBM's Tivoli Federated Identity Manager [250] is designed for web platform based on policy rules that determine the access request to be allowed, denied, or challenged at runtime. However, these are limited to static devices only, e.g., a personal computer and laptops, etc.

Sepczuk et al. [228] designed the remote-services for authentication management, which can be registered by the user either manually or automatically. Manual registration requires users to fill a form describing their day-to-day activities, e.g., what they do between 9 a.m. to 5 p.m? or which network they use at home or workplace. Whereas, automatic data gathering configures the system to collect contextual data, spontaneously. However, the solution may be subjected to insider attacks and lacks transparency, as service providers could misuse user contextual data, i.e., they are aware of an individual's day-to-day activities.

Generally, the contextual or historical data or both, to generate a risk profile of a user, is considered more suitable for risk-based authentication approaches [122, 202, 114]. However, the existing systems apply simplistic risk management models or ad-hoc rule-based techniques, which prove to be ineffective for risk assessment [99]. Furthermore, they mainly rely on knowledge-based authentication mechanisms such as `username/password`, or multi-factor authentication (e.g., OTP, token generator) [92], which affects the usability of a system adversely.

4.3 Hold & Tap: Our Solution

This section presents the assumed threat model. Afterward, we explain the working of our risk-driven one-shot-cum-continuous authentication system and its architecture.

4.3.1 Threat Model

We considered physical attacks, where (i) the adversary accidentally finds an unlocked smartphone, (ii) the adversary is a friend or colleague (who possibly knowing user's PIN/Passwords), and (iii) the adversary records users while they interact with their smart devices. Eventually, the adversary exploits the weaknesses of PIN/password-based authentication schemes to gain access to sensitive resources (data and applications) residing on users' smart devices.

Prior studies [231, 203] also indicated that the above-discussed scenarios are quite apparent, as users use their smart devices at commons places like offices, homes, meeting rooms, or streets, which may give opportunities to adversaries to target their smart devices, easily. As a consequence, smartphone users can be a victim of monetary frauds, identity thefts, or similar unfavorable incidents.

4.3.2 How HOLD & TAP Works?

Figure 4.1 illustrates the design of our one-shot-cum-continuous authentication scheme explaining how it addresses security and usability issues in existing `user/password`-based, and 2-factor authentication schemes.

The scheme enables users to enter any random $8-digit$ alphanumeric text to access the application to enhance the usability of existing PIN/Password-based one-shot authentication schemes. Further, the scheme verifies the users' identity based on timing differences between the entered keystrokes and their hand-movement in 3-dimensional space instead of just a binary comparison, to enhance security.

After the successful sign-in, the scheme *continuously* monitors client-attributes and computes the risk-score at the instant users initiate critical activities. Based on the risk-score, it permits users to perform that activity, otherwise, scheme prompts for re-authentication. Thus, HOLD

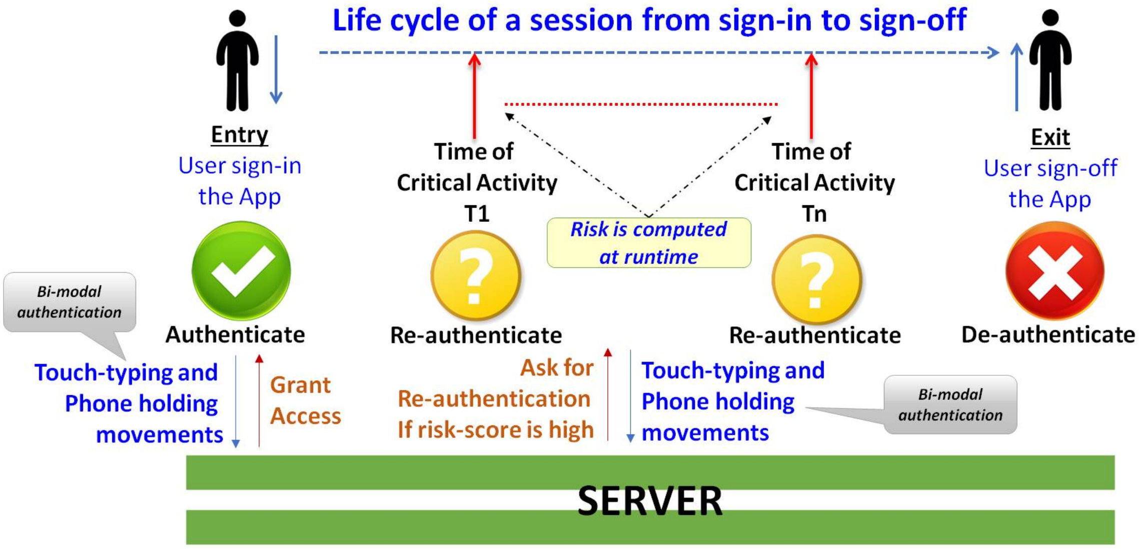

Life cycle of a session from sign-in to sign-off
Entry
User sign-in the App
Authenticate
Time of Critical Activity T1
Re-authenticate
Risk is computed at runtime
Time of Critical Activity Tn
Re-authenticate
Exit
User sign-off the App
De-authenticate
Bi-modal authentication
Touch-typing and Phone holding movements
Grant Access
Ask for Re-authentication If risk-score is high
Touch-typing and Phone holding movements
Bi-modal authentication
SERVER

Figure 4.1: HOLD & TAP authentication scheme design.

& TAP is capable of detecting any anomalies in the users' usage pattern throughout the life-cycle of a typical user session and apparently, 2-factor authentication can be safely disregarded.

4.3.3 HOLD & TAP Architecture

The system adopts a client-server architecture [94] as shown in Figure 4.2. The client consists of data acquisition (DA) modules that can be added to existing smartphone applications, seamlessly. The DA collects the two behavioral biometric traits along with client-attributes and transfers the encrypted data to the server at runtime for further processing.

The server includes two independent modules, i.e., the User Authentication (UA) and the Risk Assessment (RA) module those work in tandem. The UA module performs user authentication based on features extracted from touch-typing and hand-movements behavioral traits, as explained in Section 4.4.2. The RA module, using the Runtime-Risk-Assessor (RRA) inside the Risk Engine (RE), computes the risk-score at run time, as ex-

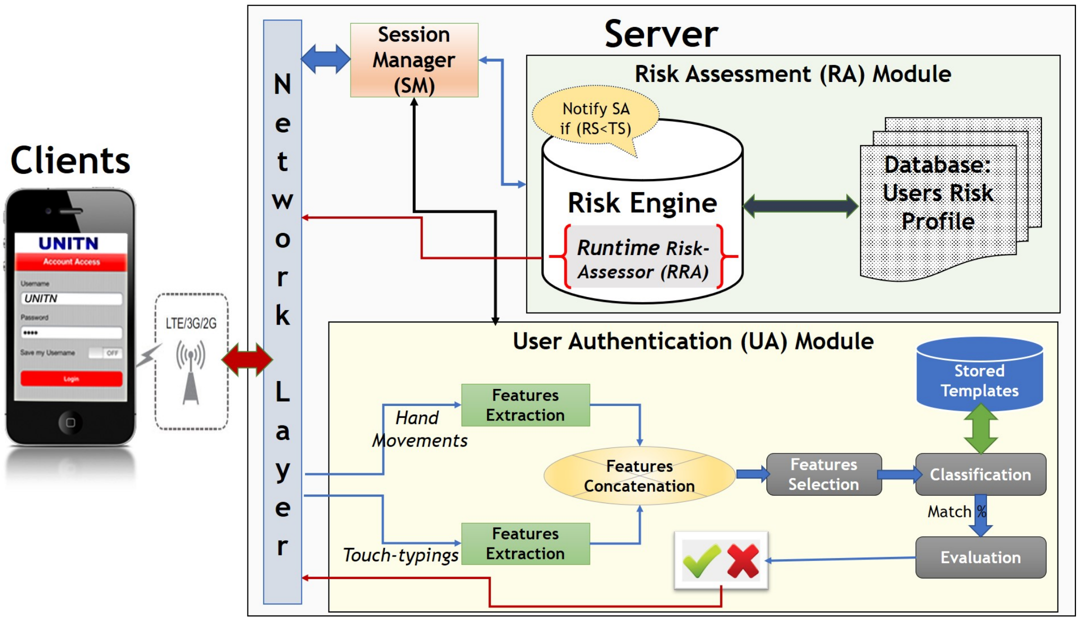


Figure 4.2: HOLD & TAP: system architecture.

plained in Section 4.4.6, each time a critical operation is performed. The RE then notifies the Session Manager (SM) if the computed risk-score is higher than the predefined threshold. Afterward, the SM sends the command to the UA module for re-authentication.

4.4 Methodology

In this section, we explain the steps taken to design and evaluate the HOLD & TAP.

4.4.1 Data Collection

We develop a prototype application (app) that can be installed on Android devices having OS version $4.4.x$ or higher for data collection. We then collaborated with Ubertesters[2] - a crowdsourcing software testing platform to conduct our experiment. Ubertesters recruited vetted testers having a diversified background, and they billed us on an hourly basis

[2] https://ubertesters.com

per tester. They strictly ensure that the ethical guidelines prescribed by the government or controlling bodies of the countries of the testers' location were maintained. And, we followed the GDPR ethics and data protection guideline [86] that states, "*in research settings, data protection impose obligations on researchers to provide research subjects with detailed information about what will happen to the personal data that they collect*." We provided the complete instructions to test our prototype application that includes installation steps and the details of the motion sensor data being collected. Each tester signed the consent form after reading the instruction to test our application.

The app enables testers to test the app for approximately, an hour that spans over 3 days with 1 session per day, i.e., 3 sessions in 3 days. A unique label was assigned to each tester. During each training session, testers can interact with the app for 15 minutes in 3 different activities, i.e., *sitting, standing, and walking*. On the third day, the testers can also test the app with 30 testing samples in any activity of their choice. Afterward, the testers performed the SUS survey, and they filled their demographic information presented in Appendix A. During the experiment, the survey data and motion sensors data generated on each tester's smartphone were securely transferred to our servers in an automated manner and no direct contact was established with any testers to protect their privacy.

Approximately 100 testers participated to test our prototype application. Each tester tested our prototype application on their smartphones under real-life conditions. However, we discard the data from 5 testers for reasons like their smartphones did not have the required sensors or Internet connectivity was too slow to transfer the sensors' data in real-time to our server. Table 4.1 summarizes the demographics of testers selected to participate in our experiment.

Table 4.1: User demographics (M = Male, F = Female, R = Right, L = Left).

Parameter	Description
No. of Users	95
Sample Size	**Sitting -** $2,850$ **(**95×30**)** **Standing -** $2,850$ **(**95×30**)** **Walking -** $2,850$ **(**95×30**)** **Testing -** $2,850$ **(**95×30**)**
Devices	Android Smartphones having OS `4.4.x` version or above
No. of Sessions	3
Password	8-digit ***free-text***
Gender	75(M), 20(F)
Handedness	89(R), 6(L)
Age Groups	90 $(20-40)$, 5 $(41-60)$

Overall, we collected $11,400$ samples with 120 samples from each tester (30 samples in each of the 3 different training activity and 30 samples during testing) and received 95 SUS responses in this experiment. Thus, we evaluated HOLD & TAP on a collected dataset of 95 users having a total of $11,400$ samples.

4.4.2 Feature Extraction

We used the touchscreen sensor and seven 3-dimensional motion sensors (*i.e., the accelerometer, the high-pass sensor, the low-pass sensor, the orientation sensor, the gravity sensor, the gyroscope, and the magnetometer*) to collect raw data for touch-stroke and hand-movement, respectively [4]. The high-pass and low-pass sensory data are computed mathematically, by applying High-Pass (HP) and Low-Pass (LP) filters as shown in Equation 4.1 and 4.2.

$$Value_{HP} = Value_{Gravity} \times \alpha + Value_{Accelerometer} \times (1 - \alpha) \tag{4.1}$$

$$Value_{LP} = Value_{Accelerometer} - Value_{Gravity} \tag{4.2}$$

Where, $Value_{HP}$, $Value_{LP}$, $Value_{Accelerometer}$, and $Value_{Gravity}$ represent the value of the high-pass, low-pass, accelerometer, and gravity sensor, respectively at a time t. We set α to 0.1 that was determined, empirically. As shown in Figure 4.3, touch-typing features consist of 8 *Type0* (timing difference between each key release and key press), 7 *Type1* (timing difference a key press and previous key release, 7 *Type2* (timing difference two successive keys release), 7 *Type3* (timing difference two successive keys press), and 1 *Type4* (timing difference between last and first key press). Thus, we extracted 30 touch-typing features from the 8-digit *random-text* entry.

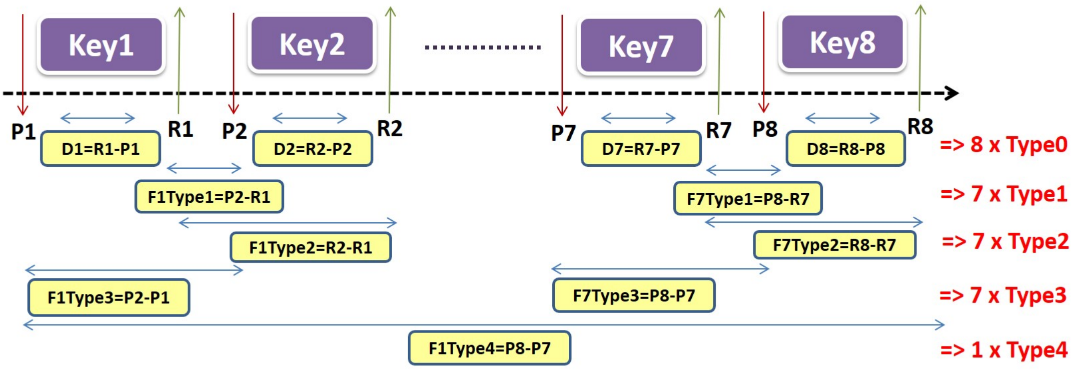


Figure 4.3: Touch-typing features for 8-keys entry.

Similarly, a user's hand-movement is modelled in terms of 3-D data streams, i.e., X, Y and Z, from each motion sensor. In addition, we computed the 4^{th} dimension, Magnitude (M), by using Equation 4.3.

$$Value_M = \sqrt{(Value_x^2 + Value_y^2 + Value_z^2)} \tag{4.3}$$

Where, $Value_M$ is the Magnitude and $Value_x$, $Value_y$ and $Value_z$ are the values of X, Y and Z value of a sensor, at a time t.

We obtained 4 data streams from each of the seven motion sensors with the delay set at *SENSOR_DELAY_GAME* [4]. Then, from each data stream, we extracted 4 statistical features, namely Mean (μ), Standard Deviation (σ), Skewness (s), and Kurtosis (k), that gives 16 statistical features per sensor as shown in Table 4.2.

Table 4.2: Statistical features per sensor for a hand-movement behavior.

No.	Hand-movement Features			
1-4	μ_X	μ_Y	μ_Z	μ_M
5-8	σ_X	σ_Y	σ_Z	σ_M
9-12	s_X	s_Y	s_Z	s_M
13-16	k_X	k_Y	k_Z	k_M

Finally, we concatenate 30 touch-stroke features and 112 hand-movements features to create a feature vector of size 142. Here, we prefer to choose the feature level fusion over the sensor level fusion because sensory data could have inconsistent and/or unusable data that may affect classifiers' accuracy [198].

4.4.3 Feature Selection

The primary purpose of any feature selection scheme is to filter out the redundant and less productive features to determine the most productive features [95]. This improves the performance of a classifier as processing smaller feature vectors would be computationally faster. We applied Information Gain Attribute Evaluator (IGAE) - a Weka [276] implemented Information Gain based feature selection scheme. We obtained the threshold for feature selection by dividing the number of users (95) by the total number of features (142). The feature with higher weight was picked for further analysis.

4.4.4 Classifier Selection

Classifier selection depends on various parameters, such as data size, data characteristics, and training time, etc. We selected simple, yet effective state-of-the-art classifiers: Naive Bayes (NB), Neural Net (NN), and Random Forest (RF) classifiers.

Bayesian classifiers, such as Belief Networks and Naive Bayes employ the probabilistic technique for the classification tasks. The Naive Bayes method starts with a strong but "naïve" assumption that the features are independent of each other. It works perfectly well if this condition holds. Furthermore, it is widely used because of its super simplicity, faster learning capability, elegance, and robustness [102].

NN classifier belongs to the Artificial Neural Network (ANN) family. These models represent many interconnected network elements designed essentially to classify different patterns. These models have been shown to be quicker and accurate [53]. We used the Levenberg-Marquardt trained feed-forward neural network as the classifier in our analysis.

RF has been considered as an accurate and efficient classifier in recent years [25]. The reasons for their popularity include: (i) its accuracy among the current algorithms even without any optimization, (ii) it generally does not overfit, (iii) it efficiently handles the missing data, and (iv) its effectiveness on small as well as for large datasets, etc. We preferred this classifier because of its effectiveness in the previous studies [33]. RF classifier works on the principle of growing many classification trees and to classify, it puts the query sample down to each of the trees in the forest. Each tree classifies that sample and "vote" for a particular class. The final decision chosen by the forest is based on the higher number of votes (over all the trees in the forest).

4.4.5 Classifier Training & Testing

We consider remote-user-authentication to access security-sensitive applications on smartphones as a multiclass classification problem. We used PRTools [60], a Matlab-based toolbox, to construct a classification model and validated users in two scenarios, (i) a verifying legitimate user scenario, and (ii) an attack scenario.

We evaluate the classification model by partitioning the dataset into training and testing sets. We trained selected classifiers with 5, 10, and 15 samples and used the remaining samples for testing.

4.4.6 Risk Assessment Model

According to ISO 9000:2015 [127], the risk is the “effect of uncertainty on objectives” and an effect can be a positive or negative deviation from what is expected. An objective can be strategic, tactical, or operational. Generally, the existing risk-driven authentication system uses a risk-score to estimate the risk associated with the user’s activities including the sign-in attempt, in a typical user session [125]. A user-session can be characterized by using historical and contextual attributes, such as transactions pattern, user’s geographic location, access-time, IMEI number, MAC and IP address of registered devices, the user’s typing speed and so on, collectively can be defined as the *client-attributes*.

The *risk-score* can be computed by determining cumulative *uncertainty* (degree of deviation) associated with each client-attribute. By using a mathematical formula or expression, the degree of deviation can be easily determined to establish a relationship between the present value, and previously recorded values (where the *objectives* achieved successfully) of client-attributes.

In our system, the Risk Engine (RE) configures a client profile of each customer by using contextual and historical data, e.g., transactions patterns, location, access-time, IMEI number, MAC and IP address of registered devices, operating system, applications installed, and stylometry, etc., as client-attributes.

To create the user's client profile, RE initially assigns a unique weight (natural value) to each client-attribute as per the user's preferences.

$$CA_i = WEIGHT \begin{cases} \forall\, i \in M \\ WEIGHT \geq 1 \end{cases} \tag{4.4}$$

Equation 4.4 describes the weight assignment process to each of the M client-attributes. RE assigns a higher value to the client-attribute based on the user preference order. For example, if a user has given more importance to *Smartphone IMEI* over *access time* than will be $CA_{IMIE} > CA_{AccessTime}$. Two client-attributes can have a common integer value. However, the model can reassign the weights by analyzing the user's usage pattern, thus, updates the client-profile, automatically.

Table 4.3 presents the structure of a user's client-profile. Each row comprises of a client-attribute, its weight, and values of the current session, i.e., $Session_N$ to all the $N - 1^{th}$ previous sessions. `Frequency of Non-occurrence` (FNO_i) and `Impact of Non-occurrence` (INO_i).

To obtain `Frequency of Non-occurrence` (FNO_i) and `Impact of Non-occurrence` (INO_i), we first calculate `Frequency of Occurrence` (FO_i) as follows:

The `Frequency of Occurrence` (FO_i) is an estimate of how often the current client-attribute value ($Value_{iN}$) has occurred in previous $N - 1$ sessions [277], which is determined using Equation 4.5.

Table 4.3: Structure of User's Client Profile.

#	Client-Attributes	Weight of Client-Attributes	$Session_N$	$Session_{N-1}$	...	$Session_2$	$Session_1$	Frequency of Non-occurrence	Impact of Non-occurrence
1	Transaction Pattern	CA_1	$Value_{1N}$	$Value_{1(N-1)}$	...	$Value_{12}$	$Value_{11}$	FNO_1	INO_1
2	Location	CA_2	$Value_{2N}$	$Value_{2(N-1)}$	...	$Value_{22}$	$Value_{21}$	FNO_2	INO_2
3	Access time	CA_3	$Value_{3N}$	$Value_{3(N-1)}$	...	$Value_{32}$	$Value_{31}$	FNO_3	INO_3
4	IMEI number	CA_4	$Value_{4N}$	$Value_{4(N-1)}$	...	$Value_{42}$	$Value_{41}$	FNO_4	INO_4
5	MAC address	CA_5	$Value_{5N}$	$Value_{5(N-1)}$	...	$Value_{52}$	$Value_{41}$	FNO_5	INO_5
6	IP address	CA_6	$Value_{6N}$	$Value_{6(N-1)}$	...	$Value_{62}$	$Value_{61}$	FNO_6	INO_6
7	OS Version	CA_7	$Value_{7N}$	$Value_{7(N-1)}$	...	$Value_{72}$	$Value_{71}$	FNO_7	INO_7
8	Apps Installed	CA_8	$Value_{8N}$	$Value_{8(N-1)}$	...	$Value_{82}$	$Value_{81}$	FNO_8	INO_8
9	Touch-typing speed	CA_9	$Value_{9N}$	$Value_{9(N-1)}$	...	$Value_{92}$	$Value_{91}$	FNO_9	INO_9
...	...	...	...	...	...	...	...	...	...
M	Stylometry	CA_M	$Value_{MN}$	$Value_{M(N-1)}$	...	$Value_{M2}$	$Value_{M1}$	FNO_M	INO_M

$$\begin{aligned} O_i &= \sum_{j=1}^{N-1} [Value_{iN} = Value_{ij}] \; \forall\, i \in M, \quad \text{and} \\ FO_i &= \frac{O_i}{N-1} \; \forall\, i \in M \end{aligned} \tag{4.5}$$

Where, O_i is the occurrence of $Value_{iN}$ of a i_{th} client-attribute. The value of FO_i towards ≈ 1 indicates lower risk, whereas towards ≈ 0 indicates higher risk.

Subsequently, `Frequency of Non-occurrence` (FNO_i) and `Impact of Non-occurrence` (INO_i) are measured at runtime using Equation 4.6 and Equation 4.7, respectively.

$$FNO_i = 1 - FO_i \quad \forall\, i \in M \tag{4.6}$$

$$INO_i \; = \; FNO_i \times CA_i \quad \forall \, i \in M \tag{4.7}$$

Where, FO_i is defined as the frequency of occurrence, which can be calculated using Equation 4.5, CA_i is the weight of each client-attribute and M is the number of client-attributes. The value of FNO_i towards ≈ 0 indicates lower risk, whereas towards ≈ 1 indicates higher risk.

For example, a customer has accessed her banking app from X location $\pm 10KM$ in the previous 10 sessions. But, in the current session, the access location is found to be Y so the frequency of its occurrence ($FO_{location} = \frac{0}{10}$) becomes 0. Therefore, the frequency of its non-occurrence ($FNO_{location}$) becomes 1, which is calculated using Equation 4.6. As described in Equation 4.7, multiply $FNO_{location}$ with $CA_{location}$ to calculate $INO_{location}$, which gives a positive number. Similarly, the impact of the non-occurrence of other client-attributes can be calculated.

Finally, the risk-score is computed using Equation 4.8, which can be defined as the sum of all the impact-of-non-occurrence of each client-attribute. Higher the number means higher the risk.

$$Risk\ Score \; = \; \sum_{i=1}^{M} INO_i \tag{4.8}$$

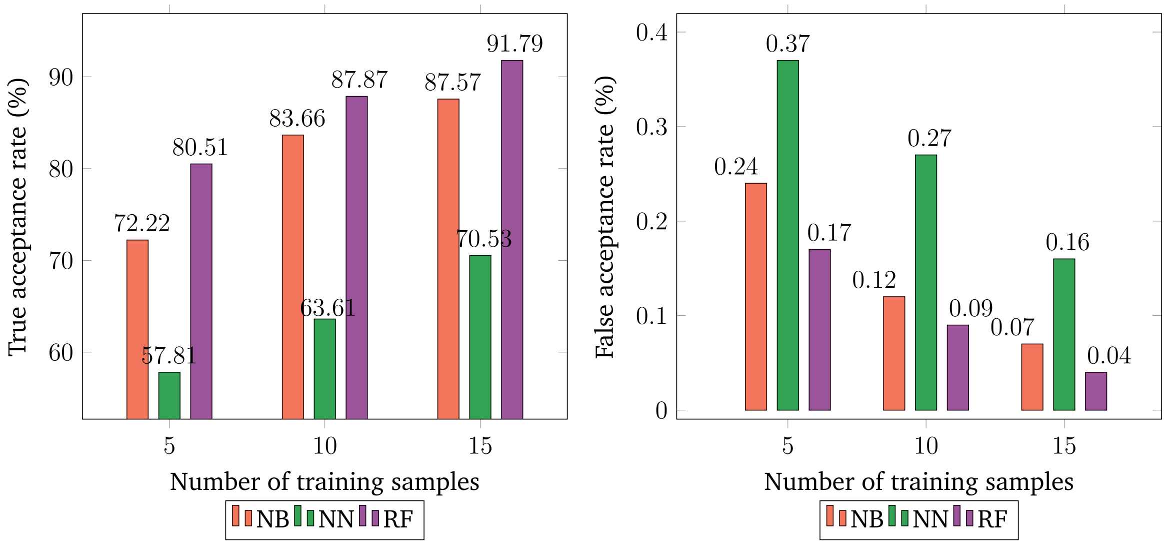
Where, M is number of client-attributes.

The risk-score is computed and matched with the threshold before any of the critical operations is performed. If the risk-score is higher than the predefined value (e.g., an average of the risk-scores in previous $N-1$ sessions), re-authentication is exercised leveraging the proposed behavioral biometric-based bimodal authentication scheme.

Thus, our authentication scheme utilizes the concept of one-shot and continuous authentication mechanisms driven by risk assessment, as explained in Section 4.3.2, offering a user-friendly verification mechanism.

4.5 Results

Figure 4.4, 4.5, and 4.6 report TAR and FAR on full features for sitting, standing, and walking postures, respectively. RF classifier performed consistently well across all the activities and for the different number of samples. We achieved a TAR of 80.51% (in *sitting*), 82.91% (in *standing*), and 81.38% (in *walking*), on just 5 training samples, and this TAR increased up to 91.79%, 91.58%, and 86.95%, on 15 training samples. The highest achieved TAR by RF is 91.79% (at just 0.04% FAR), on 15 training samples.

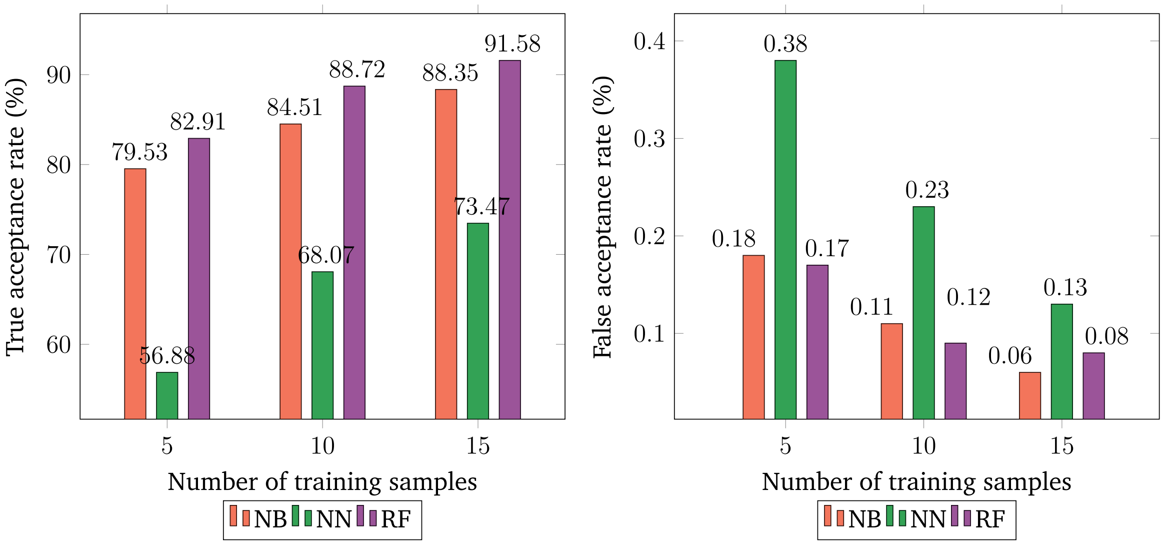


(a) True Acceptance Rate (TAR)

(b) False Acceptance Rate (FAR)

Figure 4.4: Results for sitting posture with all features for 5, 10, and 15 training samples.

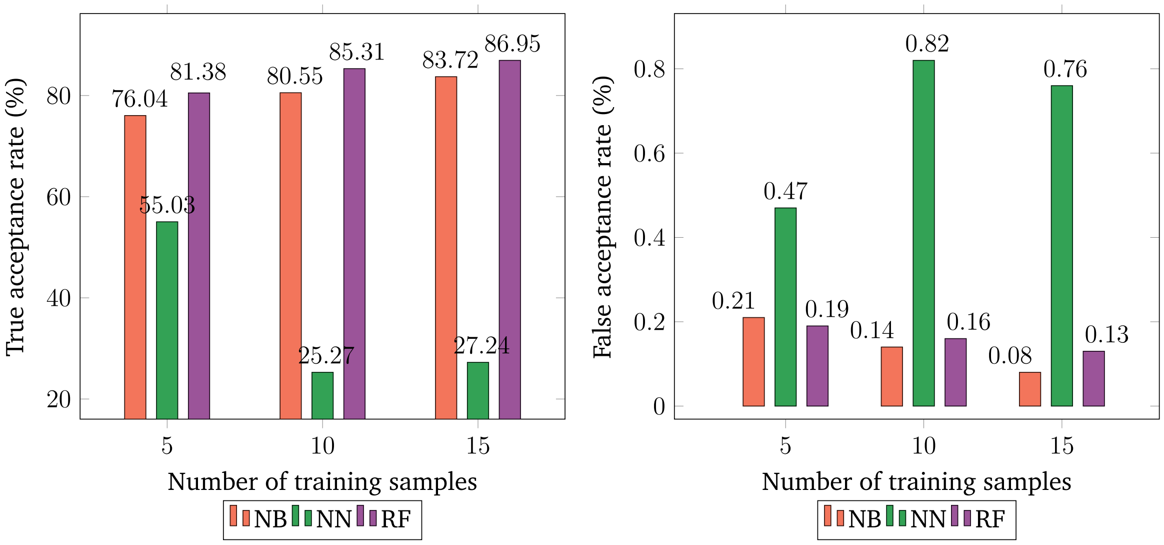
Figure 4.7, 4.8, and 4.9 report TAR and FAR on IGAE selected features for sitting, standing, and walking postures, respectively. The results of all the classifiers improved, significantly, over the extracted IGAE features except for NB in *standing* and *walking* activities, over 5 training samples. NN performed comparatively well on the smaller feature vectors. RF classifier improved the authentication results on IGAE features, i.e., from 88.04% to 89.10%, 92.88% to 95.18% and 94.87% to 96.00% for three



(a) True Acceptance Rate (TAR)

(b) False Acceptance Rate (FAR)

Figure 4.5: Results for standing posture with all features for 5, 10, and 15 training samples.

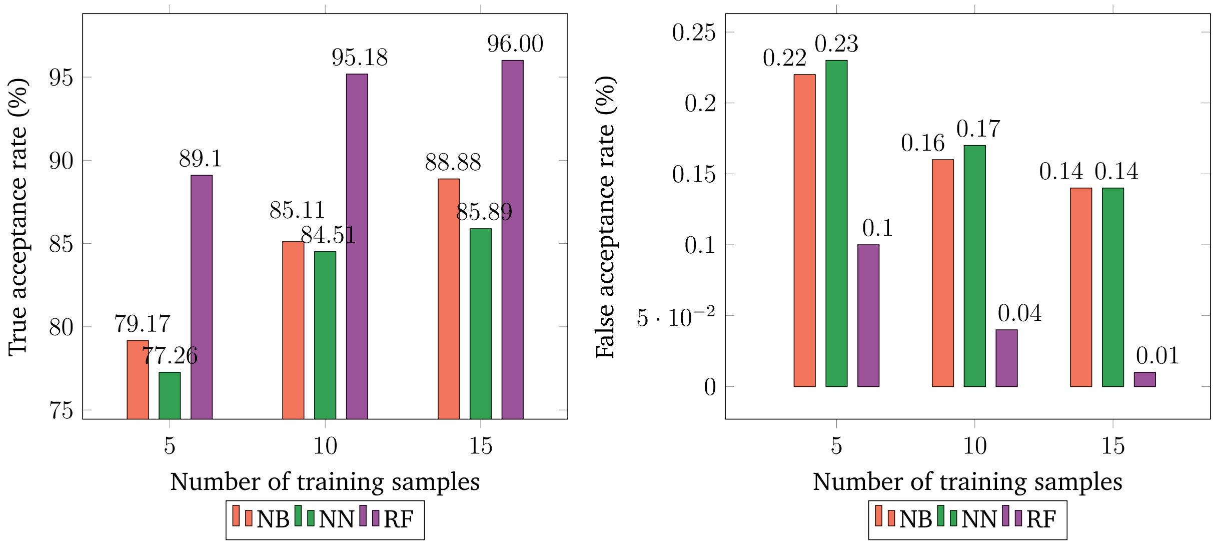


(a) True Acceptance Rate (TAR)

(b) False Acceptance Rate (FAR)

Figure 4.6: Results for walking posture with all features for 5, 10, and 15 training samples.

activities, on 5, 10, and 15 training samples, respectively. It is evident that HOLD & TAP is very robust against the zero-effort attacks, i.e., TRR is much higher and FAR is very low.



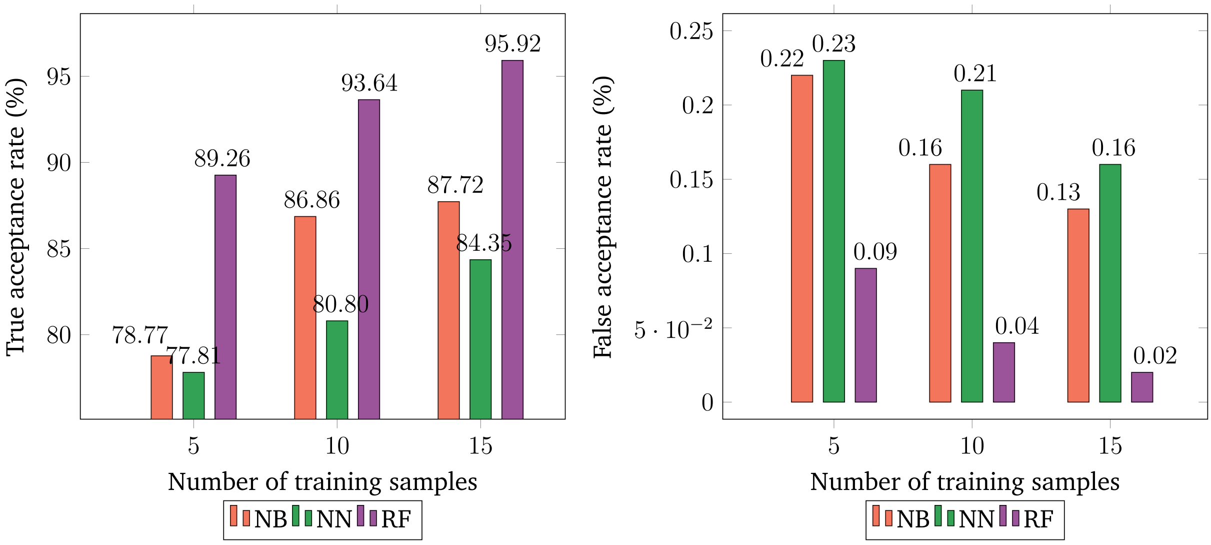
(a) True Acceptance Rate (TAR)

(b) False Acceptance Rate (FAR)

Figure 4.7: Results for sitting posture with selected features for 5, 10, and 15 training samples.

We, also, show the results of RF classifier in terms of ROC curves (see Figures 4.10, 4.11, and 4.12). We show an average ROC of all the users obtained through Vertical Averaging (VA) [69]. In this averaging, the averages of the TAR rates are plotted against the researcher-defined fixed FAR. Due to the space limitations, we illustrate ROC curves for best-performing classifiers, i.e., for RF, for all the activities, and all the training sample scenarios. Figure 4.10 to 4.12 reflects RF classifier as very productive and accurate classifier throughout.

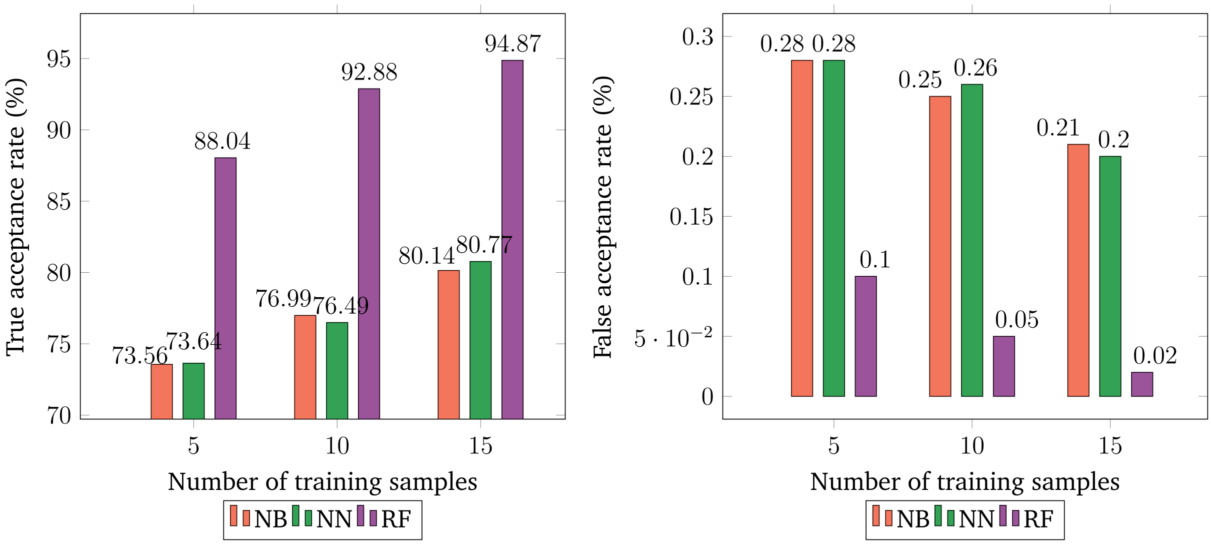
RF classifiers outperformed both NB and NN classifiers because of its ability to reduce the variances and its most unlikeliness to over-fitting. NB classifier requires Gaussian distributed data, which might not be true in the dataset, hence it failed to address the problem of concept-drift. The



(a) True Acceptance Rate (TAR)

(b) False Acceptance Rate (FAR)

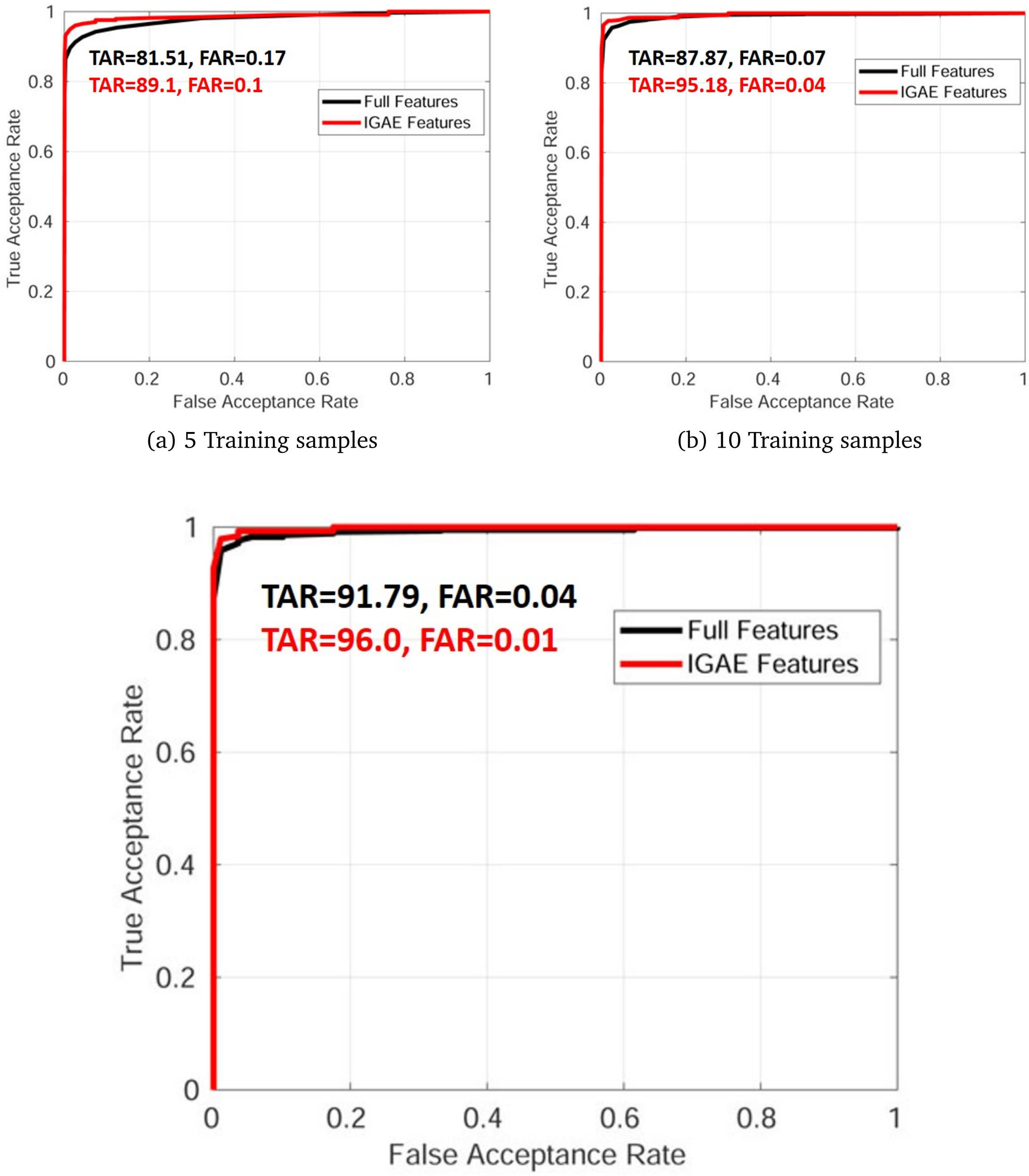
Figure 4.8: Results for standing posture with selected features for 5, 10, and 15 training samples.



(a) True Acceptance Rate (TAR)

(b) False Acceptance Rate (FAR)

Figure 4.9: Results for walking posture with selected features for 5, 10, and 15 training samples.

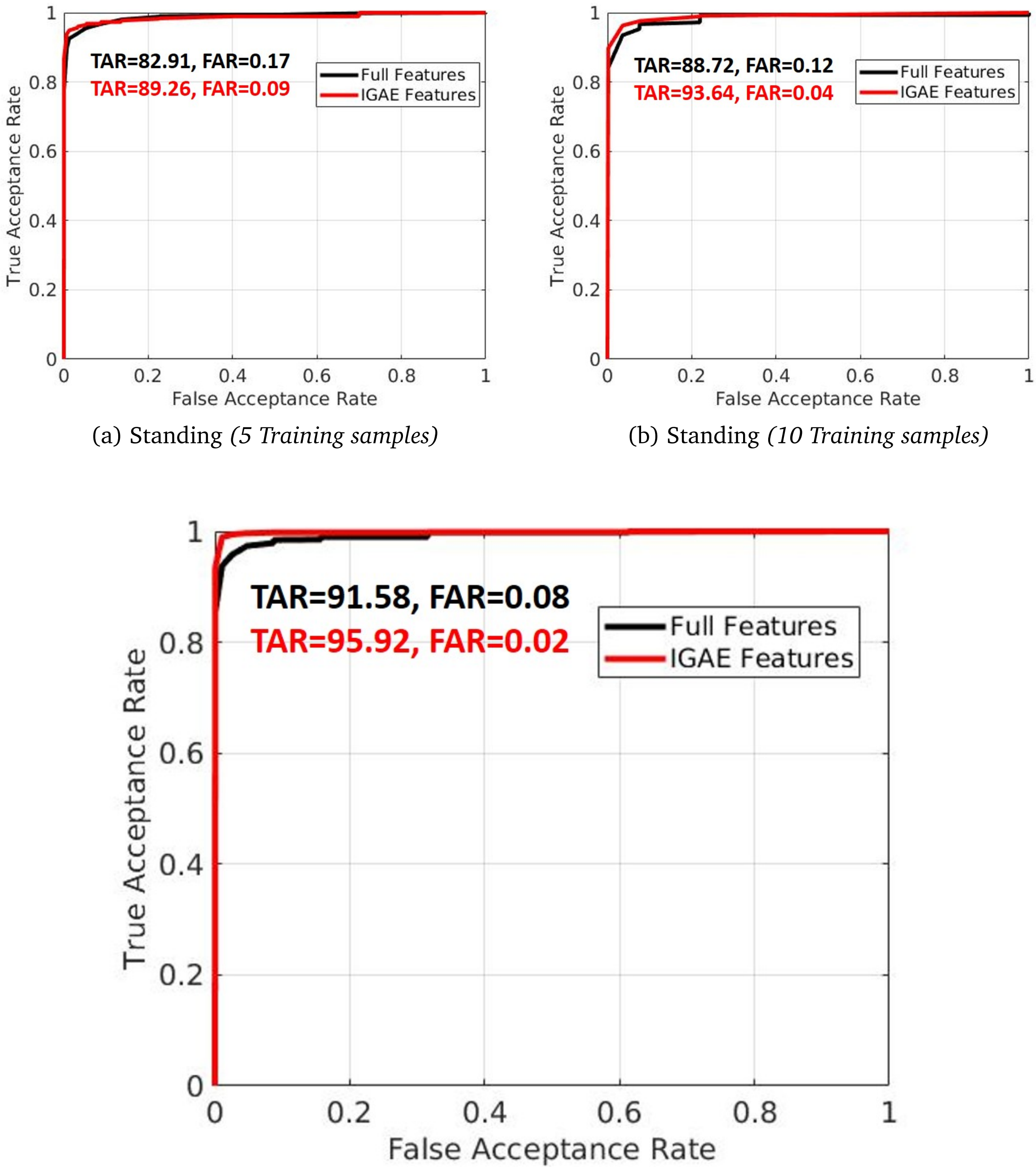


(a) 5 Training samples

(b) 10 Training samples

(c) 15 Training samples

Figure 4.10: The ROC curves of RF classifier on full and IGAE features for sitting posture with different training samples.

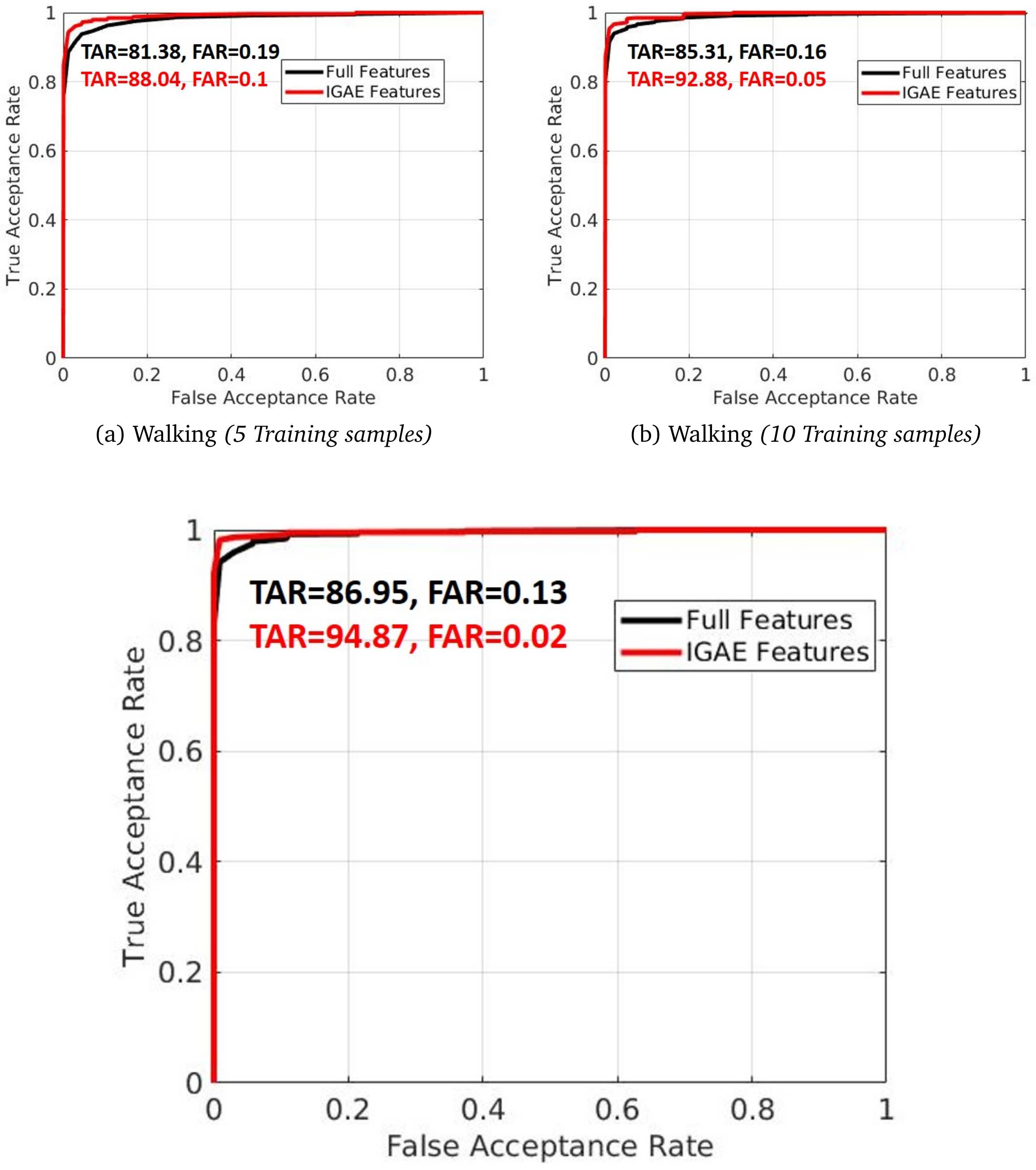


(a) Standing *(5 Training samples)*

(b) Standing *(10 Training samples)*

(c) Standing *(15 Training samples)*

Figure 4.11: The ROC curves of RF classifier on full and IGAE features for standing posture with different training samples.



(a) Walking *(5 Training samples)*

(b) Walking *(10 Training samples)*

(c) Walking *(15 Training samples)*

Figure 4.12: The ROC curves of RF classifier on full and IGAE features for walking with different training samples.

NN classifier did not perform well due to the limited number of training samples. It generally requires more training samples to learn well.

4.6 Security Analysis

To determine the robustness of HOLD & TAP, we performed some additional experiments to replicate a couple of attack scenarios, namely, random attack and mimic attack.

4.6.1 Mimic Attack

We recruited 8 testers to carry out the mimic attack. Each one of the 8 testers trained the prototype application installed on a smartphone, which is closely observed by the remaining 7 testers to learn the holding and typing patterns. In each tester's training session 30 observations (10 per 3 postures, i.e., sitting, standing, and walking) are collected. Then, the remaining 7 testers tried 10 times to carry out the mimic attack.
A multi-class classification model for 8 testers is generated by using RF classifier with 30 training samples per class, i.e., a total of 240 training samples. Subsequently, we tested this classification model with 8 sets of 70 mimic attack samples collected from the remaining 7 testers (10 samples per tester), labeling each set from 1 to 8.

Table 4.4: Mimic attack results.

Class	True Acceptance	False Rejection	Robustness(%)
1	0	70	100
2	0	70	100
3	0	70	100
4	1	69	98.57
5	0	70	100
6	0	70	100
7	2	68	97.14
8	0	70	100
	3	237	**98.75**

Table 4.4 presents the result for each class in terms of True Acceptance (TA) and False Rejection (FR). Higher the FR better the robustness of the system. Thus, the overall robustness of HOLD & TAP against mimic attack comes out to be 98.75%.

4.6.2 Random Attack

To carry out the random attack, we asked each of the 8 testers to test the application 10 times in any of the 3 postures. Then, we tested the classification model robustness with 70 random attack samples (excluding the samples of a legitimate user) 8 times by assigning labels from 1 to 8.

Table 4.5: Random attack results.

Set	True Acceptance	False Rejection	Robustness(%)
1	0	70	100
2	0	70	100
3	0	70	100
4	0	70	100
5	0	70	100
6	0	70	100
7	0	70	100
8	0	70	100
	0	240	**100**

Table 4.5 presents the random attack results for each class in terms of TA and FR. None of the 240 random attack attempts were successful. Thus, the overall robustness of HOLD & TAP against random attack comes out to be 100%.

4.7 Usability Analysis

Figure 4.13 illustrates the SUS questionnaire and the collected responses from all the 95 participants. We did not collect any information relating to an identified or identifiable natural person, as defined by GDPR ethics and data protection guideline [86]. Overall, HOLD & TAP achieves the

SUS score of ≈ 73, which is significantly above the standard average score of 68 [225]. After analyzing the recorded feedback, it can be inferred the majority of the participants are satisfied to use HOLD & TAP and they perceived our proposed scheme as simple, extremely convenient, user-friendly, and intuitive.

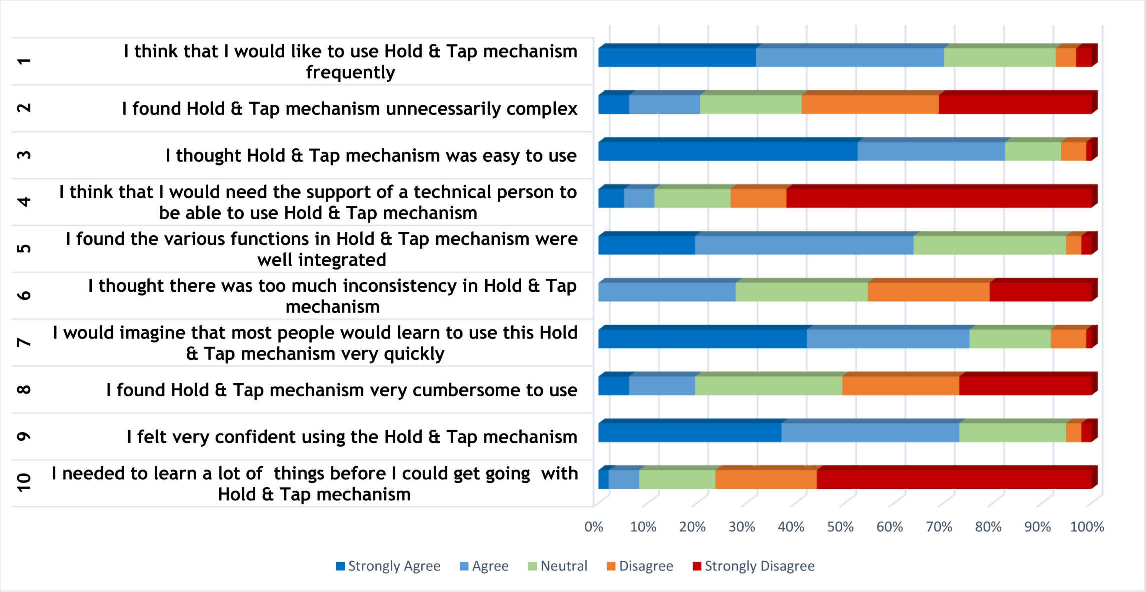


Figure 4.13: SUS questionnaire and users responses.

Overall most of the testers seem comfortable and confident about HOLD & TAP mainly because of the flexibility of typing any combination of 8-digit text. Experimental results show that our scheme as usable, practical and would be widely acceptable.

4.8 Summary

The proposed one-shot-cum-continuous user authentication scheme is a simple, effective, and user-friendly solution for smartphone security-sensitive applications (e.g., social networking app, online mobile banking app, etc.). The scheme can be seamlessly integrated into the existing PIN/password-based authentication schemes to enhance their usability and security. Flexibility to access an application by entering any random 8-digit alphanumeric text makes the sign-in process very convenient for smartphone users. At the same time, mimicking invisible, and inherently secure natural human behaviors simultaneously can be an onerous job for attackers.

With RF classifier, we obtained 96% TAR (at the cost of 0.01% FAR) in *sitting* activity for 15 samples training-set with selected features, whereas 95.92% and 94.87% TAR is achieved in *standing* and *walking* activity, respectively. Security analysis involving ≈ 480 adversarial attempts demonstrated HOLD & TAP resilience against mimic and random attacks. HOLD & TAP obtained a SUS score of ≈ 73 out of 100 that can be considered positive feedback.

Chapter 5

STEP & TURN - A Novel Bimodal Behavioral Biometric-based User Authentication Scheme for Smart Ecosystems

This chapter presents STEP & TURN - a novel bimodal behavioral biometric-based authentication system that utilizes two natural human actions, i.e., single footstep and hand-movement, to secure access to smart ecosystems. In today's rapidly evolving digital world, smart ecosystems such as smart homes, smart offices, and smart cities cannot rely on conventional authentication systems (e.g., digital keypads, physiological biometrics sensors, smart-card readers, or smart device pairing) entirely, to secure user access.

This work is partially published in [95]: *Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. "SmartHandle: A Novel Behavioral Biometric-based Authentication Scheme for Smart Lock Systems." Proceedings of the 3rd International Conference on Biometric Engineering and Applications. ACM (pp. 15-22). 2019.*

5.1 Introduction

Over recent years, the world is going through vast digital reforms, which is evident by the rapid evolvement of smart homes, smart offices, and smart cities, collectively, can be dubbed as smart ecosystems. Indeed, user authentication plays a vital role in safeguarding the smart ecosystems' security spectrum. However, studies have shown that the conventional authentication systems, i.e., knowledge-based schemes (e.g., PIN/Password), or device-pairing (e.g., smartphones, smart cards), deployed to secure user access are vulnerable to common attacks, such as a dictionary-, insider-, observation-, replay-, spoofing-attack, as well as they are reported to have several usability concerns [83, 115]. Consequently, smart ecosystems require next-generation user authentication systems owing to various drawbacks present in conventional authentication schemes.

Our authentication scheme exploits behavioral biometric traits to secure access to smart ecosystems. Some of the benefits of behavioral biometrics are that: 1) they do not require to be remembered like PIN or password, 2) they can not be shared or transferred to an unauthorized person, 3) they possess characteristics to meet usability criteria more stringently, in contrast to conventional authentication methods, and 4) the sensors, e.g., accelerometer, gyroscope, pressure, etc., required to acquire behavioral biometrics modalities are less expensive as compared to fingerprint, face, or iris data acquisition sensors [92]. Consequently, behavioral biometric traits open avenues to provide usable and secure user authentication schemes.

We present a novel bimodal behavioral biometric-based user authentication scheme for smart ecosystems that exploit the user's single footstep and their hand-movement to turn the door handle, as illustrated in Fig-

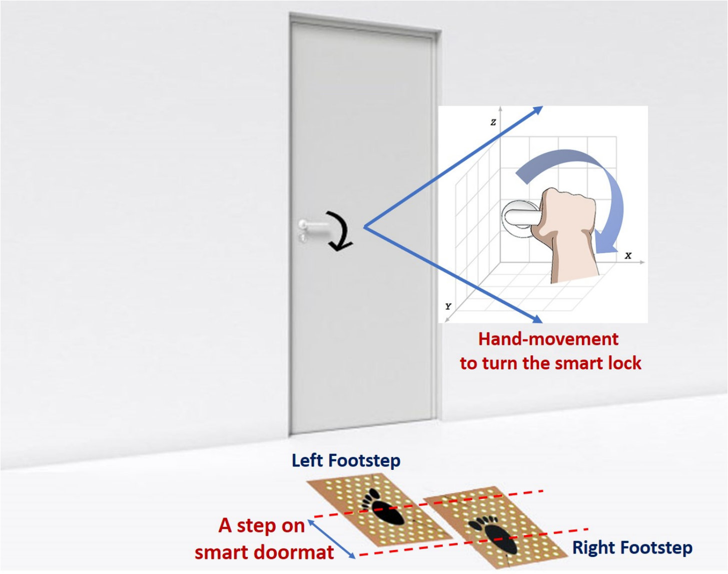


Figure 5.1: A pictorial illustration of STEP & TURN user authentication system.

ure 5.1. The left and right footstep pressure-data recorded from the array of 88 pressure sensors fitted in the 2 doormats and hand-movement is modeled in terms of X, Y, and Z coordinates in 3-dimensional space by using 3-axis accelerometer, magnetometer, and gyroscope sensors. To build the user authentication system, we selected three simple, yet effective, state-of-the-art machine learning classifiers, namely, random forest, state vector machine, and Fisher linear discriminant classifier. Classification Learner [168] is used to assess the classifiers' prediction performance and their selection. Furthermore, we performed usability analysis to establish the efficiency, effectiveness, and satisfaction of our user authentication methods.

5.1.1 Contributions

The main contributions of this paper are presented below:

- STEP & TURN - a novel user authentication scheme based on user's single footstep and hand-movement, which can be easily deployed to secure smart ecosystems access to their authorized users.

- We collect the hand-movement of 40 participants and then, constitute a chimerical dataset by combining the Swansea University Speech and Image Research Group footstep data of an equal number of participants with our collected dataset containing $1,600$ samples (40 per participants).

- The experimental validation and usability assessment of STEP & TURN by replicating a smart-office scenario.

5.1.2 Chapter Organization

The rest of the chapter is organized as follows: Section 5.2 discusses the related work. Section 5.3 covers the experimental setup and hardware details of STEP & TURN user authentication system. Section 5.4 describes the methodology used in data collection, features extraction, and features selection. Section 5.5 presents the design of the user authentication model and the experimental results under different settings. Section 5.6 presents the usability assessment of STEP & TURN user authentication system. Finally, Section 5.7 concludes the paper with the outline for possible future works.

5.2 Related Work

In the next few years, behavioral biometrics will irrevocably transform the user authentication landscape for smart ecosystems, such as smart homes, offices, and cities [93, 94]. The availability of various sensors (refer Section 5.3.2) has expedited the use of behavioral biometric traits, e.g., voice, digital signatures, keystroke/touch dynamics, gait, footsteps, and hand-movement to hold or wear smart devices, etc., for user authentication schemes [92]. This section reviews the prior work that utilized *hand-movement* and *footstep* behavioral biometric traits for user authentication.

Studies have shown that behavioral biometric can be utilized to design and develop usable authentication schemes [33, 32]. SMARTHANDLE - a user authentication scheme deployed in door handle utilized the user's hand-movement in 3-dimensional space by fetching the X, Y, and Z coordinates from 3 sensors, namely, accelerometer, magnetometer, and gyroscope corresponding to the hand-movement trajectory, to generate a user-identification-signature [95]. They validated their solution for a multi-class classification scenario and achieved a True Acceptance Rate (TAR) of 87.27% at the False Acceptance Rate (FAR) of 1.39% with the Linear Discriminant Classifier (LDC) on their collected dataset of 11 users. Jang et al. [136] proposed a bimodal door locking scheme that leverages fingerprint and grip patterns to authenticate users, however, they did not publish any experimental results to validate their schemes.

A motion-based authentication method for smart wearable devices, MOTIONAUTH, constructed users' identifiable signature by profiling their different natural gestures such as raising or lowering the arm [280]. They achieved an equal error rate of 2.6% on a dataset of 30 users. Similarly, SNAPAUTH [32] exploited users' hand-movement to authenticate them on smartwatches, while they perform finger-snapping action. They achieved the TAR of 82.34% by using Multilayer Perceptron (MLP) classifier on a dataset of 11 users.

Another user authentication scheme for smartphones leveraged users' hands-movement while they type on their phone, holding it in their hand. The scheme achieved a TAR of 96% on a dataset of 95 users by using MLP classifier. Similarly, HMOG user authentication scheme collected hand movement, orientation, and grasp data to continuously authenticate smartphone users by exploiting features like micro-movement and orientation dynamics when they interact with their smartphone [233].

They achieved an authentication Equal Error Rate (EER) of 7.16% and 10.05% for walking and sitting postures, respectively.

Rodriguez et al. [268] performed footstep biometric assessment on their collected 9,990 stride signals from 127 persons by using floor-based sensors. Their approach studied footstep signals in both time and space domains. In the time domain, the extracted features included the ground reaction force (GRF), the spatial average, and the upper and lower contours of the pressure signals, whereas, in the spatial domain, the features extracted include $3D$ images of the accumulated pressure. In their evaluation, they achieved the EERs of 15.2%, 13.4%, and 7.9% by training classification model with 40, 100, and 500 single footstep signals respectively, after fusing both time-domain and space-domain features. Similarly, Edwards et al. [66] extracted geometric and wavelet features from the footstep dataset collected by the Swansea University Speech and Image Research Group. They achieved an EER of 16.3% by retaining spatial information for wavelet analysis by using the Random Forest classifier for individual prediction within a dataset of 10,413 footstep pair instances from 94 participants.

Zhou et al. [288] proposed a system that identifies users based on their single footstep biometric without considering the shape details or interstep relationships of users' footprints. They utilized fabric sensors to register features such as shifting of the gravity center, maximum pressure point, and overall pressed area. They achieved an average identification accuracy of 76.9% on a dataset containing 529 footsteps collected from 13 participants.

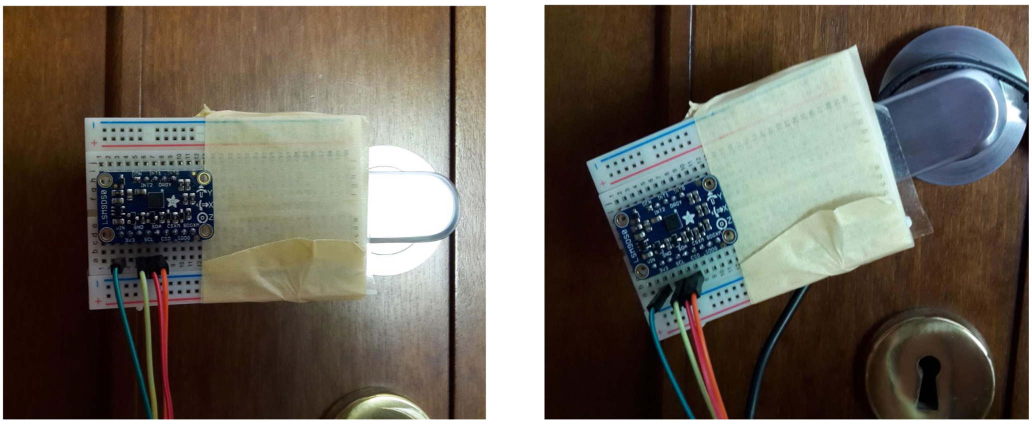
To our knowledge, the work presented in this chapter is the first step towards a behavioral biometric-based bimodal user authentication scheme that promises higher convenience and security over the conventional authentication schemes.

5.3 Step & Turn: User Authentication System

This section presents the experimental setup and hardware details of the Step & Turn user authentication system for smart homes and offices.

5.3.1 Experimental Setup

We created a smart office setup by fixing the hardware to the door handle in our lab. As depicted in Figure 5.2, the hardware is installed on the door's interior handle that can be rotated by the door exterior handle. The Adafruit LSM9DS0 hardware (refer 5.3.2) interfaced with an Adafruit Trinket M0 micro-controller for programming and controlling, is mounted on a breadboard and fixed to the door handle. Thus, the hardware installation does not alter the usage pattern of the door handle for their users, to open the door from outside.



(a) Locked position

(b) Unlocked position

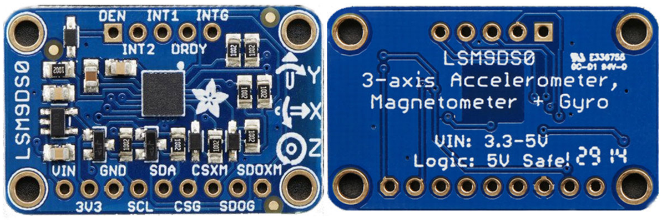
Figure 5.2: Hardware installation on the door handle, in our lab.

This setup enables us to record the hand-movement of users as they open the door from outside by rotating the door exterior handle to enter our office. Despite, the hardware is attached mechanically to the door handle (not embedded inside the handle assembly), it still replicates the conceptual model allowing us to conduct the experiments, successfully.

However, for footstep data, we utilized the data collected by Rodriguez et al. [268, 267]. They created a footstep pressure-data acquisition system by mounting 88 high-density piezoelectric sensors on a printed circuit board (PCB) of size 30 by 45 cm. These sensors are then placed under 2 separate doormats to capture users' single stride, i.e., left and right footstep pressure data. Subsequently, when users step on these 2 independent doormats, their left and right foot pressure data are recorded. We assumed that the doormats are installed in front of our smart office door fitted with the smart handle, as illustrated in Figure 5.1.

5.3.2 Hardware Details

We used the Adafruit 9-DOF Breakout Board - LSM9DS0[1] to register users hand-movements while they turn the door handle to open the door. This chip consists of three sensors, namely, accelerometer, magnetometer, and gyroscope (refer Figure 5.3). Additionally, it has a small form factor (see Table 5.1), with a dimension of 33mm length, 20mm breadth, and 2mm thickness.



Dimensions: 33mm x 20mm x 2mm
or 1.30" x .79" x .08"
Weight: 2.3g

Figure 5.3: Adafruit 9-DOF Accel/Mag/Gyro+Temp Breakout Board[1].

The 3-axis accelerometer tells how fast the board is accelerating in 3D space or which direction is down towards the Earth by measuring gravity. The 3-axis magnetometer is used to detect the magnetic north by sensing

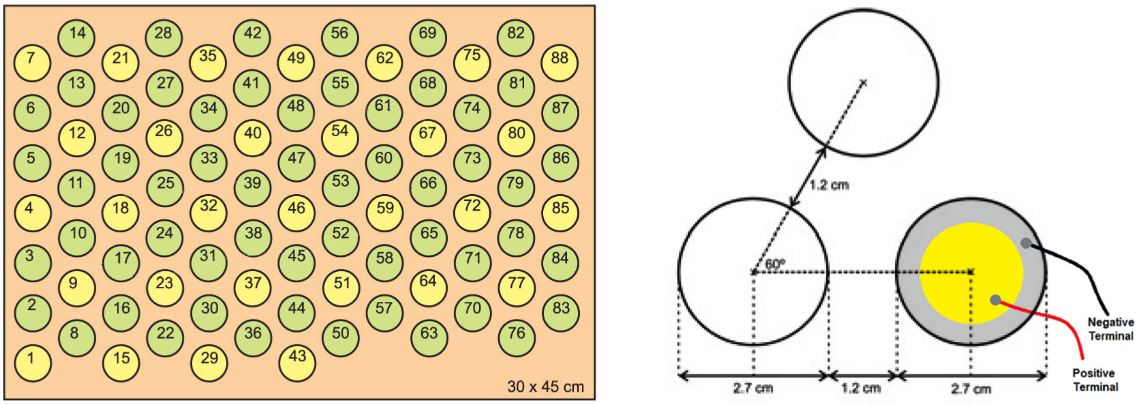
[1] https://www.adafruit.com/product/2021

Table 5.1: LSM9DS0 sensors specifications.

Sensor	Axis	Adjustable range	Resolution
Accelerometer	X, Y, Z	±2 g, ±4 g, ±8 g, ±16 g	16 bits @9600 bps
Magnetometer (compass)	X, Y, Z	±4, ±8, ±12, ±16 gauss	13 bits @9600 bps
Gyroscope	X, Y, Z	±245, ±500, and ±2000 °/sec	16 bits @9600 bps

from where the strongest magnetic force is coming. Lastly, the 3-axis gyroscope measures the spin and twist.

Rodriguez et al. [268, 267] deployed high-density piezoelectric sensors with a sampling frequency of 1.6 kHz to acquire footstep pressure data. Piezoelectric sensors measure a differential voltage output that is directly proportional to the applied pressure on a piezoelectric material.



(a) Sensors arrangement

(b) Sensors geometry

Figure 5.4: Piezoelectric sensors for a doormat of size 45 by 30 cm.

Figure 5.4a and Figure 5.4b depicts the arrangement and geometry of 88 sensors for a 45 by 30 cm size doormat used for footstep data collection by Rodriguez et al. [268, 267]. The diameter of each sensor is 2.7 cm. The adjacent sensors are separated by a distance of 1.2 cm at an angle of 60°to provide a compact layout with uniform inter-sensor distance. Table 5.2

presents some specifications of the latest piezoelectric sensors available in the market.

Table 5.2: Piezoelectric sensors specifications.

Property	**Value**
Impedance	$\leq$ 500 Ω
Operating Temperature	$-20\,^{\circ}C\ to\ +60\,^{\circ}C$
Strain sensitivity	$5V/\mu\epsilon$
Material used	Quartz
Sampling Rate	1.6 kHz

5.4 Methodology

In this section, we present the methodology to design user authentication scheme by using hand-movements and footsteps biometric. Both the hand-movement and footsteps biometric data of a user can be collected unobtrusively, which is a requisite criterion to design a usable user authentication scheme [92, 32, 267].

5.4.1 Datasets

We evaluated STEP & TURN on a chimerical dataset of 40 users by combining the hand-movement and footstep data. For hand-movement data collection, 40 persons volunteered and provided consent for their behavioral biometric data collection. The volunteers were mainly university students and staff with a diversified background. We strictly adhere to ethics and data protection guidelines [86] and followed the process described in Section 4.4.1 in getting participants' consent. As illustrated in Figure 5.1, the participants were required to step on a doormat and turn the door handle downwards from its rest position. Each participant performs this step 40 times to test our prototype.

To model the user's hand-movement trajectory in 3-D space, X, Y, and Z data streams are recorded from the three sensors at 9600 bits per second (refer Section 5.3.2). Generally, door handles are not rigid at the hinge, therefore, the sensors register both the horizontal micro-movement and the vertical movement. Thus, the hand-movement dataset contains 4 raw X, Y, Z, and M data streams per sensor.

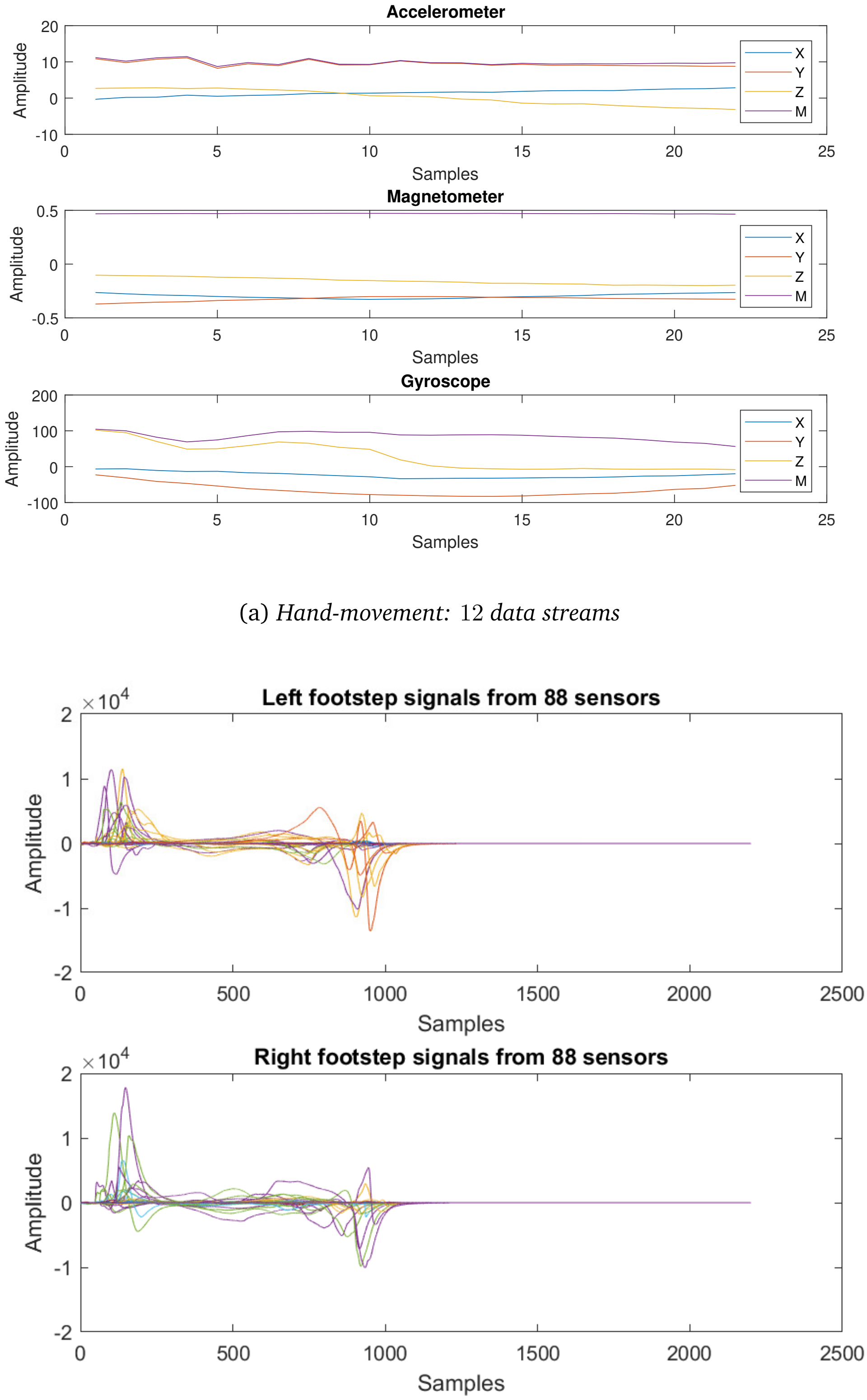
The 4^{th} dimension, called as magnitude, is mathematically derived for each sample (X, Y, Z) by using Equation 5.1.

$$M = \sqrt{(X^2 + Y^2 + Z^2)} \tag{5.1}$$

Where, M is the magnitude and X, Y, and Z are the X, Y, and Z coordinates of each sensor sample in 3-D space.

For footstep data, we rely on the Swansea University Speech and Image Research Group footstep dataset [268, 267]. It is worth mentioning that participants were allowed to walk over the footstep sensors by wearing footwear (shoes, trainers, boots, barefoot, etc.) and carrying weights such as office bags, which makes the collected dataset more realistic. This dataset consists of left and right pressure amplitude recorded from 88 pressure sensors (refer Section 5.3.2) at the sampling rate of 1.6 kHz. Thus, a single user footstep contains left and right foot pressure data of size 88×2200 each.

Figure 5.5a and 5.5b show a user hand-movement and footstep pressure data, respectively. As the two modalities, i.e., a user's hand-movement and footstep, are mutually independent of each other, we augmented the pressure-based footstep samples of 40 users to our collected hand-movement data to form a single dataset of 40 users with 40 observations per user. One clear benefit of the chimerical dataset is that biometric traits for each label are disjointed restricting our bi-modal classification model to establish any strong linkage to the volunteers, thus, ensuring



(a) *Hand-movement:* 12 *data streams*

(b) *Footstep:* 2 × 88 *data streams*

Figure 5.5: Each modality raw data streams for a single observation.

their privacy.

5.4.2 Feature Extraction

We computed statistical information from each raw data streams. Univariate statistical properties, i.e., min, max, mean, standard deviation, kurtosis, or skewness [93]. Extracting statistical features reduce the dimensionality of raw data, improve the signal-to-noise ratio, and enhance classifier performance.

5.4.2.1 Hand-movement

For each data-stream, 6 independent features, namely, min, max, mean, standard deviation, kurtosis, and skewness are computed, by using Equation 5.2.

$$
\begin{aligned}
Minimum\ (Min) &= \min_{i=1}^{N} S_i \\
Maximum\ (Max) &= \max_{i=1}^{N} S_i \\
Mean\ (\mu) &= \frac{1}{N}\sum_{i=1}^{N} S_i \\
Standard\ Deviation\ (\sigma) &= \sqrt{\frac{\sum_{i=1}^{N}(S_i\ -\ \mu)}{N}} \\
Kurtosis\ (k) &= \frac{\frac{1}{N}\sum_{i=1}^{N}(S_i\ -\ \mu)^4}{\sigma^4} \\
Skewness\ (s) &= \frac{\frac{1}{N}\sum_{i=1}^{N}(S_i\ -\ \mu)^3}{\sigma^3}
\end{aligned}
\tag{5.2}
$$

Where, S_i is the i^{th} sample in a data-stream. N is the number of samples in a data-stream. Min and Max are the minimum and maximum values respectively, in a given data-stream. Mean (μ) is the average of all samples. Standard deviation (σ) is the square root of the variance. Kurtosis (k) measures the degree of peakedness of a data-stream that helps in detecting the outlier-proneness of the distribution. Skewness (s) measures the degree of asymmetry of a data-stream from its mean value.

We extracted 6 statistical features from each data-stream. As there are 4 data-streams per sensor so 24 (4×6) features are obtained per sensor, as shown in Table 5.3.

Table 5.3: Statistical features extracted from a sensor for the hand-movement.

#	**Statistical features**					
1-6	Min_X	Max_X	μ_X	σ_X	k_X	s_X
7-12	Min_Y	Max_Y	μ_Y	σ_Y	k_Y	s_Y
13-18	Min_Z	Max_Z	μ_Z	σ_Z	k_Z	s_Z
19-24	Min_M	Max_M	μ_M	σ_M	k_M	s_M

Thus, with 3 sensors, a total of 72 $(3 \times 4 \times 6)$ statistical features are extracted. The final feature vector for hand-movement consists of 73 features in total including 72 statistical features and handle-movement action time [93].

5.4.2.2 Footstep

To obtain the footstep features, we first transformed each pressure amplitude array of size 88×2200 into 4-independent time-series arrays, namely, Spatial Average (S_{ave}), Ground Reaction Force ($GRF_{cumulative}$), Upper (S_{upper}) and Lower (S_{lower}) Contours of size 1×2200 each [66], by using Equation 5.3.

$$S_{ave}[t] = \sum_{i=1}^{N} S_i[t] \qquad GRF_{cumulative}[t] = \sum_{t=1}^{T_{max}} S_{ave}[t]$$
$$S_{upper}[t] = \max_{i=1}^{N} S_i[t] \qquad S_{lower}[t] = \min_{i=1}^{N} S_i[t] \tag{5.3}$$

Where, $S_i[t]$ is the differential pressure sample from the i^{th} piezoelectric sensors at the time t. N is the total number of piezoelectric sensors, i.e., 88. Then, 6 statistical features are computed from each time-series array by using Equation 5.2. In total, we get 48 statistical features (8×6) from 8 time-series arrays that were obtained from both left and right pressure amplitude arrays.

Ground Reaction Force (GRF_i) per sensor is computed by accumulating each sensor pressure amplitude from time T_1 to T_{max} by using 5.4.

$$GRF_i = \sum_{t=1}^{T_{max}} S_i[t] \tag{5.4}$$

Where, $S_i[t]$ is the differential pressure sample from the i^{th} piezoelectric sensors with i ranges from 1 to 88 and t ranges from 1 to 2200. In total, 176 features are obtained from both left and right pressure amplitude arrays.

Finally, we extracted 73 features from hand-movement to turn the door handle and 224 features ($48 + 176$) from both left and right foot differential pressure against time collected from the piezoelectric sensors.

5.4.3 Feature Selection

The feature selection process improves the performance of classification models by maximizing the classifier's accuracy and reducing their computation time. Gupta et al. [95] analyzed 3 different filter-based feature selection methods, namely, 1-Nearest Neighbour leave-one-out rank (R-NN) method, Information Gain Attribute Evaluation (IGAE) method, and Relief-based feature selection (RBFS) method on a similar feature-set. And, they find that the performance of the RBFS method is slightly better than the other two methods. Thus, we considered the Relief-based feature selection method to obtain the most productive feature subset to be used as the users' training template for constructing the classification model.

The advantages of RBFS are: 1) they generate a unified view on the estimation of the features in the classification, 2) they are able to determine conditional dependencies between features, and 3) they are relatively faster (with asymptotic time complexity of order $\mathcal{O}\ (instances^2 \times features)$) than the other feature selection methods [93, 263].

We fused 73 features from hand-movement and 224 features from both left and right foot differential pressure versus time to determine the most productive feature subset. RBFS compute ranks and weights of features to derive feature statistics using the concept of nearest neighbors [169] as shown in Equation 5.5.

$$[RANKED, WEIGHT] = relief(X, Y, K) \tag{5.5}$$

Where, $X\ (m \times n)$ is a given 2-d dataset, $Y\ (m \times 1)$ is the response vector, and K is a number of nearest neighbors. $RANKED$ are indices of columns in X ordered by attribute importance, meaning $RANKED[1]$ is the index of the most important feature. $WEIGHT$ are features weights ranging from -1 to $+1$ with large positive weights assigned to most important attributes.

Figure 5.6 shows the plots between features and their weights obtained by the RBFS method. We picked the top 33% features (98), which is determined empirically, out of the full feature-sets (297) demarcated by the

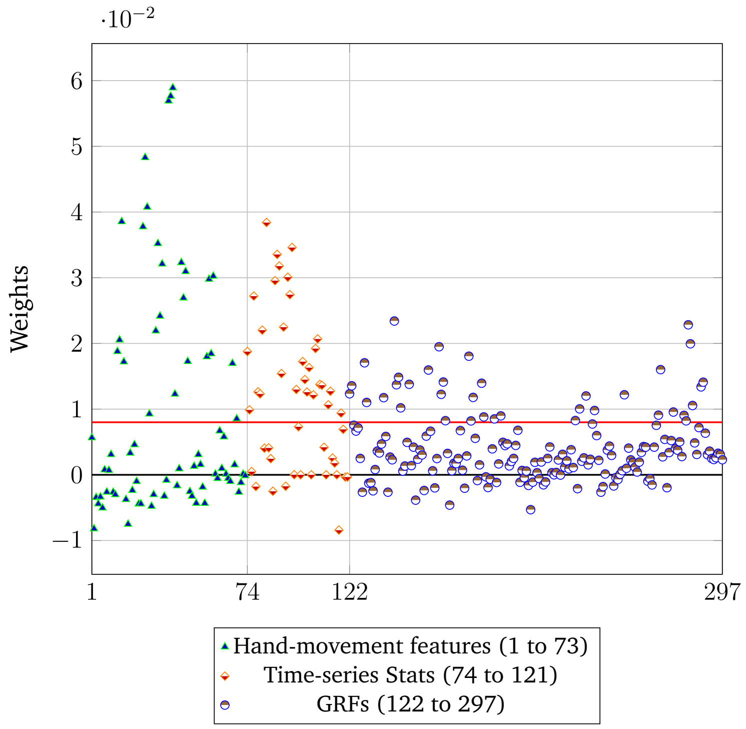


Figure 5.6: Plot between features vs. weights.

red line in Figure 5.6. We tested and validated our system on both the full feature set and selected feature set to achieve an optimal classification model.

5.5 Validation

In this section, we explain our authentication model that is built by using the multi-class classification approach. Each user is profiled as the "owner" and the remaining users as "impostors" for validation purposes. Each of the 40 users is validated in two scenarios, i.e., (i) a verifying legitimate user scenario, and (ii) an attack scenario. The results are reported in terms of true acceptance rate (TAR), false acceptance rate (FAR), and Receiver-Operating Characteristic (ROC).

5.5.1 User Authentication Model

We construct a multi-class classification model by using Matlab's PRtools[2]. We utilize 3 different types of classifiers (refer table 5.4), namely, Random Forest classifier, Support Vector Machine, and Fisher's Least Square Linear Discriminant classifier, to construct the authentication model.

Table 5.4: An overview to classifiers.

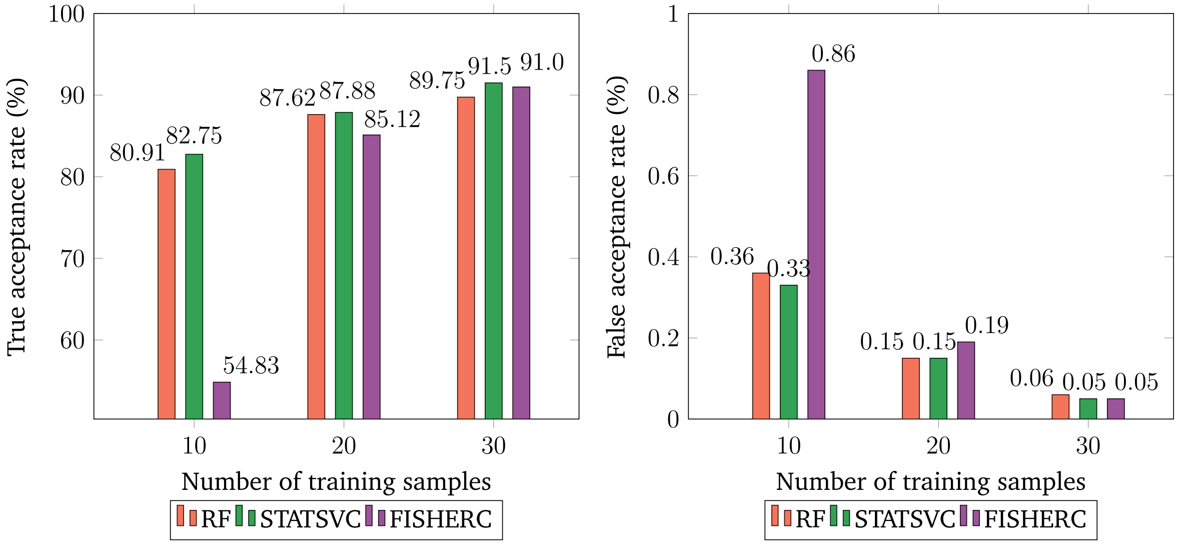
Classifier	**Description**
Breiman's random forest (RF) [70]	The classifier ensembles a decision forest by generating a number of decision trees on random feature subsets of the given dataset. While splitting a node in the decision tree, it searches for the best feature among a random subset of features rather than searching for the most important feature. Then, the decision forest aggregates the votes from all the decision trees to decide the final class of the new query. Typically, it uses averaging to improve the predictive accuracy and to control over-fitting.
Stats support vector classifier (STATSVC) [206]	The support vector machines (SVM) are a discriminative classifier that segregates the classes in a given dataset by constructing an optimal hyperplane. Internally, SVM uses different kernels, e.g., linear, quadratic, polynomial, radial basis function (RBF), and sigmoid, etc., to construct the hyperplanes. SVM possesses a special property to minimize the empirical classification error and maximize the geometric margin simultaneously, hence it is also known as maximum margin classifiers.
Fisher's Least Square Linear Discriminant (FISHERC) [205]	The classifier estimates linear discriminant function to characterize or separate two or more classes in a given dataset. The multi-class implementation uses the one-against-all strategy by selecting a decision function that maximizes the distance between classes.

To evaluate the performance of the model, the dataset consisting of 40 samples per class is divided into 2 independent and disjoint training and testing subsets. The model is first trained on the training dataset containing T training samples. We used 3 different number of training samples (T), i.e., 10, 20, and 30, to evaluate the model effectiveness. Then, the testing dataset with $40 - T$ samples is used to test the model for all the 40 classes.

[2] http://www.37steps.com

5.5.2 Results

The results are reported in terms of TAR, and FAR for legitimate users, and the impostors, respectively. RF gives the best TAR of 97.25% (@FAR = 0.01%) with 30 training samples on selected feature-set obtained by Relief-based feature selection method. With 10 and 20 training samples, the RF classifier gives the TAR of 93.25% (@FAR = 0.12%) and TAR of 94.62% (@FAR = 0.04%), respectively. Figure 5.7 and 5.8 present the performance of all the classifiers on the full features and Relief-based feature selection method.



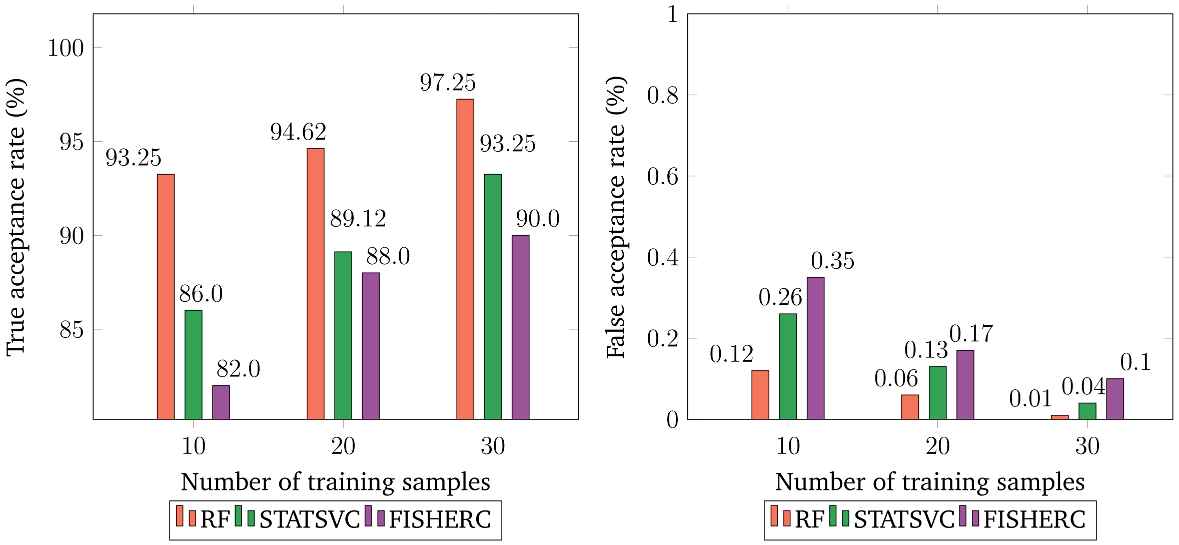
(a) *TAR for Full features*

(b) *FAR for Full features*

Figure 5.7: Results of different classifiers with 10, 20, and 30 training samples for full features (297).

Figure 5.9 presents the ROC curves for the RF classifier plotted for all the 40 classes with 10, 20, and 30 training samples with full and selected feature set obtained by RBFS method.

The two-dimensional graphs shown in Figure 5.9 plots the TAR on the Y-axis and FAR on the X-axis showing the relative trade-offs between the true positives and the false positives [93]. Coordinate $(0, 0)$ represents



(a) *TAR for RBFS selected features*

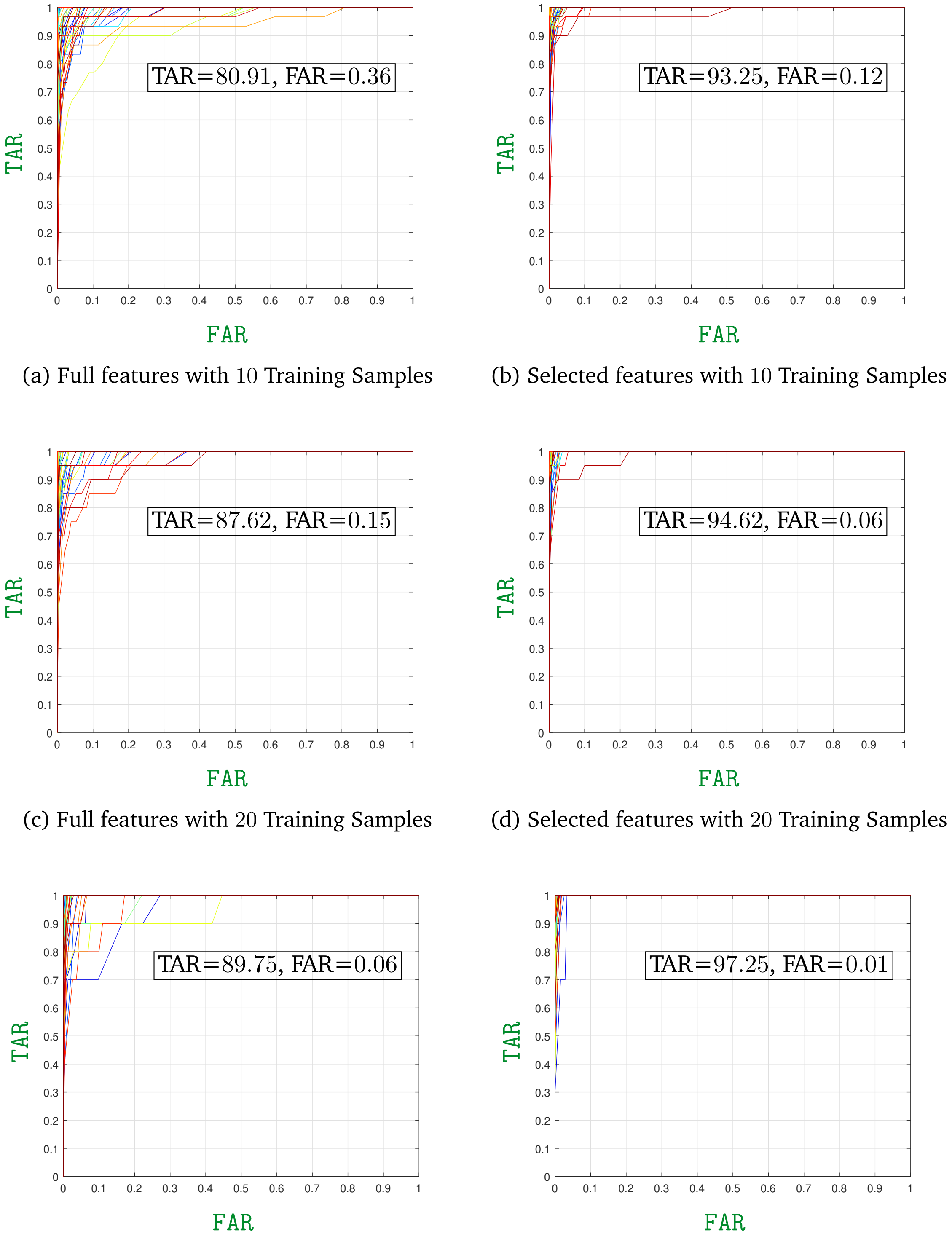
(b) *FAR for RBFS selected features*

Figure 5.8: Result of different classifiers with 10, 20, and 30 training samples for selected features (98) by using RBFS method.

the strategy of never issuing a positive classification; such a classifier commits no false-positive errors but also determines no true-positives. However, the opposite strategy, of unconditionally issuing positive classifications, is represented by coordinate $(1, 1)$. Whereas, coordinate $(0, 1)$ represent the perfect classification strategy of maximizing TAR and minimizing FAR. In Figure 5.9, it can be observed that with the increase in the number of training samples classifier performance also tends to improve.

5.6 Usability Assessment

This section presents the usability analysis of the Step & Turn system. Usability assessment becomes the strategic criteria to establish the efficiency, effectiveness, and satisfaction of the user authentication methods [24]. We used the System Usability Scale (SUS) tool [28] to perform usability assessment of Step & Turn system as explained in Section 2.3.3.3. As shown in Appendix B, we included 3 more questions



(a) Full features with 10 Training Samples

(b) Selected features with 10 Training Samples

(c) Full features with 20 Training Samples

(d) Selected features with 20 Training Samples

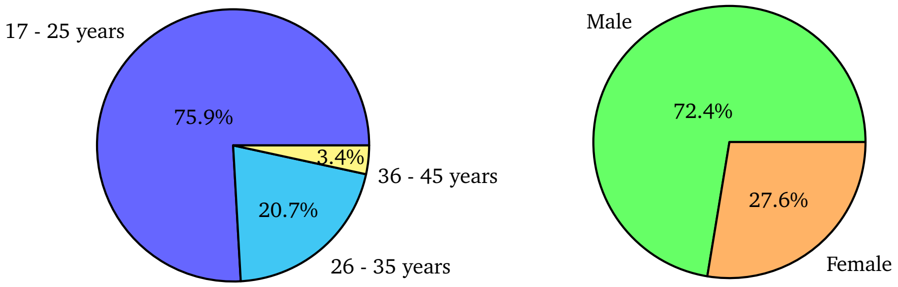
(e) Full features with 30 Training Samples

(f) Selected features 30 Training Samples

Figure 5.9: A comparison between ROCs of all the classes obtained for RF classifier with 10, 20, and 30 training samples.

related to the number of training samples, age-range, and gender.

We received the survey response from 29 participants, and the participants' demographic statistics are displayed in Figure 5.10.



(a) *Participants age group*

(b) *Participants gender*

Figure 5.10: Demographic statistics.

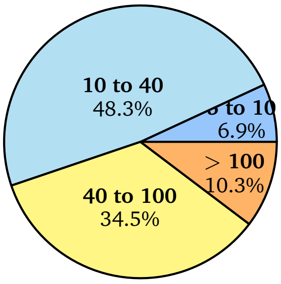


Figure 5.11: Training samples for user biometric template creation.

The number of training samples required to create users' biometric trait template is a significant criterion for a usable user authentication system design [132, 97]. The survey poll for training samples, as depicted in Figure 5.11 exhibits that 6.3%, 48.3%, 34.5%, and 10.3% of participants are happy to provide $5-to-10$, $10-to-40$, $40-to-100$ samples, and more than 100 samples, respectively to train the system.

The ten SUS questionnaire and the responses obtained from the 29 participants are displayed in Figure 5.12. Overall, our scheme achieves the SUS score of ≈ 76.72, which is significantly above the standard average score of 68 [156]. Thus, it can be interpreted from the survey results that the

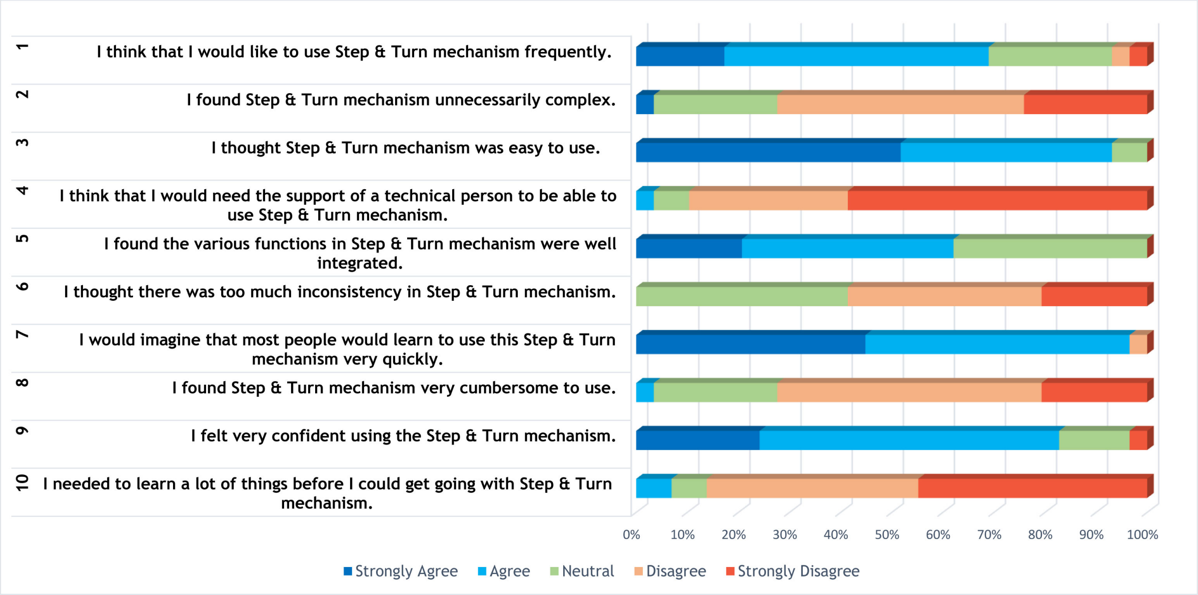


Figure 5.12: SUS questionnaire and users responses.

majority of users are satisfied with the STEP & TURN user authentication system.

5.7 Summary

STEP & TURN offers a secure and usable user authentication scheme for smart ecosystems unlike conventional authentication schemes, it does not require the active participation of the user.
We validated our solution for a multi-class classification scenario. We achieved the TAR of 97.25% (@FAR of 0.01%) by using RF classifier on a chimerical dataset of 40 users. We acknowledge that the accuracy must not be the only criteria for the real deployment of our solution. It is equally important to deploy doormats fitted with pressure sensors at the door entrance and to integrate the hardware inside the handle assembly without affecting the form and appearance of the door handles, for mass production.

Chapter 6

DRIVERAUTH: A Risk-based Multi-modal Biometric-based Driver Authentication Scheme for Ride-sharing Platforms

DRIVERAUTH is a novel risk-based multi-modal authentication scheme, to make the on-demand ride and ride-sharing services secure and safer for riders. DRIVERAUTH utilizes three biometric modalities, i.e., swipe, *text-independent* voice, and face, in a multi-modal fashion to verify the identity of driver-partners at the time of ride-booking to address customers safety and security.

We published this works in [93]: *Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. "DriverAuth: A risk-based multi-modal biometric-based driver authentication scheme for ride-sharing platforms." Computers & Security (COSE), 83 (2019): pp. 122-139, Elsevier*, and [94]: *Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. "DriverAuth: Behavioral biometric-based driver authentication mechanism for on-demand ride and ridesharing infrastructure." ICT Express, 5.1 (2019): pp. 16-20, Elsevier*.

6.1 Introduction

On-demand ride and ride-sharing services have revolutionized the point-to-point transportation market. Customers can book these rides services on short notices with 24×7 availability in all major cities in the world. Alone, Uber [56] and Lyft [57] are providing over 18 million rides per day, and they are rapidly gaining acceptance among customers worldwide.

Customers can book their rides easily, through dedicated smartphone-based ride-offering applications provided by different companies, which are downloadable at popular application stores like Play-store, App-store. Service providers rely on well-proven client-server infrastructures to design their systems. The client is a smartphone-based application used for: i) registering riders and drivers, ii) connecting drivers with riders, iii) car-sharing to share the expenses, minimize traffic congestion and saving traveling time, and iv) allowing customers to book their rides. The server typically, run by multi-national companies such as Uber, Lyft, BlaBlaCar, Ola, manages drivers and customers registrations, allocates ride assignments, sets tariffs, guarantees payments, ensures safety and security of riders, etc.

On-demand ride and ride-sharing services have facilitated quick business opportunities, allowing individuals to become partners (drivers) to offer rides to customers. However, the reliability of drivers has emerged as a critical problem, and as a consequence, issues related to riders' safety and security have started surfacing. News related to fake drivers and assaults by dishonest drivers is a severe safety and security risk for the riders [274]. Further, being a lucrative business and easy to start, on-demand rides and ride-sharing services are attracting people also with unclean police records to become driver-partners using false identities [10].

Ride-sharing companies rely on government-issued documents, e.g., passports, driver licenses, etc., to verify their drivers-partners identity and their eligibility to drive. Generally, this verification is performed only once at the time of registration. However, forging these documents is not difficult [3], as well as, all the countries do not use the same security standards to issue them. Often ride-sharing services support drivers' rating services on social media such as Facebook, LinkedIn, Twitter, and Google Plus can be easily manipulated, thus, not always reliable [12, 155, 180]. The lack of robust driver verification mechanisms has opened a room to an increasing number of misconducts (i.e., drivers subcontracting ride-assignments to an unauthorized person, registered drivers sharing their registration with other people whose eligibility to drive is not justified, etc.) [116, 141, 266].

All these factors have contributed to an increasing number of incidents involving on-demand and shared rides in recent years [274, 22]. This trend has motivated ride-sharing companies to implement more rigorous checks on their drivers [262]. The checks that have been implemented, however, did not stop the abuses, e.g., dishonest drivers creating multiple accounts with forged documents [164]. These abuses are becoming also a liability concern [43], thus, the search for new, secure, and robust driver verification mechanisms becomes extremely important. Despite background checks on the drivers at the time of registration, the system lacks a robust mechanism [204], to verify the driver's identity each time she is offering a ride [266]. Some companies have introduced a real-time identity check that requires drivers to take a selfie before going online to drive [260] but not before each ride.

These open issues motivate the design of a new risk-based verification mechanism that can verify a legitimate driver at the time of every new registration and ride-booking, and thus, minimize the associated risks of abuses. An important requirement that any new driver authentication scheme must satisfy is not to alter the existing work-flow to pose a usability burden to drivers.

DRIVERAUTH authenticates drivers by leveraging three biometric modalities, i.e., swipe, *text-independent* voice, and face, for verification purposes in a multi-modal fashion. Multi-modal systems are expected to be more reliable and accurate than unimodal systems, to verify a user. Furthermore, studies [17, 88, 149] have shown that multi-modal systems are more resilient to common attacks, e.g., presentation-, mimic-, replay-, random-attacks in comparison to unimodal systems.

6.1.1 Contributions

The main contributions are as below:

- The proposal of DRIVERAUTH - a multi-modal system that pro-actively verifies the drivers' identity every time drivers accept a new ride-booking. The proposed mechanism collects three biometric modalities, e.g., swipe gestures, *text-independent* voice and face, while they interact with the dedicated driver-application, to verify the drivers' identity. DRIVERAUTH that can minimize the threat(s) posed by fake and malicious drivers. Hence, provisioning the safety and security of riders.

- Collection of swipe and voice data of 86 participants and shared publicly for research work [96].

- Experimental evaluation of DRIVERAUTH on the dataset of 86 users.

6.1.2 Chapter Organization

The rest of the chapter is organized as follows: Section 6.2 covers the related work. Section 6.3 describes the problems in the existing driver registration process and the risk involved in this system along with the need for risk-based user verification method and the considered threat model. Section 6.4 presents DRIVERAUTH design including the verification process at the time of new registration and ride-booking assignment. Section 6.5 discusses the methodology used to collect the dataset, to extract features, to concatenate and selection of the best features from the chosen modalities. Section 6.6 covers the details of the experiments, the classification method, and presents the performance evaluation and the obtained results.

6.2 Related Work

Face recognition is one of the most widely accepted biometric modality mainly because it provides high recognition rates. Thus, Uber has introduced “Real-Time ID Check” - a face recognition system developed by Microsoft, to verify the identity of their registered drivers [260]. The system collects the face images of the person registering as driver-partner, extracts facial features, and stores them in the database for subsequent verification purposes. Only a subset of randomly-selected driver-partners is asked to verify themselves using “Real-Time ID Check”. Selected drivers are requested to take a selfie, then, this query image is compared with reference images to verify their identity. Subsequently, the system takes necessary action, i.e., allows/disallows drivers to offer rides, based on the obtained verification results from the face recognition algorithm. Uber claims 99% success rate of this mechanism, however, they have not yet published any details related to their systems’ robustness against presentation attacks and about liveness detection.

Table 6.1: Multi-modal (combination of face, voice, or touch) user authentication schemes.

Reference	Modalities Used	Algorithms Used	Dataset Size	Performance
Gofman et al. [88]	Face, Voice	Latent Dirichlet allocation (LDA) fusion method	54	EER=2.14%
Soltane et al. [234]	Face, Voice	Finite Gaussian Mixture Model (GMM) based on Expectation Maximization (EM) using score-level fusion	30	EER=0.087%
Wang et al. [271]	Face, Voice	Quantization Index Modulation (QIM) and Gaussian Mixture Models (GMM)	295	EER=2.76 – 3.79%
Menzai et al. [177]	Face, Voice	Dempster-Shafer theorem using belief function	295	HTER=0.433 – 2.875%
Kim et al. [143]	Face, Voice	Generalized cross correlation (GCC) algorithm and AdaBoost algorithm on Local binary pattern	-	Accuracy=95%
Menzai et al. [178]	Face, voice	Belief functions and Particle Swarm Optimization (PSO)	295, 52	EER=0.5% to 0.9%
Feng et al. [72]	Finger gesture Authentication System (FAST)	Random Forest classifier	40	FAR=4.66%, FRR=0.13%
Aronowitz et al. [6]	Fingertip-based writing, Face and Voice	Dynamic time warping (DTW)	32	EER=0.1% at quiet place, and 0.5% in noisy surroundings
Koreman et al [149]	Voice, face and signature	Gaussian mixture models (GMMs)	82	EER=2%
Buriro et al. [33]	Touch-timings and hands-movements to holding phone	Random Forest (RF)	95	TAR=96
Eastwood et al. [64]	Face, iris, and fingerprints	Belief (Bayesian) networks	-	-

Multi-modal biometric factors can remarkably improve the identity verification accuracy of a system by combining the pieces of evidence extracted from single modalities [135]. Multi-modal systems are also more resilient against spoofing in comparison to unimodal ones [194]. Our system is the first multi-modal biometric authentication scheme to address driver's authentication problem for ride-sharing services. Similar proposals exist but only for user authentication on smartphones. Table 6.1 summarizes the most relevant multi-modal user authentication solutions on smartphone.

Proteus, proposed by Gofman et. al. [88], is a bi-modal biometric verification system based on face and voice features, for mobile devices. This scheme extracts principle components using Principal Component Analysis (PCA) and Mel Frequency Cepstral Coefficients (MFCC) from face and voice modality, respectively, to construct a bi-model system. The system was evaluated on a dataset of 54 users and it achieved an Equal Error Rate (EER) of 2.14% using the latent Dirichlet allocation (LDA) fusion method. Another bi-modal approach [234] incorporates finite Gaussian Mixture Model (GMM) based on Expectation-Maximization (EM) and applies score-level fusion to fuse face and voice modalities. They achieved an EER of 0.449% for face and 0.003% for voice modalities, in unimodal settings, and their bi-modal settings yielded an EER of 0.087%, on the dataset of 30 participants. These experiments clearly reflect the potential of multi-modal biometrics to enhance the verification accuracy on mobile devices.

Swiping is a very common gesture required to interact with mobile devices' touchscreen. It is a collection of touch-points generated while the user dragged her finger on the smartphone touchscreen [176, 219, 278]. Feng et al. [72] proposed a Finger gesture Authentication System using Touchscreen (FAST). They applied the Random Forest classifier and achieved a FAR of 4.66% and False Reject Rate (FRR) of 0.13% for the continuous post-login user authentication on a dataset of 40 users. Another proposal by Aronowitz et al. [6], combines user's fingertip-based writing on multi-touch screens with face and voice features and uses dynamic time warping (DTW) engine for user verification. They achieved an EER of 0.1% at a quiet place, and 0.5% in noisy surroundings, on their collected dataset of 32 users (20 males and 12 females).

Koreman et al. [149] leverage voice, face, and signature modalities, for user authentication on mobile devices. This approach yielded an EER of 2% using Gaussian mixture models (GMMs). The system utilized BANCA audio-visual database [201] and BIOMET on-line signature database [85] comprising of the data collected from 82 and 84 subjects, respectively. The authors also checked each modality in unimodal settings and achieved an EER of 28%, 5%, and 8%, for face, voice, and signature modalities, respectively. The fusion of three modalities enhanced the system accuracy and reduced the EER to just 2%.

Liveness detection is generally deployed to detect spoofing attacks. According to Zhang et al. [284], mobile audio hardware can be used to exploit the articulatory gesture of a user to detect liveness and their proposed "VoiceGesture" system achieves 99% detection accuracy at approximately 1% EER. Swipe gesture is the result of a user subconscious muscle memory involving a sweeping movement on the touchscreen developed over a period of time due to the constant use of a smartphone. Swipe gestures are arguably considered hard to be imitated and the impostor's attempts are easily detectable [80]. Also, swipes have no explicit visual indicators which make it furthermore resistant to mimicry attacks [61]. Lastly, it is comparatively easier to perform liveness detection on faces because some of the robust liveness detection methods are already available [144], to prevent face spoofing attacks [193].

Our proposed scheme DriverAuth is different from existing state-of-the-art in several ways: firstly, DriverAuth is a client-server-based multiuser (`multiclass`) verification solution in contrast to the existing multimodal systems [88]. More specifically, we model this as a multi-class classification problem (classifier training with multiple users) whereas, the existing approaches dealing with smartphone user authentication are one-class or binary class classification problems. Secondly, DriverAuth utilizes both physiological and behavioral biometric modalities, i.e., swipe, face, and *text-independent* voice, equipped with liveness detection as a result more resilience to spoofing.

6.3 Problem Description

On-demand ride and ride-sharing services have revolutionized the point-to-point transportation market, in a short period. Technology-based companies, e.g., Uber, Ola, Lyft, Blablacar, Sidecar, etc., connect customers and drivers using dedicated smartphone-based applications. Customers interested in the services and individuals aspiring to become driver-partner can download these dedicated applications free-of-cost, available at online-app-stores, e.g., Play-store, App-store, Microsoft-store, etc.
To become a driver-partner, an individual needs to be older than 21 years old, should have a valid driving license, valid vehicle registration, clean driving record, and have no criminal history [261]. These background checks are performed by the service provider just once, before the registration. Once the individuals are accepted as driver-partners, they can accept rides' requests, reserved by customers, using dedicated driver-application on their smartphones, and perform their duty. Surprisingly, the system providers do not verify their drivers' identity while they accept a new ride, requested by the customers [182]. Thus, system providers are neither able to monitor fake drivers [116] nor they can curb dishonest drivers with multiple identities [273]. Therefore, the safety and security of the customers are always at risk, and this risk is increasing with the increasing number of abuses reported every year [274].
The safety and security of a customer is a huge challenge in on-demand ride and ride-sharing systems, despite being convenient, fast, and economical. Considering the volume of rides (alone, Uber and Lyft are providing over 18 million rides per day [56, 57]), even if only one rider in a million is victimized, this sum up to 18 victims per day. As driver-

partners can join and leave the service at any time without any obligation is difficult to deter abuses.

6.3.1 Threat Model

We consider two different types of malicious users in our scenario: the first type of adversary can impersonate a driver-partner by imitating a legitimate driver. The second type of attacker colludes with a legitimate driver-partner and share with him/her the registration to provide rides on behalf of the legitimate driver.

Both adversarial situations can be countered using DRIVERAUTH. DRIVERAUTH leverages swiping, voice, and face combined to verify the legitimate driver at run-time and would require the driver's presence every time she accepts a new ride request. Additionally, the fusion of the three modalities increases the resilience to common attacks, i.e., presentation, mimic, and replay attacks [17, 88, 149].

6.3.2 Risk-based Verification Mechanism

According to ISO 9000:2015 [127], *risk* is the "effect of uncertainty on objectives". The *objectives* can be defined as the strategic, tactical, or operational requirements pertaining to an ecosystem. Whereas, the *effect* can cause both positive or negative deviations on the objectives. A *risk-based verification mechanism* aims at determining uncertainties to minimize their effects on the set objectives.

At present, on-demand ride and ride-sharing services use the concept of simple verification mechanism [92], in which, users are verified at the time of entry only, and users are considered legitimate until they quit the system. However, with reference to the threat model, discussed in section 6.3.1, the drivers' verification at the time of each new ride-assignment becomes imperative, to ensure customers' safety and security. In that case, a simple verification concept does not suffice owing to their limitations to prevent potential risk hazards. Therefore, a risk-based verification mechanism could be a potential solution.

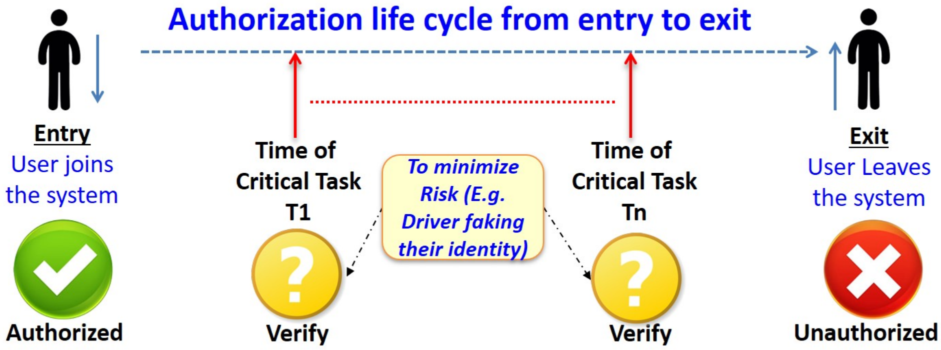


Figure 6.1: Risk-based verification mechanism.

The life cycle of a typical risk-based verification mechanism consists of users' authorization at the time of entry and their verification at every critical operation. As illustrated in Figure 6.1, users can be authorized to use the system by registering to it, i.e., $Entry$, and once they unregistered themselves, i.e., $Exit$, they are unauthorized to use the system. At the time of registration, users are added to the database for a reliable $1-to-1$ verification. Every time ($T_1...T_n$) users carry out a critical activity (e.g., accept a ride request) they are verified even though they are legitimate drivers. If an incident is reported, it is added to the incidents database tagged with the responsible user identity, for reference purposes.

The concept used in Risk Profiling tools [63, 153] to assess risk at different stages of a critical system can be applied here for proactive risk assessment [64] by analyzing the incidents database. This incidents database can be further utilized for Evidence Accumulation and Risk Assessment (EA&RA) to evaluate the driver's behavior in the past and present using special risk indicators [154].

6.4 Our Solution: DRIVERAUTH

DRIVERAUTH authenticates the drivers at the time of registration and at the time of new ride-assignments. Each service provider has its dedicated system and application for its driver-partners, however, the core functionalities are the same. Thus, DRIVERAUTH can easily be integrated into these systems and provide the required safety and security to customers.

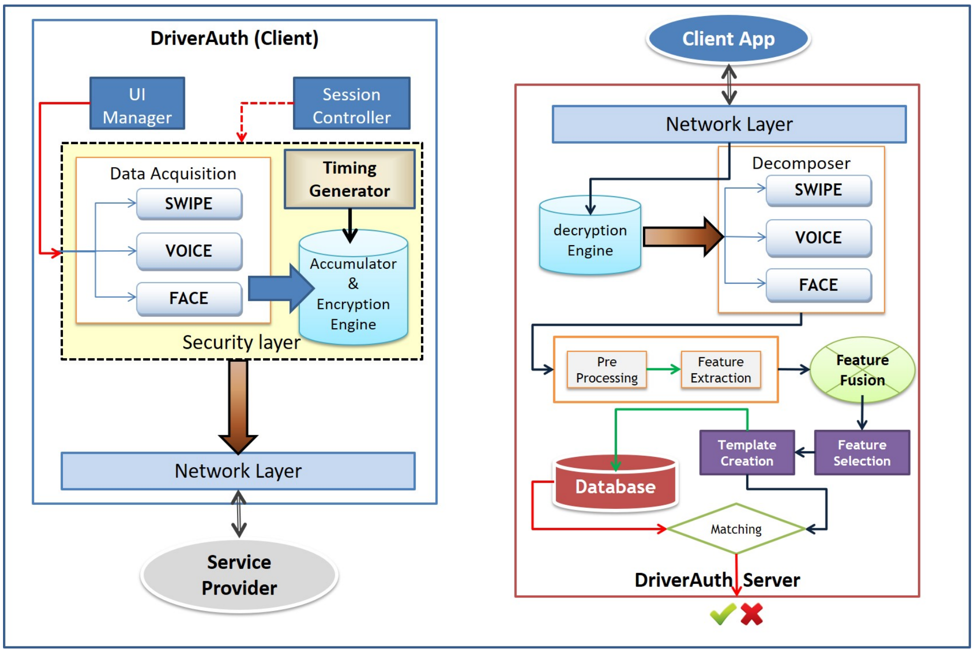


Figure 6.2: DRIVERAUTH architecture.

DRIVERAUTH uses the client-server architecture [94] as illustrated in Figure 6.2. The client application consists of a data acquisition module, an accumulator/encryption engine, and a timing generator. Data acquisition module collects the swipe data, voice-print, and face-image in a sequential manner using blocking-call-mechanism, i.e., the application allows to proceed only after it receives the required user's input. The operational details of the data collection process for driver verification are described in Section 6.4.3. The data collected, i.e., touch-points data, $2 - seconds$ voice-prints, and a face image, are temporarily stored by accumulator and encryption engine module for encryption, packaging, and time-stamping. With no delay, data is transferred to the server.

The server side consists of a) a decryption engine, b) a decomposer, c) signal preprocessing, d) features extraction module, e) feature fusion module, f) feature selection module, g) template creation module, and h) database module. The decryption engine decrypts the user-data as received from the client application, which is further decomposed into individual modalities. As the proposed scheme uses the multi-modal mechanism, features are fused and selected on a merit basis entailing the selection of only productive features for user authentication. The drivers' template is created based on the selected features subset and is then stored in the central database as training templates with a proper label. Later, a similar procedure is applied to the testing data to generate the testing template. To verify the identity of the claimant, the testing template is matched against the existing labeled training templates, present in the database.

6.4.1 DriverAuth Design

On-demand ride and ride-sharing systems have three primary stakeholders: a) centralized smartphone-based administration, b) customers and c) drivers, as illustrated in Figure 6.3.

DriverAuth verifies the person both at the time of registration and at new ride-assignments. A security layer is stitched to the driver application to collect the biometric modalities, e.g., voice, swipe gesture, and face. Simultaneously, the captured data (query input) is transferred to the server for the driver's identity verification. Also, this query input can be looked up in the stored database for any incident flagged against it.

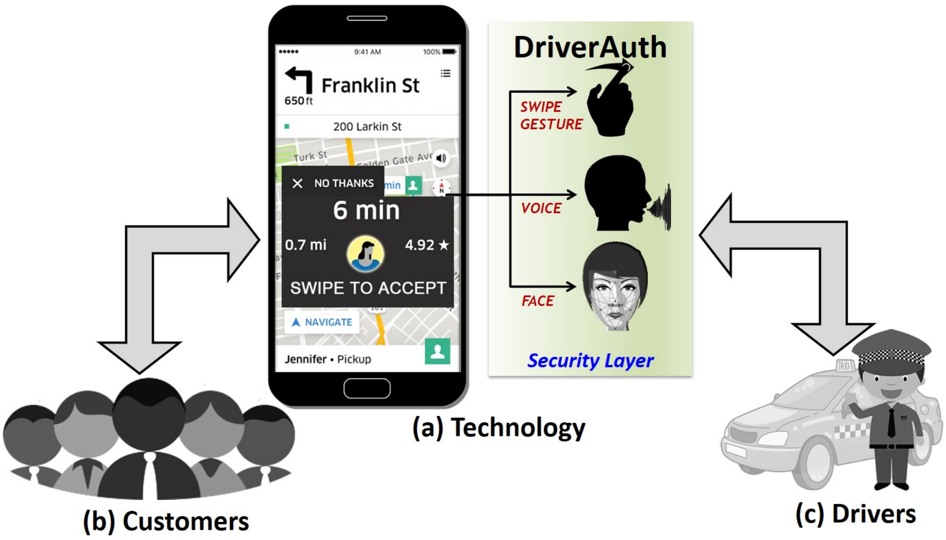


Figure 6.3: On-demand ride and ride-sharing system stakeholders.

6.4.2 Verification during Driver-partners Registration

Verification process during driver-partners registration is illustrated in Figure 6.4.

1. Individuals can apply to become drivers by filling the application form using dedicated driver-application (see Figure 6.4) on their smartphone.

2. During the registration process, DRIVERAUTH collects the swipe gesture, *text-independent* voice, and face samples of a person.

3. At the server (see Figure 6.4), query input is first compared with the stored driver-partner templates in the database. If this query input is positively verified, the registration is completed. If there is a new registration, the new template is added to the database confirming the new registration.

Thus, DRIVERAUTH minimizes the threats posed by dishonest drivers by preventing multiple or forged account creation.

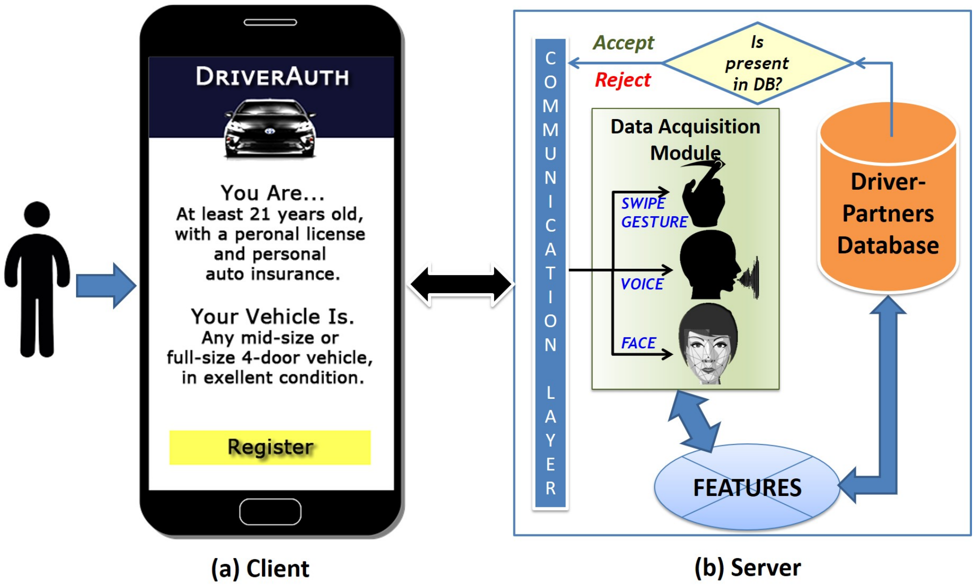


Figure 6.4: Overview of driver-partners registration process.

6.4.3 Verification during New Ride Assignment

Drivers verification process during new ride booking is illustrated in Figure 6.5.

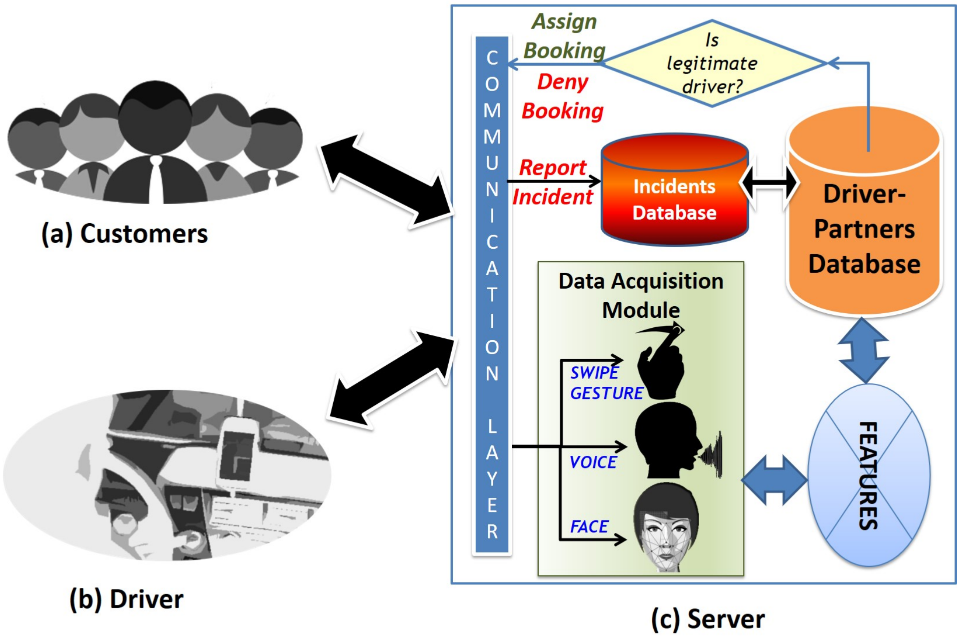


Figure 6.5: Overview of new ride assignment process.

1. The customers can book the ride by setting up their location using the dedicated on-demand ride and ride-sharing application on their smartphones. Subsequently, they can locate the available cabs (along with the driver's picture and vehicle details) near to their location to reserve the ride by selecting one of the cab [259].

2. On receiving a booking request from a customer, the system provider forwards the request to the respective driver.

3. The driver upon receiving the alert can continue to accept the new ride-assignment by swiping on the touchscreen.

4. After the swipe input is detected, the application requires a short voice-print ($2 - seconds$ of a voice recording) from the driver. This voice-print can be *text-independent* that provides flexibility to the drivers to use any language of their choice.

5. After the successful voice detection, the application turns on the camera and prompts for the driver's selfie to conclude the ride-assignment acceptance process.

6. Subsequently, DRIVERAUTH client application transfers the encrypted driver's biometric modalities, i.e., swipe gesture, voice, and face, to the server. In the meantime, the driver verification is performed on the server.

7. Based on the driver verification results, the system provider can approve the ride-assignment to the respective driver and simultaneously, intimate the customer.

8. In any case if the driver abuses or assaults the rider, then the rider can report the incident, immediately. The reported incident can be

tagged with the driver's identity which will automatically be added to the incidents database.

DRIVERAUTH minimizes the potential risks towards the safety and security of riders by verifying the drivers' identity pro-actively, at the time of every new ride assignment.

6.4.4 Liveness Detection and Spoofing Attacks Prevention

Liveness detection helps to distinguish between living and non-living, during the authentication process and, thus, prevents spoofing attacks at the data acquisition module [213]. DRIVERAUTH data acquisition module acquires data from three modalities, i.e., voice, swipe, and face, as described in Section 6.4.3. For voice liveness detection, the data acquisition module incorporates phoneme sound localization mechanism taking advantage of the user's unique vocal system and high-quality stereo recording of smartphones [285]. Studies have shown that swipe gesture is inherently difficult to spoof [61], however in the future, we will incorporate technique for swipe liveness detection too. Similarly, face modality liveliness indicators like eye blinking, mouth movements, face posture, and motion analysis, etc., are exploited for multi-spectral and reflectance analysis [167].
Thus, DRIVERAUTH prevents the spoofing or presentation attacks at the sensor level by utilizing available mechanisms to detect liveness for each modality.

6.5 Methodology

DRIVERAUTH exploits three biometric modalities, i.e., swipe gestures, voice, and face, and collects their corresponding data, while the users interact with a driver-application on their smartphones. Both physical and behavioral biometric modalities can be easily collected using smartphone's built-in hardware sensors, such as a camera, microphone, and touchscreen. We modeled this remote-user-verification as a *multi-class classification problem* because the scenario demands simultaneous classifier training and testing for multiple drivers, however, each query input needs to be assigned only to one class.

6.5.1 Datasets

We evaluated DRIVERAUTH on a dataset of 86 persons. We prototyped an Android application to collect swipe and voice data. And, for face data, we utilized the MoBio database [171].

We outsourced swipe and voice data collection activity to Ubertesters[1] - a crowd-sourcing platform to collect data in the wild (*unsupervised environment*). We paid to Ubertesters on an hourly basis per tester to carry out our experiments. All the information regarding App setup and data collection provided by us is duly informed to each tester by Ubertesters, and we ensured not to record or collect any information that can link the collected data to the testers. During the experiment, the data generated on each tester's smartphone were securely transferred to our servers in an automated manner. Interested readers can refer to the "Ubertesters License and Terms of Service" available online[2].

For our experiment, Ubertesters recruited more than 150 vetted testers worldwide having diversified background and experience. However, some testers' data were rejected for reasons, such as 1) tester's smartphones were not found compatible with our experiment because it did not have the required sensors, 2) testers could not complete the experiment as instructed, or 3) testers' data was noisy.

[1] https://ubertesters.com

[2] https://ubertesters.com/license-page/

Finally, we created a chimerical dataset by merging these three modalities, i.e., swipe gesture, voice, and face, for each label. As all the three modalities are mutually independent of each other, they can be augmented randomly to form a single dataset [214]. Another benefit of the chimerical dataset is that biometric traits for each label are disjoint, which restricts the multi-modal classification model to establish any strong linkage to the testers, thus, ensuring testers' privacy during the experiment.

6.5.1.1 Swipe & Voice Data Collection

The prototype application was developed for Android OS (OS version `4.4.x` and above). It uses built-in hardware, i.e., touchscreen and microphone, to acquire touchpoints data during swipe action and recording of the user's voice. Overall, we collected $10,320$ samples. The experiment was conducted in 4 sessions for 3 days. Each user trained the application for 90 times in 3 sessions (30 times per session) within 15 minutes each. In the fourth session, each user tested the application for 30 times. A total 120 observations were collected per user with $7,740$ (86×90) training samples and $2,580$ (86×30) testing samples.

As our developed application uses a client-server architecture, the data generated as a result of the user's actions, i.e., swipe and voice command, is encrypted and zipped on the client device, i.e., smartphone, and is automatically transferred to the server, for further processing. On-demand ride and ride-sharing companies are operating worldwide.

Our prototype collects $2 - seconds$ *text-independent* voice-print (e.g., "I accept the ride to Y"), allowing drivers to interact in the language depending on the country where they operate or the company for which they work. Therefore, we do not limit voice modality to any specific language or the particular word-sets.

Table 6.2 presents the demographics data of users participated in this experiment. Among 86 participants, 56 were males, 29 were females with 77 right-handed and 9 left-handed. Majority of participants were in Asia (28) and Europe (52) while performing the experiment, with 60 were between 20 to 30, 17 were between 30 to 40, and 3 were above 40.

Table 6.2: User demographics.

#	Parameter	Description
1	No. of Users	86
2	Gender	56 males, 29 females, 1 undisclosed
3	Handedness	77 Right, 09 Left
4	Age Groups	[20 to 30] - 60, [30 to 40] - 17, 40 plus - 3
5	Participants Location	Asia - 28, Europe - 52, North America - 5, South America - 1

6.5.1.2 MOBIO Dataset

This public dataset consists of face samples collected from 152 subjects in 2 phases using a NOKIA N93i mobile phone under a realistic and uncontrolled environment over a period of 18 months from six sites across Europe [171]. In the first phase, 21 videos per participant were collected, whereas 11 videos per participant were acquired in the second phase. The data acquisition was spread over 6 different sessions per phase for each participant. The database has 1 : 2 female to male ratio, approximately. However, we picked only 86 subjects out of 150 to match the same number of users as to our dataset.

6.5.2 Feature Extraction

In this section, we explain the extraction of features for all the three selected modalities using statistical methods. Univariate statistical properties, i.e., mean, standard deviation, kurtosis or skewness has several benefits, they reduce the dimensionality of raw data, improve the signal-to-noise ratio, and they can be processed efficiently [163].

- **Swipe Modality:**

  A sequence of touch-events is generated every time users swipe on smartphone touchscreen using their finger. These touch-events are collected and encoded as an input sequence of finite length (n). Where, each sequence contains several attributes like time-stamp of the touch event (t_n), x-and y-coordinate of the touch point (x_n, y_n), pressure calculating how hard the finger was pressed on the screen (p_n), and size of touch area (s_n). We processed the collected sequences and extracted 33 features as listed in Table 6.3. The final feature vector is the concatenation of all the 33 features.

Table 6.3: List of swipe features.

No.	Swipe Features			
1-4	Duration 1	Average event size 2	Event size down 3	Pressure down 4
5-8	Start X 5	Start Y 6	End X 7	End Y 8
9-12	Velocity X Min 9	Velocity X Max 10	Velocity X Average 11	Velocity X STD 12
13-16	Velocity X VAR 13	Velocity Y Min 14	Velocity Y Max 15	Velocity Y Average 16
17-20	Velocity Y STD 17	Velocity Y VAR 18	Acceleration X MIN 19	Acceleration X Max 20
21-24	Acceleration X AVG 21	Acceleration X STD 22	Acceleration X VAR 23	Acceleration Y MIN 24
25-28	Acceleration Y Max 25	Acceleration Y AVG 26	Acceleration Y STD 27	Acceleration Y VAR 28
29-32	Pressure Min 29	Pressure Max 30	Pressure AVG 31	Pressure STD 32
33	Pressure VAR 33	-	-	-

- **Voice Modality:**

  The voice signal contains 2 channels sampled at 44100 Hz with 16 bits per sample. The signal is first filtered using a bandpass filter. It can be observed in Figure 6.6 that by applying a bandpass filter there is a significant improvement in signal-to-noise ratio.

  Then, we computed MFCC [68] from these filtered voice signals. MFCCs are analogous to filters (vocal tract) in the source-filter model

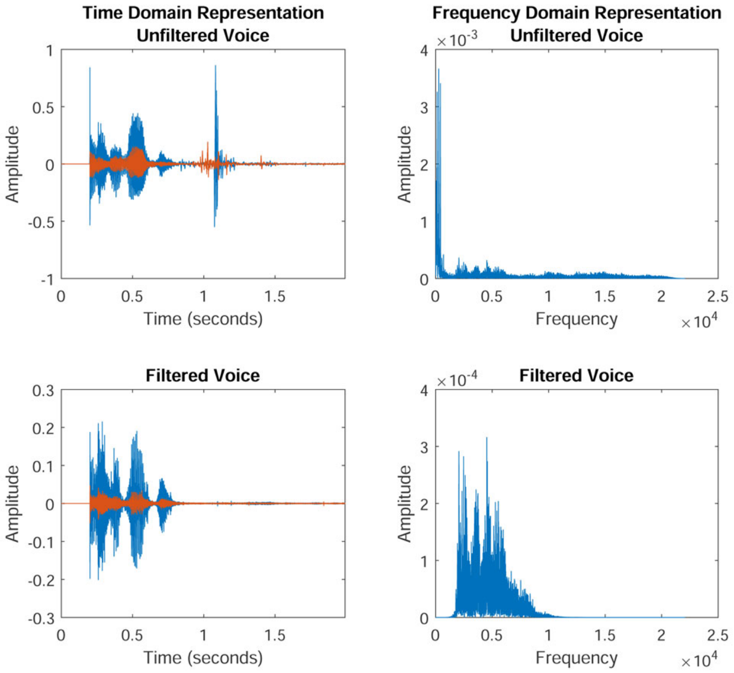


Figure 6.6: Voice signal filtering result.

of speech. Relatively, the frequency response of the vocal tract is smoother than the source of voiced speech. Thus, the vocal tract can be estimated by the spectral envelope of a speech segment. This technique is often used in voice recognition because it tracks the invariant feature of human speech among different persons.

Figure 6.7 illustrates the MFCCs computation process. After improving the signal-to-noise ratio, the Fourier transform of a window of the voice signal is performed, then scaling of frequency axis to the non-linear Mel scale (using triangular overlapping windows) is done. In the next step, a Discrete Cosine Transform (DCT) is performed on the log of the power spectrum of each Mel band. The MFCCs are the amplitudes of the resulting spectrum, which is a $2-D$ vector of size $13 \times variable\ length$ (the length of vector depends on the voice signal duration).

We computed 4 statistical features, namely mean, standard deviation, kurtosis, and skewness, from a 2-D MFCC vector. Thus, the total 8 statistical features each of size 1×13 are generated from each left and the right voice channel. Finally, these 8 vectors of size 1×13 are concatenated to form a single $1 - D$ feature vector of dimension 1×104.

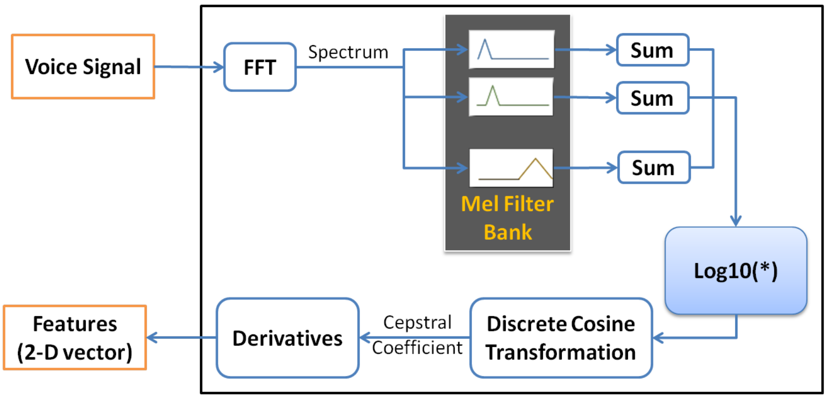


Figure 6.7: Voice features: MFCC computation process.

- **Face Modality:**

  On the server, the region of interest (ROI) is extracted automatically, by cropping the original images, as illustrated in Figure 6.8. Then, each image is converted into an 8-bit grayscale format. We used the *Binarized Statistical Image Features* (BSIF) filter to obtain statistical features [139].

  Given an image patch X of size $l \times l$ pixels and a filter W of size $n \times n$ pixels, where n is less than l. The filter response s_i can be obtained as shown in Equation 6.1.

$$s_i = X[l, l] * W[n, n] \tag{6.1}$$

  We extracted 256 features per image using a filter of size 3×3 with 8 bits word-length. BSIF filter applies learning, instead of manual tuning, to compute statistically meaningful representation of an image.

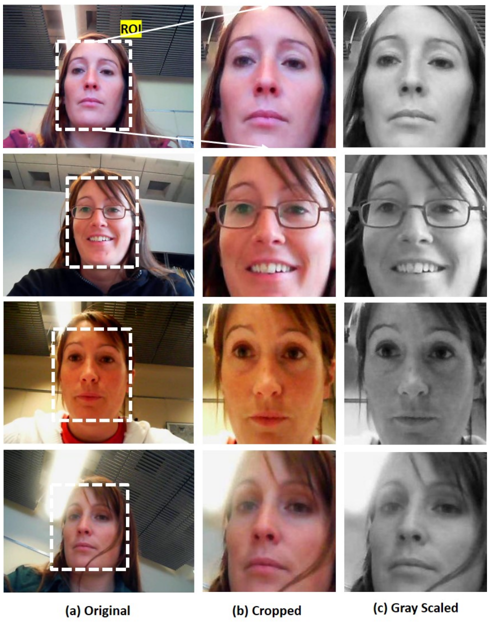


Figure 6.8: Face features: BSIF computation process

6.5.3 Features Concatenation

Data fusion in a biometric system is a process of integrating multiple modalities to produce more accurate, consistent, and comprehensive information of users. Biometric researchers often consider that early data fusion increases the accuracy of the system [135, 88]. However, sensor-level fusion does not yield the best results owing to the presence of noise during data acquisition. Thus, feature-level fusion is a better choice to improve the accuracy of the system, because feature representation reflects more relevant information on users. Lastly, this setting is preferred as it combines independent modalities [165]. Therefore, we applied feature level concatenation to generate the final features vector.

6.5.4 Feature Subset Selection

Feature selection plays an important role in the fine-tuning of the chosen classifiers. It helps in reducing the dimension of data as well as prevent the over-fitting by identifying productive features out of the full feature-set. This process not only maximizes the accuracy of a classifier but also contributes to improving the classifier's decision-making time. Feature selection methods can be categorized as *Filter*, *Wrapper*, *Embedded*, and *hybrid* methods, based on their relationship with the construction of a model [263]. We considered Information Gain Ranking Filter[276], Simple Correlation Ranking Filter [276], CFS Subset Evaluator with greedy forward search [276], and ReliefF [263] to obtain most productive feature subset, for our analysis. However, relief-based algorithms (RBAs) provided the best accuracy result.

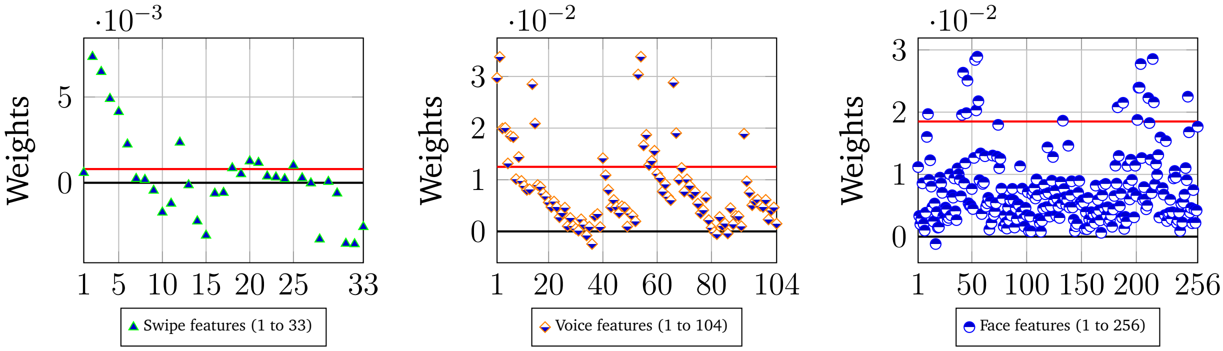
RBAs belong to the individual evaluation $filter$ method. The advantages of RBAs are: 1) they can detect conditional dependencies between features, 2) they provide a unified view on the estimation of the features in classification, and 3) they are relatively faster (with asymptotic time complexity of order $\mathcal{O}\ (instances^2 \times features)$) to other feature selection methods [263, 181].

RBAs compute ranks and weights of features to derive feature statistics using the concept of nearest neighbors as shown in Equation 6.2.

$$[RANKED, WEIGHT] = relief(X, Y, K) \tag{6.2}$$

Where, $X\ (m \times n)$ is a given 2-d dataset, $Y\ (m \times 1)$ is the response vector, and K is a number of nearest neighbors. $RANKED$ are indices of columns in X ordered by attribute importance, meaning $RANKED[1]$ is the index of the most important feature. $WEIGHT$ are features weights ranging from $-1\ \mathit{to}\ +1$ with large positive weights assigned to most important attributes.

We performed feature selection in three settings and evaluated DRIVERAUTH in unimodal, bimodal, and trimodal settings. Then, we tested and validated our system on both the full feature set and selected feature set to achieve an optimal design. In the following sections, we explain our feature selection strategy for our experiments.



(a) Swipe features (11)

(b) Voice features (20)

(c) Face features (20)

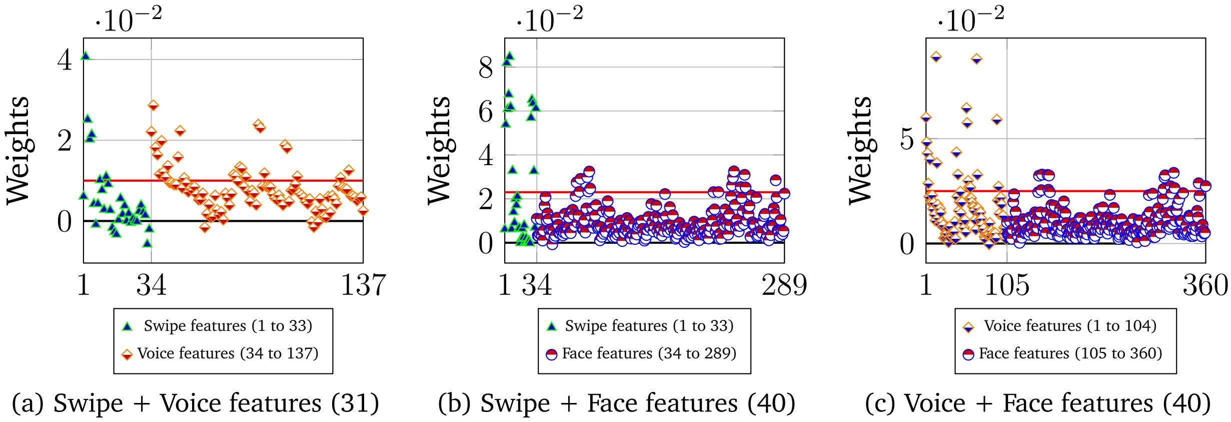
Figure 6.9: Unimodal system: plot between features vs. weights.

- **Unimodal:** We obtained in total 33, 104, and 256 features from processed swipe, voice, and face modalities, respectively, to design the unimodal systems. We evaluated the system firstly on the full feature set. To evaluate the system on the selected feature set, we estimated the importance of features of each modalities using ReliefF algorithm[3]. Then, we picked top 30% or 20 features of the total (whichever is less) as per their weights. The features vs. weight for the three modalities are shown in Figure 6.9.

  The number of features required for the best classification model creation was computed, empirically. In case of a swipe, the total number of features available are 33, we, firstly, trained our classification model by picking all the features with positive rank, i.e., above zero as shown in Figure 6.9a and observed that the same TAR is achieved with top 11 features, i.e. 33% of total available features as demarcated by a red line in Figure 6.9a. Whereas, in case of voice and face, the classification model is trained by picking top 33% of to-

[3] https://in.mathworks.com/help/stats/relieff.html

tal available features, i.e., 34 and 85 features, respectively. But, we observed that with only the top 20 features the same TAR is achieved as demarcated by a red line in Figure 6.9b and Figure 6.9c.



(a) Swipe + Voice features (31) (b) Swipe + Face features (40) (c) Voice + Face features (40)

Figure 6.10: Bimodal system: plot between features vs. weights.

- **Bimodal:** We concatenated swipe and voice, swipe and face, and voice and face creating feature set of dimension 137, 289, and 360, respectively, to design a bimodal system. In this case, for each combination, the two feature sets are firstly fused and then ranked using the ReliefF algorithm. Finally, the system is evaluated on a full and selected feature set. The dimension of selected features for swipe + voice, swipe + face, and voice + face are 31, 40, and 51, as demarcated by a red line in Figure 6.10a, Figure 6.10b and Figure 6.10c, respectively.

- **Trimodal:** We concatenated the feature sets of each modality together to create a single feature set of dimensions 393 for evaluation of DRIVERAUTH in trimodal settings. Figure 6.11 represents features ranking obtained by applying the ReliefF algorithm on the fused feature set. Finally, the system is evaluated on both full and selected feature-set of dimension 51.

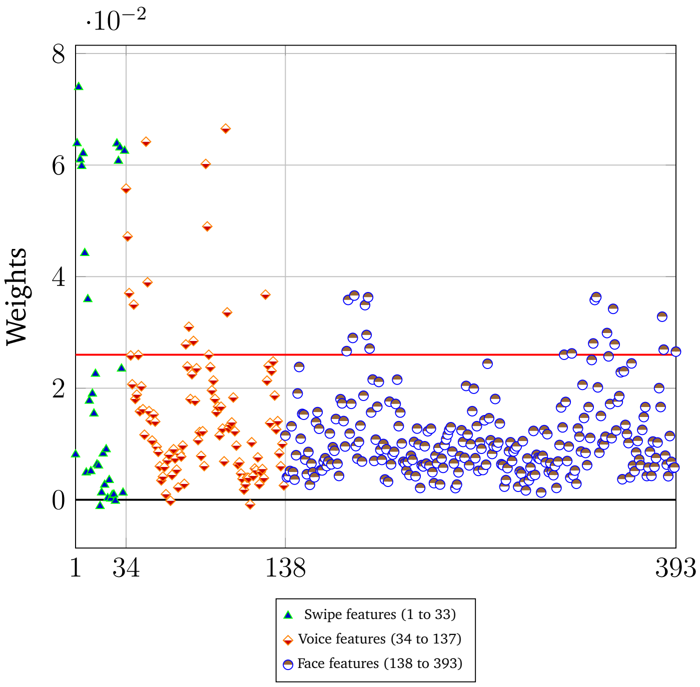


Figure 6.11: Trimodal system: plot between features vs. weights (51).

6.6 Validation

We utilized Classification Learner [168] to generate a classification model. Classification Learner can perform automated training to search for the best classification model type, e.g., support vector machines, nearest neighbors, ensemble classification, etc. We used 5-fold cross-validation to assess the classifiers' prediction performance. Cross-validation protects against over-fitting by partitioning the data set into folds and estimate accuracy on each fold. Thus, this method gives a good estimation of the predictive accuracy of the final model trained with full data.

However, security-sensitive infrastructures, e.g., banks, prefer to design classification models with a fewer number of training samples (typically up to 10). Thus, we evaluated our trimodal system with the most productive feature-set achieved by applying the ReliefF algorithm for a different number of training samples, i.e., 10, 20, 30, and 40, to determine its effectiveness. To achieve it, we split the dataset into two parts, i.e., training- and testing- datasets and evaluated the model in two different scenarios. In the first scenario, we utilized a designated number of training samples (n) to train the classifier and used $120 - n$ samples to test the model. Here, we presented the result in terms of TAR, which can be further studied in Figure 6.12. In the second scenario, i.e., the zero-effort attack scenario (where an impostor could only make random tries to access the system without knowing the actual user), we excluded legitimate samples, i.e., 120 samples, of each user and used the remaining samples, i.e., 10200 (85×120) to attack the model, for all the remaining 85 users. Here, we presented the results in terms of FAR, which can be further studied in Figure 6.13.

6.6.1 Classification Methods

In a biometric system, the role of a classifier is to recognize the similarities or detect the anomalies between the query input and stored templates to authenticate a user. We selected Support Vector Machines, Nearest Neighbor, and Ensemble classifiers to evaluate DRIVERAUTH, using a multi-class classification model. These classifiers are well suited for the multi-class environment and have shown to be very effective for similar biometric modalities, i.e., swipe, voice, and face, in recent studies [72, 139, 165].

6.6.2 Results

Table 6.4 and 6.5 show the performance of classifiers with full and selected features, respectively.

The results are presented for each modality, independently, as well as for binary and ternary feature-level fusion. The performance is measured in terms of TAR averaged for all the 86 users with 120 observations per user

Table 6.4: Performance of classifiers with full features for unimodal, bimodal and trimodal configuration based on 5-fold cross-validation.

	Unimodal			Bimodal			Trimodal
Modalities	Swipe	Voice	Face	Voice + Face	Swipe + Voice	Swipe + Face	Swipe + Voice + Face
Total number of features	*33*	*104*	*256*	*380*	*137*	*289*	*393*
Classifier	TAR(%)						
Quadratic SVM	**87.0**	**90.9**	**91.2**	**98.2**	**95.1**	**97.5**	**99.0**
Ensemble Bagged Tree	84.7	88.2	85.0	95.2	94.3	96.6	98.2
Weighted KNN	70.2	85.4	88.7	94.7	90.4	94.1	96.7

Table 6.5: Performance of classifiers with selected features for unimodal, bimodal and trimodal configuration based on 5-fold cross-validation.

	Unimodal			Bimodal			Trimodal
Modalities	Swipe	Voice	Face	Voice + Face	Swipe + Voice	Swipe + Face	Swipe + Voice + Face
Number of selected features	*11*	*20*	*20*	*40*	*31*	*31*	*51*
Classifier	TAR(%)						
Quadratic SVM	**79.99**	**89.60**	**90.61**	**97.63**	**93.53**	**98.04**	**99.04**
Ensemble Bagged Tree	77.66	86.00	86.72	95.04	91.89	97.08	98.02
Weighted KNN	68.83	86.51	90.71	96.36	90.68	96.93	98.26

using a 5-fold cross-validation method.

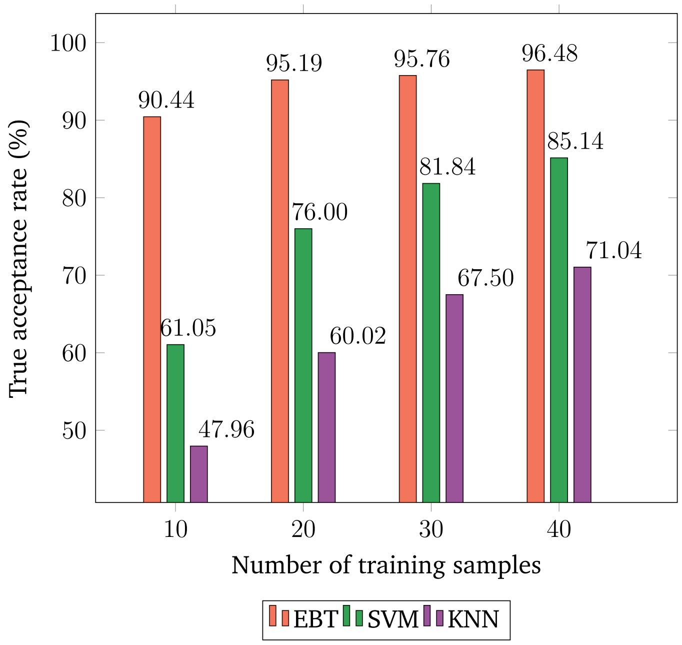


Figure 6.12: True acceptance rate (TAR) with selected features for trimodal configuration with 10, 20, 30, and 40 training samples.

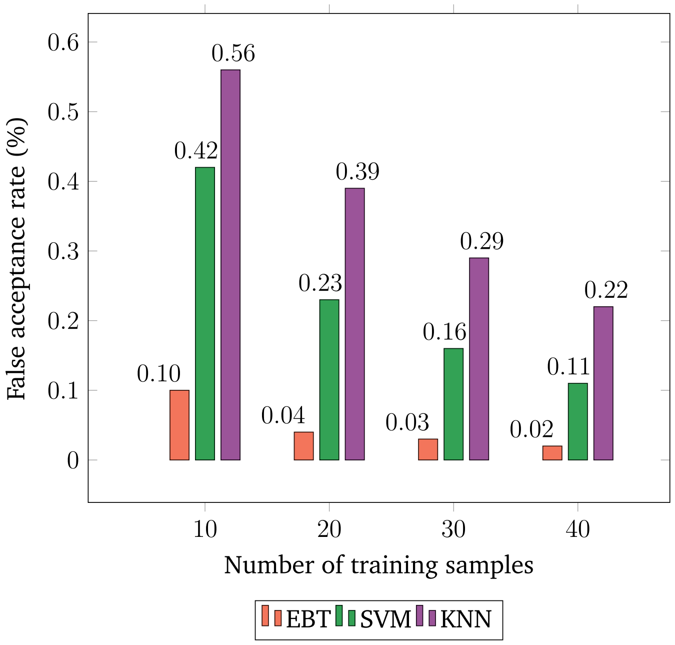
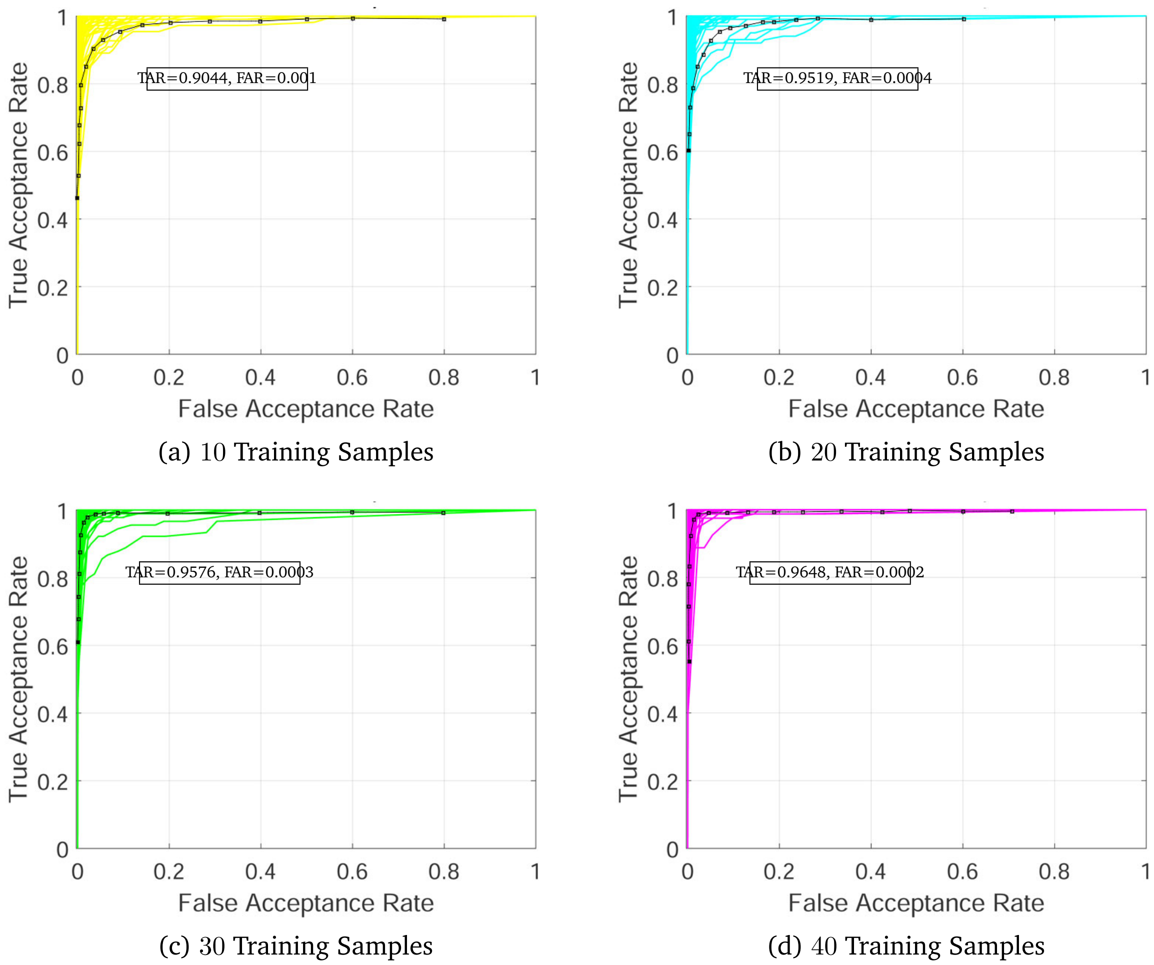


Figure 6.13: False acceptance rate (FAR) with selected features for trimodal configuration with 10, 20, 30, and 40 training samples.

Figure 6.12 and 6.13 show the results of the trimodal system for 10, 20, 30, and 40 training samples with selected feature-set, in term of TAR and FAR, respectively.



(a) 10 Training Samples

(b) 20 Training Samples

(c) 30 Training Samples

(d) 40 Training Samples

Figure 6.14: Average ROC curves of EBT classifier for different training samples.

Managing ROC curves for a multi-class classification problem is much more complex in comparison to 2-class classification [70]. Typically, in a multi-class classification model with n-*classes*, the resultant confusion matrix having dimension n *by* n possesses n correct classifications (the major diagonal entries) and n^2 =-n possible errors (the off-diagonal entries). According to Fawcett [70], a *class reference formulation* is an efficient method to handle n-*classes* by producing n-different ROC graphs.

Specifically, if C is the set of all classes, ROC graph i reports the classifier performance per class c_i by plotting positive results (P_i), i.e., TAR, as shown in Equation 6.3 and negative results (N_i), i.e., FAR, as shown in Equation 6.4.

$$P_i = c_i \tag{6.3}$$

$$N_i = \bigcup_{j \neq i} c_j \in C \tag{6.4}$$

This method is reasonably flexible as an optimal threshold t_i can be set, at which TAR is maximum and FAR is minimum. Thus, improving the overall performance of the classification model.

Figure 6.14 illustrates average ROC curves of EBT classifier for (a) 10, (b) 20, (c) 30, and (d) 40 training samples. In the two-dimensional graphs as shown in Figure 6.14, TAR is plotted on the Y-axis, and FAR is plotted on the X-axis, depicting relative trade-offs between the true positives and false positives. Coordinate $(0, 0)$ represents the strategy of never issuing a positive classification; such a classifier commits no false-positive errors but also determines no true positives. However, the opposite strategy, of unconditionally issuing positive classifications, is represented by coordinate $(1, 1)$. Whereas, coordinate $(0, 1)$ represent the perfect classification strategy of maximizing TAR and minimizing FAR. Readers can observe in Figure 6.14 with the increase in the number of training samples classifier performance also tends to improve, accordingly.

6.6.3 Discussion on Results

The cross-validation method is used to evaluate how well the model is trained and how it performs when it is tested on the test dataset. K-fold cross-validation is popular because it is computationally cheap as compared to other cross-validation variants. In K-fold cross-validation, the dataset is divided into K equal folds and the model is trained on the dataset of $K-1$ folds, and the remaining fold is used to test the system. The process is repeated K times. Cross-validation is preferred when the dataset size is small and it ensures the testing of all the samples. As we had 120 samples for each user, we started the evaluation with 5-fold cross-validation. SVM performed well in this scenario resulting in 99.04% TAR.

Training/Testing split is another method to evaluate the performance of the classifier. The dataset is generally split into two parts, i.e., training and testing sets. The model is trained on the training set (generally, 66% of the whole data) and the remaining test dataset is used to test the model.

In real-world scenarios, e.g., banking applications, generally, the systems require a few attempts to train the classifier and is evaluated every time the user wants to access their services. Thus, it is worthy to test the classifier with a few numbers of training samples and check for the performance. We tested the pre-trained classifier (trained on 10, 20, 30, and 40 training samples each) and report our obtained results.

In the case train/test split scenario, the EBT classifier performed better than the SVM and KNN classifiers owing to its ability to reduce the variances and affinity against over-fitting with fewer training samples. It can be noticed that with an increase in the number of training samples, the performance (TAR and FAR) of each classifier improves. For instance, the TAR of EBT classifier improved by $+4.75\%$, $+0.57\%$ and $+1.29\%$, whereas FAR became better by -0.06%, -0.01% and -0.01%, with 20, 30 and 40 training samples in comparison to performance with 10 training samples. The same trend can be observed for the other 2 classifiers, i.e., SVM and KNN, in Figure 6.12 and 6.13.

6.7 Summary

DRIVERAUTH is a highly accurate drivers' verification system designed for the on-demand ride and ride-sharing services in which customers and the driver-partners are connected to the service provider (server) by the dedicated smartphone applications (clients). Based on the news related to violent altercations, or assaults by malicious drivers and fake drivers offering rides [116, 266, 273, 43]. It is evident that the safety and security of customers are obviously at risk. Therefore, the risk-based verification mechanism can equip service providers to verify the subject at the time of critical decisions (e.g., accepting new registration from a person to join as a driver or assigning new ride assignments to the driver-partners) and trusting the subject with the lives of customers.

We presented a risk-based multi-modal biometric-based driver authentication scheme that uses swipe gesture, voice, and face modalities to profile the driver's identity. We evaluated, DRIVERAUTH, on a dataset of 86 users with 120 observations per user and achieved a TAR of 99.0%, 98.2%, and 96.7% for a trimodal system using SVM, EBT, and KNN classifiers, respectively, on the full feature set.

Feature selection plays a critical role in optimizing the classification model in terms of reduction of feature set dimension and improvement in the decision-making time of computationally exhaustive classifiers. We achieved a TAR of 99.04%, 98.02%, and 98.26% using SVM, EBT, and KNN classifiers, respectively, on a selected feature set of dimension 51, which is one-fourth of full feature set, approximately.

Chapter 7

RIDERAUTH: A perspective study towards biometric-based rider authentication schemes for driverless taxis

RIDERAUTH is a proposal for biometric-based secure and usable riders authentication schemes for driverless taxis. Our study is complemented by an online survey that comprises 75 responses from participants, worldwide. We published the survey on social media platforms like Linkedin, Facebook, Twitter, and various public transport users groups to collect public poll for rider authentication for driverless taxis. Approximately, 90% of the overall participants in our survey either strongly agreed or agreed with the necessity to deploy biometric-based rider authentication for driverless taxis.

Some sections of this chapter are published in [97]: *Sandeep Gupta, and Bruno Crispo. "A Perspective Study Towards Biometric-based Rider Authentication Schemes For Driverless Taxis." In proceedings of the 3*rd *International Conference On Innovation And Intelligence For Informatics (3ICT), Bahrain, 2019.*

7.1 Introduction

Driverless vehicles are no more science fiction. Driverless vehicles exploit Artificial Intelligence (AI) to offer rides to their users with minimal or no human input. In 2019, Waymo[1] unveiled driverless taxi services in the United States dubbed as Waymo One (refer Figure 7.1). Customers can book Waymo's service by using a smartphone application, similar to the on-demand ride-booking applications provided by companies, such as Uber, Lyft, etc. Typically, driverless taxis use Artificial Intelligence (AI) by exploiting sensors and digital systems to control, navigate, and drive the vehicle. However, riders authentication, i.e., verifying the riders identity, is an important requirement among the many other overarching challenges in driverless taxis.

Figure 7.1: Driverless taxis by © Waymo One[1].

Driverless vehicles as taxis are indeed evolving an entirely new transportation concept. They have reached a point where they can be used to provide Transportation-As-A-Service[2] (TAAS) to facilitate rides to their customers with high efficiency and safety on the road, steered by efficient IoT architectures [210]. Typically, the servers, managed by multinational

[1] https://waymo.com
[2] https://taas.technology

companies (e.g., Waymo), operate driverless taxis for public transportation, whereas the clients are simply the smartphone-based applications that can be used by customers for one-time registration and booking rides with driverless taxis anytime anywhere.

Several studies have been performed to assess crucial security mechanisms deployed in driverless vehicles to ensure secure sensing, positioning, vision, and networking [50, 103, 148]. However, unsupervised physical access to riders in the driverless taxis may lead to unexpected safety and security risks. Section 7.3.1 outlines the potential risks that may materialize as a consequence of customers' diversified motivations like curiosity, monetary benefits, malicious intentions, or terrorism [50]. Thus, research on rider authentication schemes for driverless taxis is essential for the security and safety of their customers and the general public.

We perform a perspective study to design biometric-based rider authentication schemes for driverless taxis. For this study, we conducted an online survey to gather public opinion on different biometric traits for rider identification. In the survey, we also collect information to understand the security and usability criteria to design a secure and usable rider authentication schemes. Then, we propose a rider authentication framework for driverless taxis to verify customers in real-time before allowing the rides, by using a client-server architecture.

7.1.1 Contributions

The main contributions are presented below:

- Online survey to study public opinion about rider authentication for driverless taxis by publishing the survey on social media platforms like Linkedin, Facebook, Twitter, and various public transport users groups.

- Proposal for a real-time rider authentication system to verify the customers before allowing them the rides to foster safety and security to their customers and the general public. The rider authentication system for driverless taxis is designed taking into consideration the results of the survey.

7.1.2 Chapter Organization

The rest of the chapter is organized as follows: Section 7.2 presents a study of user authentication schemes that use physiological and behavioral biometric traits that can be deployed for rider authentication. Section 7.3 discusses the motivation for rider authentication for driverless taxis. Section 7.4 presents the survey results with the analysis of the rider authentication requirements. Section 7.5 presents the proposal for the rider authentication framework by considering survey results.

7.2 Related Work

This section surveys different physiological and behavioral biometric-based user authentication schemes that can be deployed for rider authentication in driverless taxis. In autonomous vehicles to improve the human-vehicle relationship biometric devices can be either embedded inside the vehicle or can be included as the accessories and wearables, externally [161]. These biometric devices can enhance the security, efficiency, and reliability of autonomous vehicles by authenticating genuine riders.

Face, fingerprint, and iris are among the most popular physiological biometric traits in deployed systems owing to their high recognition rates and simplicity to acquire them [132]. Driverless taxis are already fitted with the high-resolution digital camera that can be used to acquire face images of customers for their authentication. DRIVERAUTH 6, a multimodal biometric-based authentication scheme, exploits face, text-independent voice, and swipe. They achieved a True Acceptance Rate (TAR) of 96.48% at False Acceptance Rate (FAR) of 0.02% using Ensemble Bagged Tree (EBT) classifier on a dataset of 86 users for the on-demand ride and ride-sharing services. A face and appearance-based real-time driver authentication framework proposed by Derman et al. [54] combine a CNN-based face classifier with a GMM-based appearance verifier to authenticate legitimate vehicle owner among 52 different subjects. They achieved an average True Positive Rate (TPR) of 92.46% and 87.13% corresponds to 1% and 0.1% False Positive Rate (FPR), respectively for multiple drivers test scenarios.

Fingerprint and grip patterns based authentication scheme for door access proposed by Jang et al. [136], can be used in driverless taxis doors handle for riders authentication. However, the authors did not publish any experimental results for the validation of their proposed scheme. There are several fingerprint-based authentication schemes are proposed for the vehicle owner identification [76, 290]. These fingerprint-based authentication schemes can be deployed for rider authentication in driverless taxis by modifying the design, accordingly.

Iris recognition based scheme proposed by Raiyn [208] to authenticate vehicle to vehicle communication in autonomous vehicles (AVs) can be applied for rider authentication. Biometric identification based on inner eye organs, i.e., iris and retina, are very precise and can be used in areas with high-security requirements [100].

A multimodal authentication scheme based on fingerprint, iris, and voiceprints proposed for identifying drivers by installing sensors on the doors, steering wheel, and camera mounted on the front mirror of vehicles [162]. This scheme can also be utilized for riders' authentication by modifying the sensors' installations as per the requirements. Similarly, another user authentication scheme on the Java platform combines face, fingerprint, and speech for automobile locking purpose [186]. A human vehicle interaction system, VoGe, based on voice and gestures can be used for rider authentication [224]. The authors presented the proof of concept in a driving simulator that enables users to communicate with the vehicle and make spontaneous decisions over the route.

The user-identification-signatures can be generated for various gestures, such as swiping, holding or typing, by extracting statistical features from X, Y, and Z coordinates fetched by sensors, i.e., accelerometer, magnetometer, and gyroscope, while the users do that action on their smart devices 4. Interested readers can refer to the driver authentication framework designed for the on-demand ride and ride-sharing services based on the aforementioned behavioral biometric traits while the drivers interact with their dedicated smartphone-based application [94].

Tolosana et al. [254] proposed a signature verification architecture based on the number of lognormal from the Sigma LogNormal writing generation model that is adapted to the signature complexity. Additionally, they performed an exhaustive comparative analysis of both pen- and touch-based scenarios for smartphones and tablets. Another bimodal authentication scheme for financial applications exploits users' touch-typing and hand-movements transparently, while the users access their banking apps by inserting 8-digit PIN/password [33]. This client-server based multiclass authentication scheme achieved 96% TAR with 0.01% FAR by using 15 training samples on a dataset of 95 users. Similarly, DIALERAUTH authenticated users based on touch-stroke timing-differences and hand micro-movements for 10-digit PIN/password [33]. And, they achieved the TAR of 85.77% by using one-class Multilayer Perceptron (MLP). Smartphone-based authentication scheme, SNAPAUTH, exploited users' hand-movement while the users perform finger-snapping action [32].

This authentication scheme achieved the TAR of 82.34% by using MLP classifier with 15 training samples on a dataset of 11 users.

Human gait can be collected unobtrusively, as users do not require to perform any explicit interaction with their smart devices. Biometric gait recognition based on vision, underfoot pressure, accelerometry, and audio sensory features can be explored for rider authentication [44]. A smartphone-based gait recognition system against zero-effort- and live-minimal-effort- impersonation attacks under realistic scenarios and it achieved an Equal Error Rate (EER) of 13% on a dataset of 35 participants [183]. Similarly, smartwatch-based gait biometrics can be deployed for rider authentication for driverless taxis [138]. However, to deploy gait-based recognition schemes, a vehicle trusting biometric measurements from external devices (e.g. a smartwatch) may have some security implications that need careful evaluation.

Biometrics, such as the face, fingerprint, iris, retina, voice, touch signature, keystroke/touch dynamics, gait, and hand-movements to hold or wear smart devices, can be easily employed for riders' authentication. To acquire these traits, requisite sensors or devices can be either installed in the driverless taxis; or can be fetched from the smart devices paired by the customers, at the time, they board the driverless taxi that they have booked online. In the realtime, the acquired customers' biometric data can be used for their authentication before the driverless taxis commence their ride.

Our survey for rider authentication will provide some insights for technology providers to implement rider authentication schemes that can be acceptable by the customers.

7.3 Motivation

In January 2019, Waymo[1] has launched the driverless taxi services throughout Phoenix, Arizona. Similarly, other companies involved in driverless technologies are planning to launch their driverless taxi services soon. However, there has been minimal research for rider authentication schemes requirements for driverless taxis. We conducted an online survey to collect public opinion to study the requirements for the rider's authentication as these taxis can be used individually or shared with other riders.

7.3.1 Threat Model

[50] and [93] analyze what are the security threats associated with the possible human intervention in driverless taxis.

- How to identify a person who hires the driverless taxi, and then causes some damages to the taxi, which could be hazardous for following customers of that taxi?
- How to deny rides to the persons who were indulged in activities, intentionally or unintentionally, that resulted in the malfunctioning of crucial safety systems of driverless taxis?
- How to catch persons having malicious intentions, e.g., someone who planted some illicit object like explosives in a taxi that resulted in mass casualties or caused serious damage to the subsequent customers?
- Do the customers prefer to share a ride with strangers in a driverless taxi without their verification done by the service providers?

- How to identify a rider who robs or abuses the fellow passengers in the shared driverless taxis?
- Lastly, how to avoid unforeseen incidents as the consequences of unsupervised access to riders with diversified motivations, such as curiosity, monetary benefits, malicious intentions, or terrorism?

Thus, reliable riders' authentication schemes for driverless taxis become imperative to mitigate the possible threats that we just discussed. Conventional authentication techniques, i.e., knowledge-based and token-based mechanism, are reported to be less reliable due to their inherent drawbacks [92, 132]. Moreover, it is evident that biometric-based authentication schemes are more efficient to counter attacks when employed in security-critical systems [190].

7.3.2 Why Biometrics for Authenticating Riders?

Biometrics refers to the identification of individuals based on their physiological and/or behavioral characteristics [134]. The advances in sensor technologies, data processing techniques, and machine learning algorithms led to the strengthening of biometric-based authentication systems. Many studies have shown that biometric-based authentication schemes are more reliable than conventional authentication schemes like knowledge-based and token-based authentication schemes [217]. Thus, multi-modal biometrics has the potential to become the defacto standard for authentication for various IoT services to enhance consumers' safety and security [218].

Some benefits of biometrics are: 1) biometrics are capable of ensuring the fast and reliable establishment of the individual's identity, 2) they can not be easily stolen, shared, transferred, conjectured, or hacked, 3) they do not add cognitive load on users, 4) they are hard to falsify, and 5) for smart devices, biometric-based authentication schemes have shown higher usability acceptance in contrast to conventional authentication schemes [92, 187, 190].

7.4 Rider Authentication Survey

We conducted an online survey[3] to study public opinion about rider authentication requirements for driverless taxis. The survey consists of 20 questions (refer Appendix C for questionnaire), overall. The questionnaire collects basic demographic data of the participants and includes questions from the need of rider authentication to the participants' awareness of biometrics, their opinion on physiological and behavioral biometric traits selection for rider authentication, their preferences for the employment of authentication mechanisms, and their major usability concerns.

The survey was published on various online public transport users groups and social media platforms like Linkedin, Facebook, Twitter for 4 weeks. We received approximately 75 responses, worldwide that were completely anonymous. The reporting of the survey results is divided into four sections: 1) demographic statistics, 2) rider authentication acceptance analysis, 3) security requirements analysis, and 4) usability requirements analysis.

7.4.1 Demographic Statistics

Our survey contains 3 demographics questions related to the participant's continent-wide location, age group, and gender. Demographic statistics of 75 participants are displayed in Figure 7.2.

Continent-wise participants distribution reported in Figure 7.2a shows the participation of all the continents having people's presence. Fig-

[3] https://forms.gle/BMg4aVbMqoZVf5mH7

ure 7.2b shows approximately 93.3% of survey participants were from the 17 *to* 45 age group, which is likely to be the age-group using public transport the most. Figure 7.2c exhibits gender-wise distribution with 69.3% male and 26.7% female participants.

7.4.2 Rider Authentication Acceptance Analysis

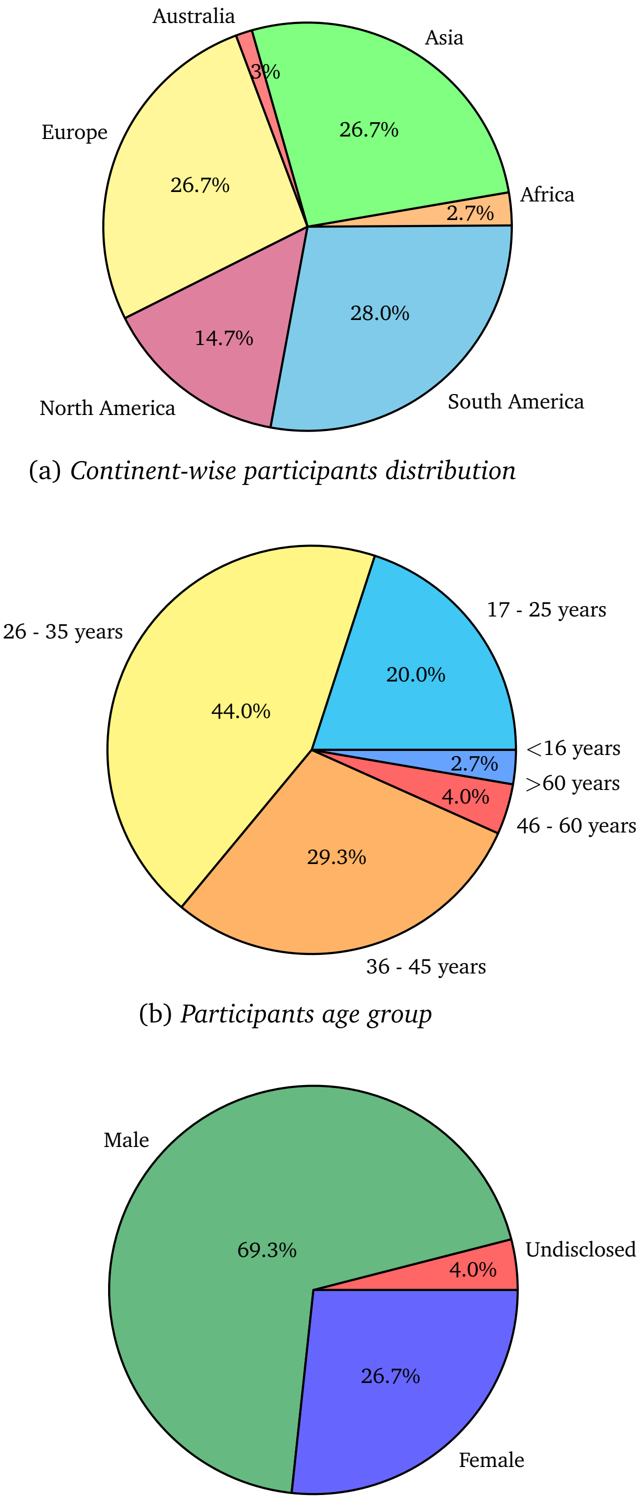
Figure 7.3 exhibits that approximately 90% of the overall participants either strongly agreed or agreed for the introduction of rider authentication for driverless taxis. However, only 4% of participants disagreed to introduce rider authentication, and 6.7% of participants' responses were neutral.

Participants' self-declaration on biometrics knowledge can be examined in Figure 7.4. Among all participants, 92% of participants are aware of biometric-based authentication schemes, and 76% of participants are using biometric-based authentication schemes as reported in Figure 7.4a and 7.4b, respectively. Lastly, 16%, 46.7%, 29.3%, and 8% indicated their knowledge on biometrics as excellent, good, fair, and negligible, respectively.

7.4.3 Security Requirements Analysis

Rider authentication survey poll shown in Figure 7.3 suggests that a robust authentication scheme to identify riders for driverless taxis emerged as a genuine requirement to foster better safety and security of customers and the general public.

The physiological and behavioral traits evaluated for rider authentication in the survey are listed below.



(a) *Continent-wise participants distribution*

(b) *Participants age group*

(c) *Participants gender*

Figure 7.2: Demographic statistics.

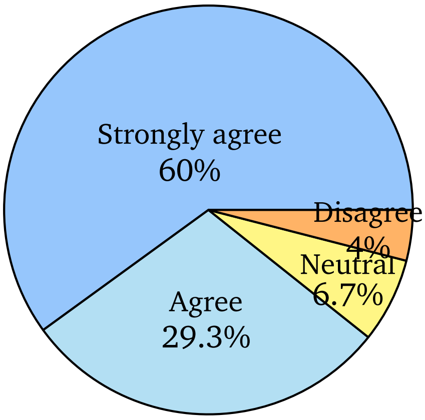


Figure 7.3: Rider authentication acceptance.

7.4.3.1 Physiological Traits

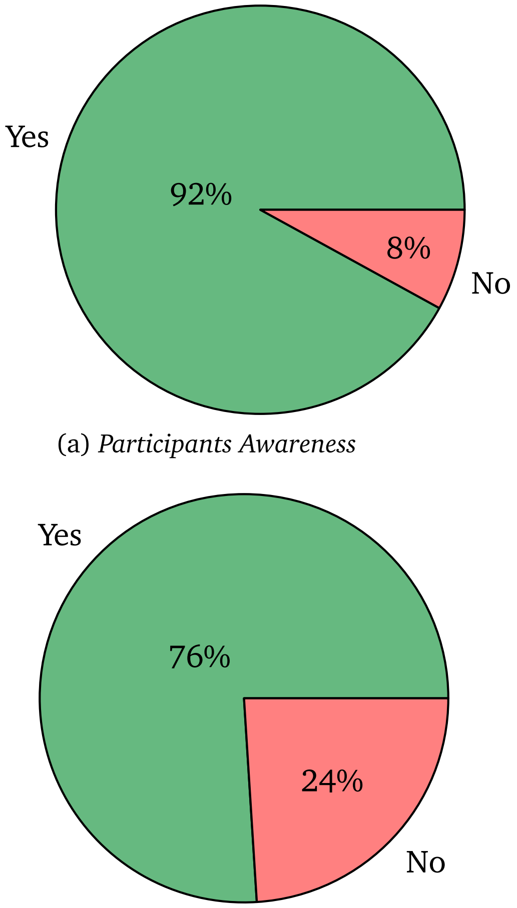
The traits included in this category are the face, fingerprint, iris, and retina.

- **Face:** It can be captured by using a two-dimensional ($2D$) camera operating in the visible spectrum [93, 197].
- **Fingerprint:** Similarly, either capacitive scanners or optical scanners can be used to capture fingerprints [161].
- **Iris/Retina:** Iris or retina can be captured with both ordinary light and invisible infrared camera [100, 208].

Driverless taxis are equipped with high-end imaging devices that can be utilized to acquire physiological traits. For example, Tesla fitted their driverless cars with eight external surround cameras to provide 360 degrees of visibility around the car at up to the range of 250 meters [249].

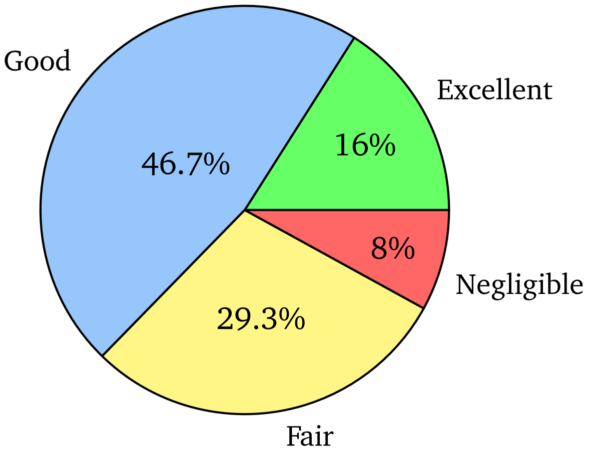
7.4.3.2 Behavioral Traits

The traits included in this category are voice, touch signature, keystroke/touch dynamics, gait, and hand-movements to hold or wear smart devices.



(a) *Participants Awareness*

(b) *Participants Usage*



(c) *Participants knowledge*

Figure 7.4: Participants self-declaration on biometrics.

- **Voice:** A digital voice recorder can be used to record the voice prints [93].
- **Touch signature:** A touch signature can be drawn by pen or stylus on touchscreen devices [254].
- **Keystroke/touch dynamics:** Features for keystroke and touch dynamics can be generated by fetching 2-D coordinates from touch sensors corresponding to the customer typing or swiping action [33].
- **Gait:** A human gait features can be extracted by fetching X, Y, and Z coordinates from sensors, such as accelerometer, magnetometer, and gyroscope [183, 138].
- **Hand-movements:** Similarly, a 3-D model for hand-movement trajectory can be created by fetching X, Y, and Z coordinates from sensors, such as accelerometer, magnetometer, and gyroscope [32, 95].

Some behavioral biometric traits, e.g., voice, touch signature, etc., can be easily implemented with existing technology deployed in modern automobiles, while others, e.g., gait, etc., may require some hardware adaptation. Seemingly, to acquire customers' voiceprints and touch signatures, hardware such as digital voice recorders and touchscreen devices can be deployed within the driverless taxis, seamlessly. Whereas, some traits like gait may depend on external devices for acquiring riders' data.

Participants' preference to introduce biometric-based rider authentication schemes for driverless taxis is shown in Figure 7.5. Approximately, 82.7% of participants suggested to employ physiological biometric-based authentication schemes, and 52% of participants suggested to employ behavioral biometric-based authentication schemes.

Furthermore, our survey poll determines that for critical systems like driverless taxis knowledge-based and token-based authentication schemes

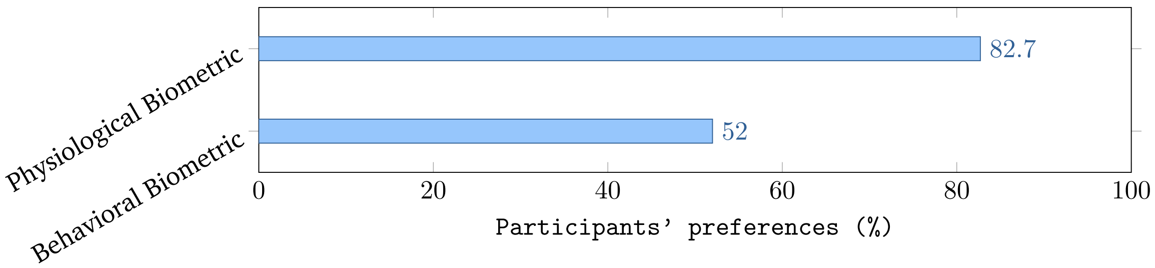
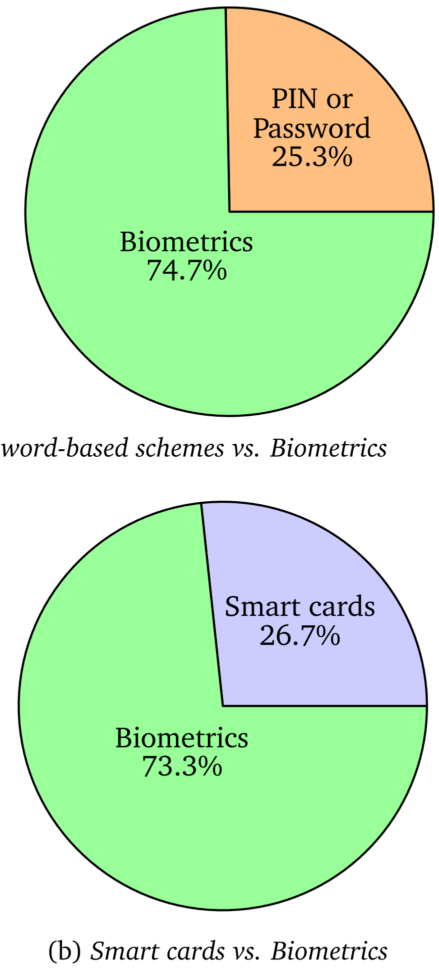


Figure 7.5: Biometric-based rider authentication scheme: participants preference.

for rider authentication have much less acceptability over biometric-based authentication schemes.



(a) *PIN/Password-based schemes vs. Biometrics*

(b) *Smart cards vs. Biometrics*

Figure 7.6: Other authentication schemes vs. biometrics for rider authentication.

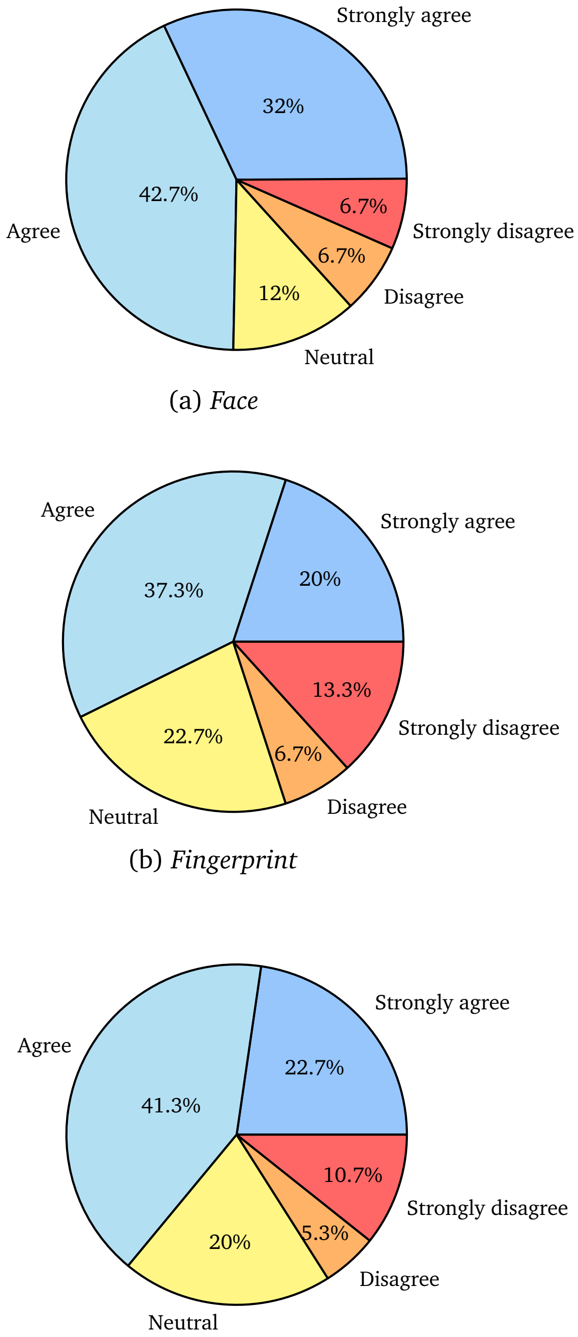
It can be observed in Figure 7.6a and Figure 7.6b, only 25.3%, and 26.7%

of overall participants suggested to employ PIN/ Password, and smart card, respectively for rider authentication in comparison to biometric-based authentication schemes. Interested readers may refer to a comprehensive literature survey by Gupta et al. [92] for more insights on types and ways of authentication schemes.

Figure 7.7a to 7.7c presents the survey participants' preferences to employ physiological biometric traits, i.e., face (74.7%), fingerprint (57.3%), and iris/retina (64.0%), for rider authentication for driverless taxis, and Figure 7.8a to 7.8e presents the survey participants' preferences to employ behavioral biometric traits, i.e., voice (49.3%), touch signatures (48.0%), keystroke/touch dynamics (38.7%), gait (26.6%), and hand-movements (33.4%) to hold or wear smart devices, for rider authentication for driverless taxis. These responses are measured on a 5-point scale ranging from "strongly agree" to "strongly disagree".

The level of acceptance (i.e. total of strongly agreed and agreed percentage) of biometric traits by the participants is shown in Figure 7.9.

According to the survey poll, the human face emerged out as the most preferred biometric trait for rider authentication. From a deployment point of view, acquiring customers' face image to authenticate them before allowing access to driverless taxis does not require any additional hardware, as driverless taxis are already equipped with high-resolution digital cameras. Our survey poll suggests biometric-based rider authentication schemes for driverless taxis clearly emerged as security requirements towards the safety and security of their customers and the general public.

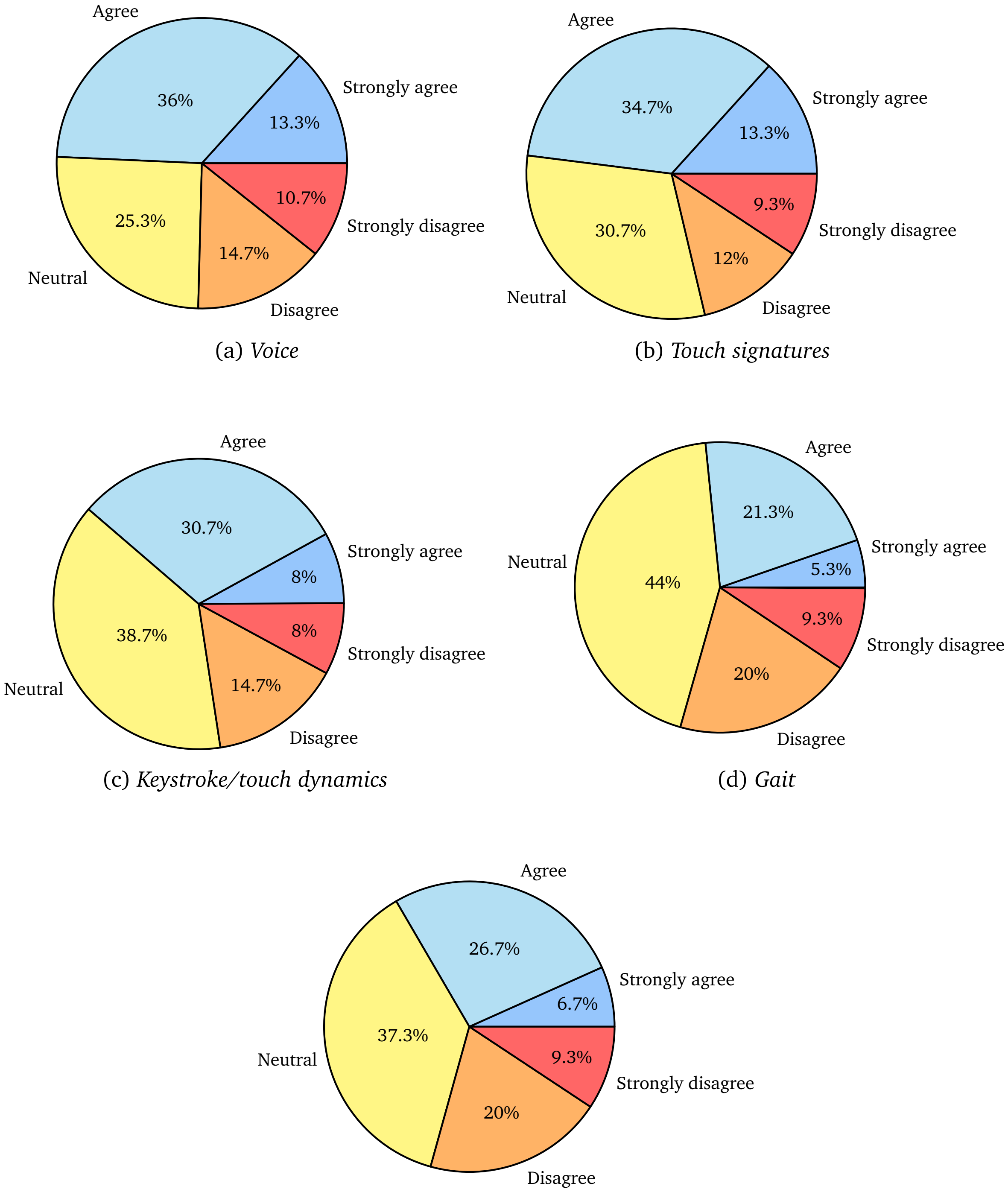


(a) *Face*

(b) *Fingerprint*

(c) *Iris/retina*

Figure 7.7: Participants' preferences to use physiological biometric traits.



(a) *Voice*

(b) *Touch signatures*

(c) *Keystroke/touch dynamics*

(d) *Gait*

(e) *Hand-movements to hold or wear smart devices*

Figure 7.8: Participants' preferences to use behavioral biometric traits.

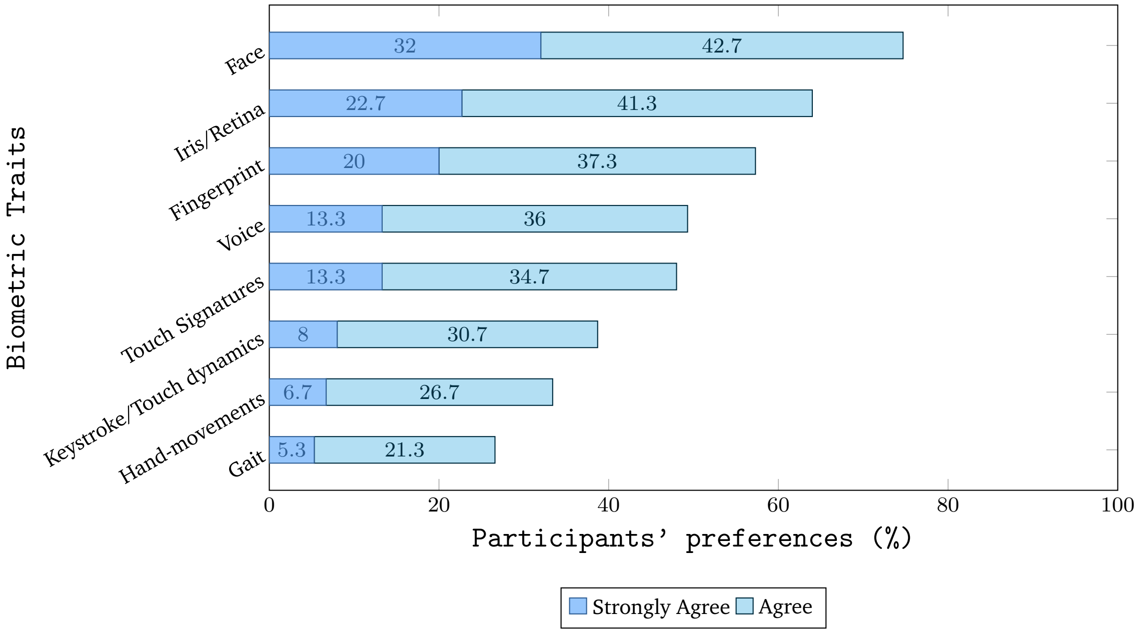


Figure 7.9: Rider authentication scheme: biometric traits-wise participants suggestion.

7.4.4 Usability Requirements Analysis

To design a usable user authentication scheme, correct implementation of desired usability requirements plays a pivotal role [24, 92]. Moreover, the usability requirements described for a particular product or system security must be feasible, verifiable, and comprehensive.

The number of training samples required to create users profile for a biometric trait is an important usability criterion for a usable user authentication system design [132]. The survey poll for training samples, as depicted in Figure 7.10, exhibits that 48%, 25.3%, and 6.7% of participants are happy to provide $1 - to - 5$, $5 - to - 10$ and $10 - to - 30$ samples, respectively. However, only, 6.7% of participants are willing to provide more than 30 samples.

The time to acquire training samples is directly proportional to the number of training samples. Users may be annoyed with authentication schemes having longer training samples acquisition time [132]. It is necessary to

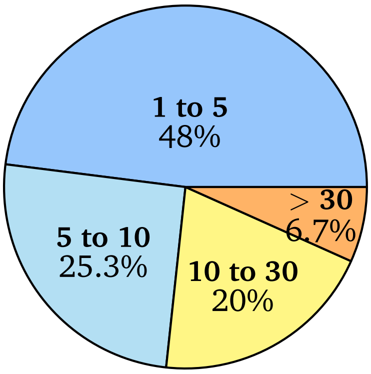


Figure 7.10: Training samples for user profile creation.

keep the number of training samples to a minimum, yet guaranteeing an acceptable level of accuracy, thus security. Most likely, a minimal number of training samples can motivate customers to accept rider authentication schemes for driverless taxis.

For a comprehensive usability requirements analysis of a rider authentication system, there are several more norms to be considered and fulfilled, however, they are out of the scope of this survey. Conclusively, the usability and security requirements to design a rider authentication system can be traded accordingly, to befitting the end-user experience.

7.5 A Proposal for Rider Authentication Framework

The Transportation-As-A-Service (TAAS) primarily consists of three stakeholders: (a) the servers maintained by a service provider, (b) the riders, and (c) the driverless taxis.

7.5.1 Interaction between the Stakeholders

During the ride-booking process, the typical interaction between these three stakeholders is illustrated in Figure 7.11.

1. A customer can book a ride by using the ride-booking smartphone application (client) provided the service provider (server). Before

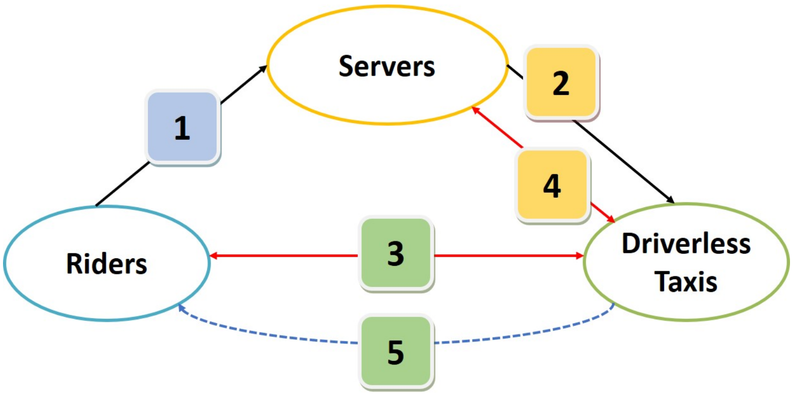


Figure 7.11: TAAS: interaction between the stakeholders.

booking a ride, a customer requires to register with the service provider, which is the one-time activity. The driverless taxis can collect the training samples from customers during their first ride and transfer the data to the server to construct the classification model.

Taking various driverless taxi usage scenarios into account, e.g., customers that prefer to use driverless taxis for a short term or only once, the user registration process is required to be user-friendly. One way to achieve a user-friendly registration design includes furnishing important information such as the number of training samples, sample acquisition time, and classification model training time, for each biometric trait a priori to customers [92]. This information will guide customers to select biometric traits for enrolment accordingly, and at the same, their expectations will meet. Similarly, a simplified method to unregister from taxi-booking applications can be incorporated into the design that ensures a hassle-free exit for customers.

2. Upon receiving a ride-booking, the server assigns the driverless taxi to pick or drop the customer from/to the location as requested by the customer.

3. The driverless taxi asks the customers to authenticate themselves before letting them board the taxi. Driverless taxi's client application provides an interface to collect the biometrics from the customer for authentication purpose. The data collected from the customer is sent to the server by the driverless taxi (client application) and matched against the training data collected from the customer during the registration process.

4. The driverless taxi transmits the data collected from the customer to the server. The server verifies the input data of the customer with her stored template at the server's database.

5. The driverless taxi decides to accept or reject the customer according to the authentication result obtained from the server.

7.5.2 Methodology for Rider Authentication

According to the survey's results, our design refers to a biometric-based authentication mechanism. Authentication or verification can be termed as a one-to-one matching process. This further can be elaborated as the process to assert the claimant's identity by matching against one or more previously enrolled templates with the help of various classification algorithms [92].

Since driverless taxis can offer rides to multiple customers, customer authentication problem can be addressed by implementing a multi-class classification model, i.e., an n-classification problem. *Multi-class classification model* can classify more than two classes. Each `class` represents an enrolled customer. Classes are mutually exclusive to each other, and each new instance particularly belongs to one of the classes present in the model.

Mathematically, the authentication process can represented by Equation 7.1.

$$R_A = \begin{cases} \text{M} & \text{if } \mathbf{CM}(C_I, C_T) \text{ is } \geq \text{ T} \\ \text{NM} & \text{if } \mathbf{CM}(C_I, C_T) \text{ is } < \text{ T} \end{cases} \tag{7.1}$$

Where, CM is a classification model that receives the claimant's input (C_I) and claimant's templates (C_T) to find the similarity between them for a given threshold (T). The authentication result (R_A) is set to `Match` (M) or `Not_Match` (NM) according to the result obtained from classification model.

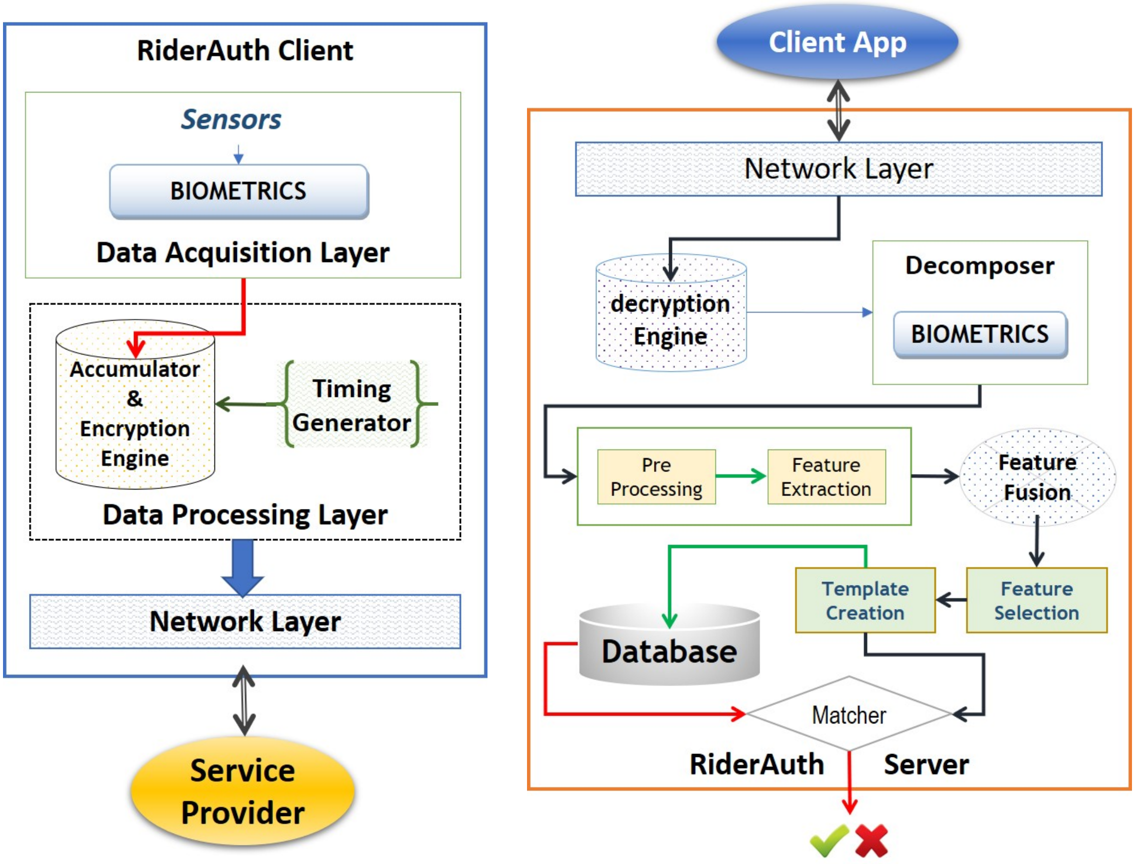
7.5.3 System Design Details

The authentication system uses a client-server architecture [94] to partitions the tasks (refer Figure 7.11) between the service providers, called servers, and service consumers, called clients. Figure 7.12 describes the design details of the Rider Authentication system. The client application consists of three layers, a) data acquisition layer, b) data processing layer, and c) the network layer as shown in Figure 7.12a. The data acquisition layer contains the required sensors to collect the biometrics data in a sequential manner using blocking-call-mechanism. Thus, the application ensures that all the user's input is acquired, successfully.

Inside the data processing layer, the data collected are temporarily stored by the accumulator and the encryption engine, for encryption, packaging, and time-stamping. Subsequently, the data is transferred to the server by the network layer.

The server side consists of a) a decryption engine, b) a decomposer, c) data preprocessing, d) features extraction module, e) feature fusion module, f) feature selection module, g) template creation module, and h) database module as shown in Figure 7.12b.

The decryption engine decrypts the user-data received from the client



(a) Client

(b) Server

Figure 7.12: Rider authentication system architecture.

application, which is further decomposed into individual biometric traits by decomposer module. After the data preprocessing and feature extraction, the feature fusion module fuses all the features extracted from each biometric. Further, inside the future selection module, the fused features are selected on the merit basis such that only productive features can be allocated for template creation.

During the user registration process, the user-training-template with selected features set is created and stored in the database by assigning a unique label for each user. When the customer access the driverless taxi to commence her ride, the driverless-taxi-client application collects and transmits the customer data to generate a test template for her in real-time. Thus, the customer is authenticated by matching her test template with her stored labeled training templates on the server.

7.6 Summary

The research community has started determining and addressing potential security risks and vulnerabilities in different areas of driverless vehicles. However, unsupervised physical access to driverless taxis exposes them to customers with different motivations, such as curiosity, monetary benefits, malicious intentions, or terrorism [50]. From customers and the general public safety and security standpoint, rider authentication for driverless taxis become an essential requirement that can also be interpreted from our online survey results.

Our online survey received 75 responses from participants, worldwide. Approximately, 90% of the overall participants in our survey either agreed or strongly agreed with the necessity to deploy biometric-based rider authentication for driverless taxis. Among several compelling challenges to be resolved, which may stymie the adoption of driverless taxis by masses - the deployment of a usable and secure rider authentication scheme is equally requisite.

Chapter 8

Conclusions

The burgeoning IoT applications are so ingrained in our lives that it is nearly impossible to think a day without smart devices, smart enterprises, smart homes or offices, etc. Almost every business verticals, e.g., automotive, energy, entertainment, education, food, finance, healthcare, manufacturing, transportation, etc., have embraced IoT, wholeheartedly. Cisco[1] has predicted that there will be more than half a trillion IoT-enabled ecosystem by 2030. The IoT applications can be a critical part of business strategies for all the business verticals going forward. Many of these IoT applications are safety-critical and any unauthorized access could have severe consequences to their consumers and society.

Human-to-machine authentication is critical for IoT applications, however, drawbacks of conventional user authentication schemes, from both security and usability perspectives, have been identified as a crucial concern to the IoT security spectrum. The various security and usability challenges that users are facing in using conventional user authentication schemes led to a realization that user authentication schemes require upgrading for new IoT age applications.

HOLD & TAP is a risk-driven one-shot-cum-continuous user authentica-

[1] https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

tion solution for smart devices' IoT applications based on users' invisible tap-timings and hand-movements. The scheme can be seamlessly integrated into the existing PIN/password-based authentication schemes to enhance their usability and security. It strengthens the widely used PIN/password-based authentication technology by giving flexibility to users to enter any random 8-digit alphanumeric text, instead of preconfigured PIN/Passwords. STEP & TURN is a novel bimodal behavioral biometric-based authentication system based on two natural human actions, i.e., single footstep and hand-movement to secure smart homes or offices access to their legitimate users.

DRIVERAUTH and RIDERAUTH offer risk-based authentication schemes for smart enterprises strengthening the security and safety of their consumers and society. DRIVERAUTH is a risk-based multi-modal authentication scheme that exploits three biometric modalities, i.e., swipe gestures, *text-independent* voice and face, to make the on-demand ride and ride-sharing services secure and safer for riders. RIDERAUTH discussed various biometric-based riders authentication schemes for driverless taxis. Survey results are analyzed to study rider authentication requirements along with the proposal for a rider authentication framework that uses physiological and behavioral biometric traits.

Our user authentication designs for smart devices, smart enterprise, smart home, or office applications are novel contributions towards the development of next-generation user authentication schemes for IoT applications.

Bibliography

[1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] Ioannis Agadakos, Chien-Ying Chen, Matteo Campanelli, Prashant Anantharaman, Monowar Hasan, Bogdan Copos, Tancrède Lepoint, Michael Locasto, Gabriela F Ciocarlie, and Ulf Lindqvist. Jumping the air gap: Modeling cyber-physical attack paths in the internet-of-things. In *Proceedings of the Workshop on Cyber-Physical Systems Security and PrivaCy*, pages 37–48. ACM, 2017.

[3] Wael Jabbar Abed Al-Nidawi, Mahdi Athab Maan, and Marini Othman. Review on national electronic identification system. In *Proceedings of 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2015*, pages 228–233. IEEE, 2015.

[4] Android. Developers guide: Sensorevent. https://developer.android.com/reference/android/hardware/SensorEvent.html, 2020 *(Accessed on 2020-07-28)*. online web resource.

[5] Manos Antonakakis. Understanding the mirai botnet. In *Proceedings of the 26th USENIX Security Symposium*, pages 1093–1110, 2017.

[6] Hagai Aronowitz, Min Li, Orith Toledo-Ronen, Sivan Harary, Amir Geva, Shay Ben-David, Asaf Rendel, Ron Hoory, Nalini Ratha, Sharath Pankanti, et al. Multi-modal biometrics for mobile authentication. In *Proceedings of International Joint Conference on Biometrics (IJCB)*, pages 1–8. IEEE, 2014.

[7] Adam J Aviv, Katherine L Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. Smudge attacks on smartphone touch screens. *Woot*, 10:1–7, 2010.

[8] Mohammed Awad, Zakaria Al-Qudah, Sahar Idwan, and Abdul Halim Jallad. Password security: Password behavior analysis at a small university. In *Proceedings of the 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, pages 1–4. IEEE, 2016.

[9] Mourad Ben Ayed. Method for adaptive authentication using a mobile device, feb #4 2014. US Patent 8,646,060.

[10] BBC. Uber driver background checks not good enough. http://www.bbc.com/news/technology-34002051, 2015 *(Accessed on 2020-07-28)*. Online web resource.

[11] Marios Belk, Panagiotis Germanakos, Christos Fidas, and George Samaras. A personalization method based on human factors for improving usability of user authentication tasks. In *Proceedings of the International Conference on User Modeling, Adaptation, and Personalization*, pages 13–24. Springer, 2014.

[12] Karissa Bell. Uber makes it harder to give drivers bad ratings. https://mashable.com/2017/11/21/uber-makes-it-harder-to-give-bad-ratings/#DghVf5kP0qqR, 2017 *(Accessed on 2020-07-28)*. Online web resource.

[13] Elisa Bertino, Claudio Bettini, Elena Ferrari, and Pierangela Samarati. An access control model supporting periodicity constraints and temporal reasoning. *ACM Transactions on Database Systems (TODS)*, 23(3):231–285, 1998.

[14] Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. *Proc. USEC*, pages 1–2, 2015.

[15] Tapalina Bhattasali, Khalid Saeed, Nabendu Chaki, and Rituparna Chaki. A survey of security and privacy issues for biometrics based remote authentication in cloud. In *Proceedings of the IFIP International Conference on Computer Information Systems and Industrial Management*, pages 112–121. Springer, 2014.

[16] Randolph G Bias. The pluralistic usability walkthrough: coordinated empathies. In *Proceedings of the Usability inspection methods*, pages 63–76. John Wiley & Sons, Inc., 1994.

[17] Battista Biggio, Giorgio Fumera, Gian Luca Marcialis, and Fabio Roli. Statistical meta-analysis of presentation attacks for secure multibiometric systems. *IEEE transactions on pattern analysis and machine intelligence*, 39(3):561–575, 2017.

[18] Ruud M Bolle, Jonathan H Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. *Guide to biometrics*. Springer Science & Business Media, 2013.

[19] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the Symposium on Security and Privacy*, pages 553–567. IEEE, 2012.

[20] Joseph Bonneau, Sören Preibusch, and Ross J Anderson. A birthday present every eleven wallets? the security of customer-chosen banking pins. In *Proceedings of the Financial Cryptography*, volume 7397, pages 25–40. Springer, 2012.

[21] Joseph Bonneau and Stuart Schechter. Towards reliable storage of 56-bit secrets in human memory. In *Proceedings of the 23*rd *USENIX Security Symposium*, pages 607–623, 2014.

[22] Robert Booth. Uber whistleblower exposes breach in driver-approval process. https://www.theguardian.com/technology/2015/jun/12/uber-whistleblower-exposes-breach-driver-approval-process, 2015 *(Accessed on 2020-07-28)*. Online web resource.

[23] Christina Braz and Jean-Marc Robert. Security and usability: the case of the user authentication methods. In *Proceedings of the 18*th *Conference on l'Interaction Homme-Machine*, pages 199–203. ACM, 2006.

[24] Christina Braz, Ahmed Seffah, and Bilal Naqvi. *Integrating a Usable Security Protocol Into User Authentication Services Design Process*. Auerbach Publications, 2018.

[25] Leo Breiman. Random forests. *Machine learning*, 45(1):5–32, 2001.

[26] Frank Breitinger and Claudia Nickel. User survey on phone security and usage. In *Proceedings of the BIOSIG*, pages 139–144, 2010.

[27] Marcelo Luiz Brocardo, Issa Traore, and Isaac Woungang. Toward a framework for continuous authentication using stylometry. In *Proceedings of the 28*th *International Conference on Advanced Information Networking and Applications (AINA)*, pages 106–115. IEEE, 2014.

[28] John Brooke. Sus: a retrospective. *Journal of usability studies*, 8(2):29–40, 2013.

[29] Roberto Brunelli and Daniele Falavigna. Person identification using multiple cues. *IEEE transactions on pattern analysis and machine intelligence*, 17(10):955–966, 1995.

[30] Kevin Brunet, Karim Taam, Estelle Cherrier, Ndiaga Faye, and Christophe Rosenberger. Speaker recognition for mobile user authentication: An android solution. In *Proceedings of the 8ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR SSI)*, page 10, 2013.

[31] Manuel Burghardt. Usability pattern identification through heuristic walkthroughs. In *Proceedings of the International Conference of Design, User Experience, and Usability*, pages 219–230. Springer, 2016.

[32] Attaullah Buriro, Bruno Crispo, Mojtaba Eskandri, Sandeep Gupta, Athar Mahboob, and Rutger Van Acker. Snapauth: A gesture-based unobtrusive smartwatch user authentication scheme. In *Proceedings of International Workshop on Emerging Technologies for Authorization and Authentication*, pages 30–37. Springer, 2018.

[33] Attaullah Buriro, Sandeep Gupta, and Bruno Crispo. Evaluation of motion-based touch-typing biometrics in online financial environments. *BIOSIG 2017*, 2017.

[34] Martin Butler and Rika Butler. Investigating the possibility to use differentiated authentication based on risk profiling to secure online banking. *Information & Computer Security*, 23(4):421–434, 2015.

[35] CAPEC-Release1.6. Common attack pattern enumeration and classification, 2016. online web resource.

[36] Brad Causey. Adaptive authentication: An introduction to risk-based authentication. http://searchsecurity.techtarget.com/tip/Adaptive-authentication-An-introduction-to-risk-based-authentication, 2013 *(Accessed on 2020-07-28)*. online web resource.

[37] ByungRae Cha, Namho Kim, and JongWon Kim. Prototype analysis of otp key-generation based on mobile device using voice characteristics. In *Proceedings of the International Conference on Information Science and Applications (ICISA)*, pages 1–5. IEEE, 2011.

[38] Arthur Charles. The guardian - iphone 5s fingerprint sensor hacked by germany's chaos computer club. https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked, 2013 *(Accessed on 2020-07-28)*. online web resource.

[39] Suresh Chavhan, Deepak Gupta, BN Chandana, Ashish Khanna, and Joel JPC Rodrigues. Agent pseudonymous authentication-based conditional privacy preservation: An emergent intelligence technique. *IEEE Systems Journal*, 2020.

[40] Hoyul Choi, Hyunsoo Kwon, and Junbeom Hur. A secure otp algorithm using a smartphone application. In *Proceedings of the 7th International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 476–481. IEEE, 2015.

[41] Ming-Chin Chuang and Meng Chang Chen. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. *Expert Systems with Applications*, 41(4):1411–1418, 2014.

[42] ClearLogin. Risk-based authentication. http://www.clearlogin.com/glossary/risk-based-authentication/, 2017 *(Accessed on 2020-07-28)*. online web resource.

[43] Kate Conger. Uber says 3,045 sexual assaults were reported in u.s. rides last year. https://www.nytimes.com/2019/12/05/technology/uber-sexual-assaults-murders-deaths-safety.html, 2019 *(Accessed on 2020-07-28)*. Online web resource.

[44] Patrick Connor and Arun Ross. Biometric recognition by gait: A survey of modalities and features. *Computer Vision and Image Understanding*, 167:1–27, 2018.

[45] Mauro Conti, Irina Zachia-Zlatea, and Bruno Crispo. Mind how you answer me!: transparently authenticating the user of a smartphone when answering or placing a call. In *Proceedings of the 6th ACM Symposium on Information Computer and Communications Security*, pages 249–259. ACM, 2011.

[46] Nelson Cowan, Candice C Morey, Zhijian Chen, Amanda L Gilchrist, and J Scott Saults. Theory and measurement of working memory capacity limits. *Psychology of Learning and Motivation*, 49:49–104, 2008.

[47] Heather Crawford and Karen Renaud. Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management*, 1(1):7, 2014.

[48] David Crouse, Hu Han, Deepak Chandra, Brandon Barbello, and Anil K Jain. Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data. In *Proceedings of the International Conference on Biometrics (ICB)*, pages 135–142. IEEE, 2015.

[49] Madeleine Cuff. Smart digital tattoos. http://www.stylus.com/scckpj, 2014 *(Accessed on 2020-07-28)*. online web resource.

[50] Gonzalo De La Torre, Paul Rad, and Kim-Kwang Raymond Choo. Driverless vehicle security: Challenges and future research opportunities. *Future Generation Computer Systems*, 2018.

[51] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 987–996. ACM, 2012.

[52] Alexander De Luca, Alina Hang, Emanuel Von Zezschwitz, and Heinrich Hussmann. I feel like i'm taking selfies all day!: Towards understanding biometric authentication on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1411–1414. ACM, 2015.

[53] Howard B Demuth, Mark H Beale, Orlando De Jess, and Martin T Hagan. *Neural network design*. Martin Hagan, 2014.

[54] Ekberjan Derman and Albert Ali Salah. Continuous real-time vehicle driver authentication using convolutional neural network based face recognition. In *Proceedings of the 13th IEEE International Conference on Automatic Face and Gesture Recognition*, pages 577–584. IEEE, 2018.

[55] Nitesh Dhanjani. *Abusing the internet of things: blackouts, freakouts, and stakeouts*. O'Reilly Media, Inc., 2015.

[56] DMR. Amazing uber statistics, demographics and facts. https://expandedramblings.com/index.php/uber-statistics/, 2019 *(Accessed on 2020-07-28)*. Online web resource.

[57] DMR. Interesting lyft statistics and facts. https://expandedramblings.com/index.php/lyft-statistics/, 2019 *(Accessed on 2020-07-28)*. Online web resource.

[58] DMR. Interesting ola statistics and facts. https://expandedramblings.com/index.php/lyft-statistics/, 2019 *(Accessed on 2020-07-28)*. Online web resource.

[59] Jeyoun Dong and Myunghwan Byun. Enhanced usability assessment on user satisfaction with multiple devices. In *Proceedings of the Advanced Multimedia and Ubiquitous Engineering*, pages 849–853. Springer, 2018.

[60] RPW Duin, P Juszczak, P Paclik, E Pekalska, D De Ridder, DMJ Tax, and S Verzakov. A matlab toolbox for pattern recognition. *PRTools version*, 3:109–111, 2000.

[61] Deepak Chandra Dutt, Anil Buntwal Somayaji, and Michael John Kendal Bingham. System and method for implicit authentication, October 10 2017. US Patent 9,788,203.

[62] Saurabh Dutta. *Striking a balance between usability and cyber-security in IoT devices*. PhD thesis, Massachusetts Institute of Technology, 2017.

[63] Shawn Eastwood and S Yanushkevich. Risk profiler in automated human authentication. In *Proceedings of IEEE Symposium on Computational Intelligence for Engineering Solutions (CIES)*, pages 140–147. IEEE, 2014.

[64] Shawn C Eastwood, Vlad P Shmerko, Svetlana N Yanushkevich, M Drahansky, and Dmitry O Gorodnichy. Biometric-enabled authentication machines: A survey of open-set real-world applications. *IEEE Transactions on Human-Machine Systems*, 46(2):231–242, 2016.

[65] Simon Eberz, Kasper B Rasmussen, Vincent Lenders, and Ivan Martinovic. Evaluating behavioral biometrics for continuous authentication: Challenges and metrics. In *Proceedings of the Asia Conference on Computer and Communications Security*, pages 386–399. ACM, 2017.

[66] Michael Edwards and Xianghua Xie. Footstep pressure signal analysis for human identification. In *Proceedings of the 7th International Conference on Biomedical Engineering and Informatics*, pages 307–312. IEEE, 2014.

[67] Mohammed El-hajj, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni. A survey of internet of things (iot) authentication schemes. *Sensors*, 19(5):1141, 2019.

[68] Daniel P. W. Ellis. Plp, rasta, mfcc, and inversion in matlab. http://www.ee.columbia.edu/~dpwe/resources/matlab/rastamat/, 2005 *(Accessed on 2020-07-28)*. Online web resource.

[69] Tom Fawcett. Roc graphs: Notes and practical considerations for researchers. *Machine learning*, 31(1):1–38, 2004.

[70] Tom Fawcett. An introduction to roc analysis. *Pattern recognition letters*, 27(8):861–874, 2006.

[71] Florian Feldmann. *Binding credentials: Securing (SSO) authentication*. PhD thesis, Ruhr-Universität Bochum, 2016.

[72] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunar, Yifei Jiang, and Nhung Nguyen. Continuous mobile authentication using touchscreen gestures. In *Proceedings of IEEE Conference on Technologies for Homeland Security (HST)*, pages 451–456. IEEE, 2012.

[73] Earlence Fernandes, Amir Rahmati, Kevin Eykholt, and Atul Prakash. Internet of things security research: A rehash of old ideas or new intellectual challenges? *IEEE Security & Privacy*, 15(4):79–84, 2017.

[74] First4magnets. Use of neodymium magnets. https://www.first4magnets.com/tech-centre-i61/information-and-articles-i70/neodymium-magnet-information-i82/common-applications-of-neodymium-magnets-i88, 2020 *(Accessed on 2020-07-28)*.

[75] Eelke Folmer and Jan Bosch. Architecting for usability: a survey. *Journal of systems and software*, 70(1-2):61–78, 2004.

[76] CO Folorunso, LA Akinyemi, AA Ajasa, and K Oladipupo. Design and development of fingerprint based car starting system. In *Proceedings of the International Conference and Exhibition on Power and Telecommunications*, 2015.

[77] Mikhail Fomichev, Flor Alvarez, Daniel Steinmetzer, Paul Gardner-Stephen, and Matthias Hollick. Survey and systematization of secure device pairing. *IEEE Communications Surveys & Tutorials*, 2017.

[78] Nils Forsblom. Were you aware of all these sensors in your smartphone? https://blog.adtile.me/2015/11/12/were-you-aware-of-all-these-sensors-in-your-smartphone/, 2015 *(Accessed on 2020-07-28)*. online web resource.

[79] Ian J Forster and Adrian N Farr. Method for preventing unauthorized diversion of nfc tags, July 26 2017. US Patent App. 15/659,941.

[80] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, 8(1):136–148, 2013.

[81] Lex Fridman, Steven Weber, Rachel Greenstadt, and Moshe Kam. Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location. *IEEE Systems Journal*, 11(2):513–521, 2017.

[82] Erik Frøkjær and Kasper Hornbæk. Metaphors of human thinking for usability inspection and design. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 14(4):20, 2008.

[83] Steven Furnell. The usability of security–revisited. *Computer Fraud & Security*, 2016(9):5–11, 2016.

[84] Attlee M Gamundani, Amelia Phillips, and Hippolyte N Muyingi. An overview of potential authentication threats and attacks on internet of things (iot): A focus on smart home applications. In *Proceedings of IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 50–57. IEEE, 2018.

[85] Sonia Garcia-Salicetti, Charles Beumier, Gérard Chollet, Bernadette Dorizzi, Jean Leroux Les Jardins, Jan Lunter, Yang Ni, and Dijana Petrovska-Delacrétaz. Biomet: A multimodal person authentication database including face, voice, fingerprint, hand and signature modalities. In *Proceedings of the International Conference on Audio-and Video-based Biometric Person Authentication*, pages 845–853. Springer, 2003.

[86] GDPR. Ethics and data protection. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf, 2018 *(Accessed on 2020-07-28)*. online web resource.

[87] Cristiano Giuffrida, Kamil Majdanik, Mauro Conti, and Herbert Bos. I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. In *Proceeding of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 92–111. Springer, 2014.

[88] Mikhail I Gofman, Sinjini Mitra, Tsu-Hsiang Kevin Cheng, and Nicholas T Smith. Multimodal biometrics for enhanced mobile device security. *Communications of the ACM*, 59(4):58–65, 2016.

[89] Google. G suite: single sign-on on an android device. https://support.google.com/a/users/answer/2758865?hl=en, 2016 *(Accessed on 2020-07-28)*. online web resource.

[90] Richard P Guidorizzi. Security: active authentication. *IT Professional*, 15(4):4–7, 2013.

[91] Manik Gupta, Catherine Holloway, Behzad Momahed Heravi, and Stephen Hailes. A comparison between smartphone sensors and bespoke sensor devices for wheelchair accessibility studies. In *Proceedings of the 10th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015*, pages 1–6. IEEE, 2015.

[92] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. Demystifying authentication concepts in smartphones: Ways and types to secure access. *Mobile Information Systems*, 2018, 2018.

[93] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. Driverauth: A risk-based multimodal biometric-based driver authentication scheme for ride-sharing platforms. *Computers & Security*, 83:122–139, 2019.

[94] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. Driverauth: Behavioral biometric-based driver authentication mechanism for on-demand ride and ridesharing infrastructure. *ICT Express*, 5(1):16–20, 2019.

[95] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. Smarthandle: A novel behavioral biometric-based authentication scheme for smart lock systems. In *Proceedings of the 3rd International Conference on Biometric Engineering and Applications*. ACM, 2019.

[96] Sandeep Gupta, Attaullah Buriro, and Bruno Crispo. A chimerical dataset combining physiological and behavioral biometric traits for reliable user authentication on smart devices and ecosystems. *Data in brief*, 28:104924, 2020.

[97] Sandeep Gupta and Bruno Crispo. A perspective study towards biometric-based rider authentication schemes for driverless taxis. In *Proceeding of the International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pages 1–6. IEEE, 2019.

[98] Morey J Haber. Zero trust. In *Proceedings of the Privileged Attack Vectors*, pages 295–304. Springer, 2020.

[99] Yacov Y Haimes. *Risk modeling, assessment, and management*. John Wiley & Sons, 2015.

[100] Josef Hájek and Martin Drahanskỳ. Recognition-based on eye biometrics: Iris and retina. In *Proceedings of the Biometric-Based Physical and Cybersecurity Systems*, pages 37–102. Springer, 2019.

[101] Kimmo Halunen, Juha Häikiö, and Visa Vallivaara. Evaluation of user authentication methods in the gadget-free world. *Pervasive and Mobile Computing*, 40:220–241, 2017.

[102] Jiawei Han, Jian Pei, and Micheline Kamber. *Data mining: concepts and techniques*. Elsevier, 2011.

[103] Shuangshuang Han, Dongpu Cao, Li Li, Lingxi Li, Shengbo Eben Li, Nan-Ning Zheng, and Fei-Yue Wang. From software-defined vehicles to self-driving vehicles: A report on cpss-based parallel driving. *IEEE Intelligent Transportation Systems Magazine*, 11(1):6–14, 2019.

[104] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *Proceedings of the Symposium on usable privacy and security (SOUPS)*, pages 9–11, 2014.

[105] Austin Jay Harris and David C Yen. Biometric authentication: assuring access to information. *Information Management & Computer Security*, 10(1):12–19, 2002.

[106] Harvard. Technology factsheet series: Internet of things. https://www.belfercenter.org/sites/default/files/2019-06/TechFactSheet/iot%20-%205.pdf, 2019 *(Accessed on 2020-07-28)*. Online web resource.

[107] Hasib Hassan, Sylvie Wacquant, and Heinz B Seifert. Vehicle driver monitoring system, March 20 2017. US Patent App. 15/463,293.

[108] Kayla J Heffernan. Insertables workshop. https://insertables.wordpress.com/, 2016 *(Accessed on 2020-07-28)*. online web resource.

[109] Kayla J Heffernan, Frank Vetere, Lauren M Britton, Bryan Semaan, and Thecla Schiphorst. Insertable digital devices: Voluntarily under the skin. In *Proceedings of the Companion Publication on Designing Interactive Systems*, pages 85–88. ACM, 2016.

[110] Kayla J Heffernan, Frank Vetere, and Shanton Chang. Towards insertables: Devices inside the human body. *First Monday*, 22(3), 2017.

[111] Setia Hermawati and Glyn Lawson. Establishing usability heuristics for heuristics evaluation in a specific domain: Is there a consensus? *Applied ergonomics*, 56:34–51, 2016.

[112] Alex Hern. The guardian - samsung galaxy s8 iris scanner fooled by german hackers. https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security, 2017 *(Accessed on 2020-07-28)*. online web resource.

[113] Martin Reese Hestbek, Claudia Nickel, and Christoph Busch. Biometric gait recognition for mobile devices using wavelet transform and support vector machines. In *Proceedings of the 19th International Conference on Systems, Signals and Image Processing (IWSSIP)*, pages 205–210. IEEE, 2012.

[114] Daniel Hintze, Eckhard Koch, Sebastian Scholz, and René Mayrhofer. Location-based risk assessment for mobile authentication. In *Proceedings of International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, pages 85–88. ACM, 2016.

[115] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th Asia conference on computer and communications security*, pages 461–472. ACM, 2016.

[116] Josh Horwitz. Fake drivers and passengers are boosting uber's growth in china. https://qz.com/423288/fake-drivers-and-passengers-are-boosting-ubers-growth-in-china, 2015 *(Accessed on 2020-07-28)*. Online web resource.

[117] RJ Hulsebosch, Mortaza S Bargh, Gabriele Lenzini, PWG Ebben, and Sorin M Iacob. Context sensitive adaptive authentication. In *Proceedings of the European Conference on Smart Sensing and Context*, pages 93–109. Springer, 2007.

[118] Galen Hunt, George Letey, and Ed Nightingale. The seven properties of highly secure devices. *tech. report MSR-TR-2017-16*, 2017.

[119] HuntingtonVentures. Single sign on: The business of authentication. https://archive.is/20140315095827/http://www.authenticationworld.com/Single-Sign-On-Authentication, 2006 *(Accessed on 2020-07-28)*. online web resource.

[120] Susan L Hura. Usability testing of spoken conversational systems. *Journal of Usability Studies*, 12(4):155–163, 2017.

[121] IBIA. Behavioral biometrics. https://www.ibia.org/biometrics-and-identity/biometric-technologies/behavioral-biometrics, 2017 *(Accessed on 2020-07-28)*. online web resource.

[122] IBM. Ibm trusteer. https://www.ibm.com/it-it/marketplace/trusteer-mobile-sdk, 2016 *(Accessed on 2020-07-28)*. online web resource.

[123] IdentityAutomation. Risk-based authentication. https://www.identityautomation.com/iam-platform/rapididentityidentity-access-management/multi-factor-authentication/risk-based-authentication/, 2017 *(Accessed on 2020-07-28)*. online web resource.

[124] IdentityAutomation. What is adaptive authentication? http://blog.identityautomation.com/what-is-adaptive-authentication, 2017 *(Accessed on 2020-07-28)*. online web resource.

[125] Deloitte Insights Articles. Risk-based authentication: A primer. https://deloitte.wsj.com/cio/2013/10/30/risk-based-authentication-a-primer/, 2013 *(Accessed on 2020-07-28)*. online web resource.

[126] ISO13407:1999(en). Human-centred design processes for interactive systems. https://www.iso.org/obp/ui/#iso:std:iso:13407:ed-1:v1:en, 1999 *(Accessed on 2020-07-28)*. online web resource.

[127] ISO9000:2015. Quality management systems — fundamentals and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en, 2015 *(Accessed on 2020-07-28)*. online web resource.

[128] ISO/IEC24741:2018(en). Information technology — biometrics — overview and application. https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en, 2018 *(Accessed on 2020-07-28)*. Online web resource.

[129] ISO/IEC24745:2011(en). Biometric information protection. https://www.iso.org/obp/ui/#iso:std:iso-iec:24745:ed-1:v1:en, 2011 *(Accessed on 2020-07-28)*. Online web resource.

[130] Anil Jain, Ruud Bolle, and Sharath Pankanti. *Biometrics: personal identification in networked society*, volume 479. Springer Science & Business Media, 2006.

[131] Anil Jain, Karthik Nandakumar, and Arun Ross. Score normalization in multimodal biometric systems. *Pattern recognition*, 38(12):2270–2285, 2005.

[132] Anil K Jain, Karthik Nandakumar, and Arun Ross. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79:80–105, 2016.

[133] Anil K Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, and Arun Ross. Biometrics: a grand challenge. In *Proceedings of the 17th International Conference on Pattern Recognition (ICPR), 2004.*, volume 2, pages 935–942. IEEE, 2004.

[134] Anil K Jain and Arun Ross. Bridging the gap: from biometrics to forensics. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 370(1674):20140254, 2015.

[135] Anil K Jain, Arun A Ross, and Karthik Nandakumar. *Introduction to biometrics*. Springer Science & Business Media, 2011.

[136] Min-Soon Jang, Tea-Min Park, Jung-Kwon Lee, and Bo-Hyeun Wang. One grip based doorpull shaped doorlock system using fingerprint recognition and touch pattern. *Journal of Korean Institute of Intelligent Systems*, 26(1):30–36, 2016.

[137] Martin Janiak, Cathy Schaub, Don Lynam, Barry Howe, Greg Wachter, and Greg Krueger. Biometric authentication device for use with a personal digital assistant, May 11 2001. US Patent App. 09/854,078.

[138] Andrew H Johnston and Gary M Weiss. Smartwatch-based biometric gait recognition. In *Proceedings of the 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–6. IEEE, 2015.

[139] Juho Kannala and Esa Rahtu. Bsif: Binarized statistical image features. In *Proceedings of the 21st International Conference on Pattern Recognition (ICPR)*, pages 1363–1366. IEEE, 2012.

[140] Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, and George Samaras. Security and usability in knowledge-based user authentication: A review. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics*, page 63. ACM, 2016.

[141] Marisa Kendall. Uber slow to boot alleged drunken drivers off the app, state regulators say. https://www.mercurynews.com/2017/04/13/uber-slow-boot-alleged-drunk-drivers-off-app-state-regulators-say/, 2018 *(Accessed on 2020-07-28)*. Online web resource.

[142] Hassan Khan, Urs Hengartner, and Daniel Vogel. Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In *Proceedings of the SOUPS*, pages 225–239, 2015.

[143] Taewan Kim, Hyungsoo Park, Sang Hoon Hong, and Yunmo Chung. Integrated system of face recognition and sound localization for a smart door phone. *IEEE Transactions on consumer Electronics*, 59(3):598–603, 2013.

[144] Wonjun Kim, Sungjoo Suh, and Jae-Joon Han. Face liveness detection from a single image via diffusion speed model. *IEEE transactions on Image processing*, 24(8):2456–2465, 2015.

[145] Els J Kindt. *Privacy and data protection issues of biometric applications*, volume 1. Springer, 2016.

[146] Josef Kittler, Jiri Matas, Kenneth Jonsson, and MU Ramos Sánchez. Combining evidence in personal identity verification systems. *Pattern Recognition Letters*, 18(9):845–852, 1997.

[147] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2595–2604. ACM, 2011.

[148] Philip Koopman and Michael Wagner. Autonomous vehicle safety: An interdisciplinary challenge. *IEEE Intelligent Transportation Systems Magazine*, 9(1):90–96, 2017.

[149] J Koreman, AC Morris, D Wu, S Jassim, H Sellahewa, J Ehlers, G Chollet, G Aversano, H Bredin, S Garcia-Salicetti, et al. Multi-modal biometric authentication on the securephone pda. *ÉNS des Télécomm*, 2006.

[150] Steve Kovach. Business insider - samsung's galaxy s8 facial recognition feature can be fooled with a photo. *http://www.businessinsider.com/samsung-galaxy-s8-facial-recognition-tricked-with-a-photo-2017-3?IR=T*, 2017.

[151] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M Angela Sasse. ”they brought in the horrible key ring thing!” analysing the usability of two-factor authentication in uk online banking. *arXiv preprint arXiv:1501.04434*, 2015.

[152] Mohit Kumar, Aditya Insan, Norbert Stoll, Kerstin Thurow, and Regina Stoll. Stochastic fuzzy modeling for ear imaging based child identification. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 46(9):1265–1278, 2016.

[153] Ruggero Donida Labati, Angelo Genovese, Enrique Muñoz, Vincenzo Piuri, Fabio Scotti, and Gianluca Sforza. Biometric recognition in automated border control: a survey. *ACM Computing Surveys (CSUR)*, 49(2):24, 2016.

[154] Kenneth Lai, Shawn C Eastwood, Warren Adam Shier, Svetlana N Yanushkevich, and Vlad P Shmerko. Mass evidence accumulation and traveler risk scoring engine in e-border infrastructure. *IEEE Transactions on Intelligent Transportation Systems*, 2017.

[155] Shawn Langlois. Don't tip your uber driver? it could cost you a 5-star rating. https://www.marketwatch.com/story/dont-tip-your-uber-driver-it-could-cost-you-a-5-star-rating-2015-08-12, 2018 *(Accessed on 2020-07-28)*. Online web resource.

[156] James R Lewis and Jeff Sauro. Item benchmarks for the system usability scale. *Journal of Usability Studies*, 13(3):158–167, 2018.

[157] Lingjun Li, Xinxin Zhao, and Guoliang Xue. Unobservable re-authentication for smartphones. In *Proceedings of the NDSS*, volume 56, pages 57–59, 2013.

[158] Shancang Li and Li Da Xu. *Securing the internet of things*. Syngress, 2017.

[159] Zhen Ling, Kaizheng Liu, Yiling Xu, Chao Gao, Yier Jin, Cliff Zou, Xinwen Fu, and Wei Zhao. Iot security: an end-to-end view and case study. *arXiv preprint arXiv:1805.05853*, 2018.

[160] Jiajia Liu and Wen Sun. Smart attacks against intelligent wearables in people-centric internet of things. *IEEE Communications Magazine*, 54(12):44–49, 2016.

[161] Jorge de J Lozoya-Santos, Victorino Sepúlveda-Arróniz, Juan C Tudon-Martinez, and Ricardo A Ramirez-Mendoza. Survey on biometry for cognitive automotive systems. *Cognitive Systems Research*, 55:175–191, 2019.

[162] C Lupu and V Lupu. Multimodal biometrics for access control in an intelligent car. In *Proceedings of International Symposium on Computational Intelligence and Intelligent Informatics*, pages 261–267. IEEE, 2007.

[163] Shuangge Ma and Jian Huang. Penalized feature selection and classification in bioinformatics. *Briefings in bioinformatics*, 9(5):392–403, 2008.

[164] Winston Ma. *China's mobile economy: opportunities in the largest and fastest information consumption boom*. John Wiley & Sons, 2016.

[165] Upal Mahbub, Sayantan Sarkar, Vishal M Patel, and Rama Chellappa. Active user authentication for smartphones: A challenge data set and benchmark results. In *Proceedings of the 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–8. IEEE, 2016.

[166] Jani Mantyjarvi, Mikko Lindholm, Elena Vildjiounaite, S-M Makela, and HA Ailisto. Identifying users of portable devices from gait pattern with accelerometers. In *Proceedings of the International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, volume 2, pages ii–973. IEEE, 2005.

[167] Sébastien Marcel, Mark S Nixon, and Stan Z Li. Handbook of biometric anti-spoofing-trusted biometrics under spoofing attacks, ser. *Advances in Computer Vision and Pattern Recognition. Springer*, 2014.

[168] Matlab. Classification learner app. https://in.mathworks.com/help/stats/classification-learner-app.html, 2018 *(Accessed on 2020-07-28)*. Online web resource.

[169] Matlab. Relieff feature selection method. https://www.mathworks.com/help/stats/relieff.html, 2019 *(Accessed on 2020-07-28)*. Online web resource.

[170] Liam M Mayron. Behavioral biometrics for universal access and authentication. In *Proceedings of the International Conference on Universal Access in Human-Computer Interaction*, pages 330–339. Springer, 2015.

[171] Christopher McCool, Sebastien Marcel, Abdenour Hadid, Matti Pietikäinen, Pavel Matejka, Jan Cernockỳ, Norman Poh, Josef Kittler, Anthony Larcher, Christophe Levy, et al. Bi-modal person recognition on a mobile phone: using mobile phone data. In *Proceedings of the International Conference on Multimedia and Expo Workshops (ICMEW)*, pages 635–640. IEEE, 2012.

[172] Cara McGoogan and Danielle Demetriou. The telegraph - peace sign selfies could let hackers copy your fingerprints. http://www.telegraph.co.uk/technology/2017/01/12/peace-sign-selfies-could-let-hackers-copy-fingerprints, 2017 *(Accessed on 2020-07-28)*. online web resource.

[173] Mary Meeker. Internet trends: 2019. https://www.bondcap.com/pdf/Internet_Trends_2019.pdf, 2019 *(Accessed on 2020-07-28)*. online web resource.

[174] Maryam Mehrnezhad, Ehsan Toreini, Siamak F Shahandashti, and Feng Hao. Stealing pins via mobile sensors: actual risk versus user perception. *International Journal of Information Security*, pages 1–23, 2016.

[175] Weizhi Meng, Duncan S Wong, Steven Furnell, and Jianying Zhou. Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials*, 17(3):1268–1293, 2015.

[176] Yuxin Meng, Duncan S Wong, Roman Schlegel, et al. Touch gestures based biometric authentication scheme for touchscreen mobile phones. In *Proceedings of the International Conference on Information Security and Cryptology*, pages 331–350. Springer, 2012.

[177] L Mezai, F Hachouf, and M Bengherabi. Fusion of face and voice using the dempster-shafer theory for person verification. In *Processings of the 7^{th} International Workshop on Systems, Signal Processing and their Applications (WOSSPA)*, pages 103–106. IEEE, 2011.

[178] Lamia Mezai and Fella Hachouf. Score-level fusion of face and voice using particle swarm optimization and belief functions. *IEEE Transactions on Human-Machine Systems*, 45(6):761–772, 2015.

[179] Microsoft. Key principles of software architecture. https://msdn.microsoft.com/en-us/library/ee658124.aspx, 2018 *(Accessed on 2020-07-28)*. online web resource.

[180] Akmal Mirsadikov, Andrew Harrison, and Brian Mennecke. Tales from the wheel: An it-fueled ride as an uber driver. In *Proceedings of the 22nd Americas Conference on Information Systems*. AMCIS, 2016.

[181] Luis Carlos Molina, Lluís Belanche, and Àngela Nebot. Feature selection algorithms: A survey and experimental evaluation. In *Proceedings of the International Conference on Data Mining, ICDM*, pages 306–313. IEEE, 2002.

[182] Youngme Moon. Uber: changing the way the world moves. *Case, Harvard Business School*, 101(9-316), 2015.

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

[184] Kazuya Murao, Hayami Tobise, Tsutomu Terada, Toshiki Iso, Masahiko Tsukamoto, and Tsutomu Horikoshi. Mobile phone user authentication with grip gestures using pressure sensors. *International Journal of Pervasive Computing and Communications*, 11(3):288–301, 2015.

[185] Alvaro Muro-De-La-Herran, Begonya Garcia-Zapirain, and Amaia Mendez-Zorrilla. Gait analysis methods: An overview of wearable and non-wearable systems, highlighting clinical applications. *Sensors*, 14(2):3362–3394, 2014.

[186] Sumita Nainan, Akshay Ramesh, Vipul Gohil, and Jaykumar Chaudhary. Speech controlled automobile with three-level biometric security system. In *Proceedings of the International Conference on Computing, Communication, Control and Automation (ICCUBEA)*, pages 1–6. IEEE, 2017.

[187] Tempestt J Neal and Damon L Woodard. Surveying biometric authentication for mobile device security. *Journal of Pattern Recognition Research*, 1:74–110, 2016.

[188] Toan Van Nguyen, Napa Sae-Bae, and Nasir Memon. Draw-a-pin. *Computers and Security*, 66(C):115–128, 2017.

[189] NuData-Security. What is risk based authentication? https://nudatasecurity.com/blog/ecommerce/what-is-risk-based-authentication/, 2020 *(Accessed on 2020-07-28)*. online web resource.

[190] Mohammad S Obaidat, Issa Traore, and Isaac Woungang. *Biometric-Based Physical and Cybersecurity Systems*. Springer, 2019.

[191] Barclay Osborn, Justin McWilliams, Betsy Beyer, and Max Saltonstall. Beyondcorp: Design to deployment at google. In *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation*, 2016.

[192] PandaSecurities. No password? you're asking to be hacked. https://www.pandasecurity.com/mediacenter/tips/smartphone-risk-dont-use-password, 2016 *(Accessed on 2020-07-28)*. online web resource.

[193] Keyurkumar Patel, Hu Han, and Anil K Jain. Secure face unlock: Spoof detection on smartphones. *IEEE transactions on information forensics and security*, 11(10):2268–2283, 2016.

[194] Vishal M Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, 33(4):49–61, 2016.

[195] Vishal M Patel, Nalini K Ratha, and Rama Chellappa. Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5):54–65, 2015.

[196] Padma Polash Paul, Marina L Gavrilova, and Reda Alhajj. Decision fusion for multimodal biometrics using social network analysis. *IEEE transactions on systems, man, and cybernetics: systems*, 44(11):1522–1533, 2014.

[197] Mahesh R Pawar and Imdad Rizvi. Face authentication and iot-based automobile security and driver surveillance system. In *Proceeding of the International Conference on ISMAC in Computational Vision and Bio-Engineering*, pages 679–686. Springer, 2018.

[198] Ivan Pires, Nuno Garcia, Nuno Pombo, and Francisco Flórez-Revuelta. From data acquisition to data fusion: a comprehensive review and a roadmap for the identification of activities of daily living using mobile devices. *Sensors*, 16(2):184, 2016.

[199] Norman Poh and Jerzy Korczak. Hybrid biometric person authentication using face and voice features. In *Proceedings of the AVBPA*, volume 1, pages 348–353. Springer, 2001.

[200] Pomemom. The 2019 state of password and authentication security behaviors report. https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Authentication-Report.pdf?source=pepperjam&publisherId=96525&clickId=3212951265&utm_source=pepperjam&utm_medium=affiliate&utm_campaign=96525, 2019 *(Accessed on 2020-07-28)*. online web resource.

[201] Fabienne Porée, Johnny Mariéthoz, Samy Bengio, and Frédéric Bimbot. The banca database and experimental protocol for speaker verification. Technical report, IDIAP, 2002.

[202] Davy Preuveneers and Wouter Joosen. Smartauth: dynamic context fingerprinting for continuous user authentication. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, pages 2185–2191. ACM, 2015.

[203] OWASP Mobile Security Project. Owasp mobile security project. https://owasp.org/www-project-mobile-security/, 2020 *(Accessed on 2020-07-28)*. online web resource.

[204] The Pros and Cons Of Fingerprinting Uber Drivers. Maurice emsellem. https://www.huffingtonpost.com/maurice-emsellem/fingerprinting-uber-drivers_b_10972428.html, 2017 *(Accessed on 2020-07-28)*. Online web resource.

[205] PRTools. Fisher's least square linear discriminant. http://www.37steps.com/prhtml/prtools/fisherc.html, 2019 *(Accessed on 2020-07-28)*. Online web resource.

[206] PRTools. Stats support vector classifier. http://www.37steps.com/prhtml/prtools/statssvc.html, 2019 *(Accessed on 2020-07-28)*. Online web resource.

[207] Kritika Puri and Sanjay Kumar Dubey. Analytical and critical approach for usability measurement method. In *Proceedings of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 4045–4050. IEEE, 2016.

[208] Jamal Raiyn. Data and cyber security in autonomous vehicle networks. *Transport and Telecommunication Journal*, 19(4):325–334, 2018.

[209] Raghavendra Ramachandra and Christoph Busch. Presentation attack detection methods for face recognition systems: a comprehensive survey. *ACM Computing Surveys (CSUR)*, 50(1):8, 2017.

[210] Partha Pratim Ray. A survey on internet of things architectures. *Journal of King Saud University-Computer and Information Sciences*, 30(3):291–319, 2018.

[211] Xuguang Ren and Xin-Wen Wu. A novel dynamic user authentication scheme. In *Proceedings of International Symposium on Communications and Information Technologies (ISCIT)*, pages 713–717. IEEE, 2012.

[212] Rene Ritchie, Daniel Rubino, Kevin Michaluk, and Phil Nickinson. The future of authentication: Biometrics, multi-factor, and co-dependency. https://www.androidcentral.com/talk-mobile/future-authentication-biometrics-multi-factor-and-co-dependency-talk-mobile, 2013 *(Accessed on 2020-07-28)*. online web resource.

[213] Nils Rogmann and Maximilian Krieg. Liveness detection in biometrics. In *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–14. IEEE, 2015.

[214] Arun A Ross, Anil K Jain, and Karthik Nandakumar. Information fusion in biometrics. *Handbook of Multibiometrics*, pages 37–58, 2006.

[215] Joseph Roth, Xiaoming Liu, Arun Ross, and Dimitris Metaxas. Biometric authentication via keystroke sound. In *Proceedings of the International Conference on Biometrics (ICB)*, pages 1–8. IEEE, 2013.

[216] RSA. Rsa adaptive authentication system. https://www.rsa.com/content/dam/rsa/PDF/h9096-rsa-risk-engine-sb-11-2.pdf, 2017 *(Accessed on 2020-07-28)*. online web resource.

[217] Zhang Rui and Zheng Yan. A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE Access*, 7:5994–6009, 2019.

[218] Nelson Sabater. *Biometrics as Password Alternative*. PhD thesis, Utica College, 2019.

[219] Napa Sae-Bae, Nasir Memon, Katherine Isbister, and Kowsar Ahmed. Multitouch gesture-based authentication. *IEEE transactions on information forensics and security*, 9(4):568–582, 2014.

[220] Hataichanok Saevanee, Nathan Clarke, and Steven Furnell. Multi-modal behavioural biometric authentication for mobile devices. *Information Security and Privacy Research*, pages 465–474, 2012.

[221] Hataichanok Saevanee, Nathan Clarke, Steven Furnell, and Valerio Biscione. Continuous user authentication using multi-modal biometrics. *Computers & Security*, 53:234–246, 2015.

[222] Alex Salazar. Sso vs. centralized authentication. https://stormpath.com/blog/sso-vs-centralized-auth, 2014 *(Accessed on 2020-07-28)*. online web resource.

[223] Allen Sarkisyan, Ryan Debbiny, and Ani Nahapetian. Wristsnoop: Smartphone pins prediction using smartwatch motion sensors. In *Proceedings of International Workshop on Information Forensics and Security (WIFS)*, pages 1–6. IEEE, 2015.

[224] Pablo Sauras-Perez, Andrea Gil, Jasprit Singh Gill, Pierluigi Pisu, and Joachim Taiber. Voge: A voice and gesture system for interacting with autonomous cars. Technical report, SAE Technical Paper, 2017.

[225] Jeff Sauro. Measuring usability with the system usability scale (sus), 2011.

[226] Bruce Schneier. Risk-based authentication. https://www.schneier.com/blog/archives/2013/11/risk-based_auth.html, 2013 *(Accessed on 2020-07-28)*. online web resource.

[227] SecureGroup. Lock pattern, pin, or password: What is the most reliable way to lock a phone. https://blog.securegroup.com/lock-pattern-pin-or-password-what-is-the-most-reliable-way-to-lock-a-phone, 2017 *(Accessed on 2020-07-28)*. online web resource.

[228] Mariusz Sepczuk and Zbigniew Kotulski. A new risk-based authentication management model oriented on user's experience. *Computers & Security*, 73:17–33, 2018.

[229] Dilip Kumar Sharma, Neeraj Baghel, and Siddhant Agarwal. Multiple degree authentication in sensible homes basedon iot device vulnerability. In *Proceedings of the International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, pages 539–543. IEEE, 2020.

[230] Weidong Shi, Jun Yang, Yifei Jiang, Feng Yang, and Yingen Xiong. Senguard: Passive user identification on smartphones using multiple sensors. In *Proceedings of the 7^{th} International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 141–148. IEEE, 2011.

[231] Devu Manikantan Shila and Kunal Srivastava. Castra: Seamless and unobtrusive authentication of users to diverse mobile services. *IEEE Internet of Things Journal*, 5(5):4042–4057, 2018.

[232] David Silver, Suman Jana, Dan Boneh, Eric Yawei Chen, and Collin Jackson. Password managers: Attacks and defenses. In *Proceedings of the USENIX Security Symposium*, pages 449–464, 2014.

[233] Zdeňka Sitová, Jaroslav Šeděnka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, and Kiran S Balagani. Hmog: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security*, 11(5):877–892, 2016.

[234] Mohamed Soltane, Noureddine Doghmane, and Noureddine Guersi. Face and speech based multi-modal biometric authentication. *International Journal of Advanced Science and Technology*, 21(6):41–56, 2010.

[235] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. Eyeveri: A secure and usable approach for smartphone user authentication. In *Proceedings of the the 35^{th} Annual IEEE International Conference on Computer Communications, IEEE INFOCOM 2016*, pages 1–9. IEEE, 2016.

[236] Rick Spencer. The streamlined cognitive walkthrough method, working around social constraints encountered in a software development company. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 353–359. ACM, 2000.

[237] Mark Stanislav. *Two-factor authentication*. IT Governance Ltd, 2015.

[238] Statista. What authentication methods do you usually use when logging in to your main bank? https://www.statista.com/statistics/786638/online-banking-authentication-security-methods-usage-united-kingdom/, 2018 *(Accessed on 2020-07-28)*. online web resource.

[239] Ariel Stolerman, Alex Fridman, Rachel Greenstadt, Patrick Brennan, and Patrick Juola. Active linguistic authentication revisited: Real-time stylometric evaluation towards multimodal decision fusion. In *Proceedings of the IFIP WG*, volume 11, pages 1–11, 2014.

[240] Paul Strohmeier, Cedric Honnet, and Samppa Von Cyborg. Developing an ecosystem for interactive electronic implants. In *Proceedings of the Conference on Biomimetic and Biohybrid Systems*, pages 518–525. Springer, 2016.

[241] Madeena Sultana, Marina Gavrilova, and Svetlana Yanushkevich. Multi-resolution fusion of dtcwt and dct for shift invariant face recognition. In *Proceedings of the International Conference on Systems, Man and Cybernetics (SMC)*, pages 80–85. IEEE, 2014.

[242] Madeena Sultana, Padma Polash Paul, and Marina L Gavrilova. Social behavioral information fusion in multimodal biometrics. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2017.

[243] He Sun, Kun Sun, Yuewu Wang, and Jiwu Jing. Trustotp: Transforming smartphones into secure one-time password tokens. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 976–988. ACM, 2015.

[244] Xiaoyuan Suo, Ying Zhu, and G Scott Owen. Graphical passwords: A survey. In *Proceedings of the 21st annual Computer security applications conference*, pages 10–pp. IEEE, 2005.

[245] Sowmya Nagasimha Swamy, Dipti Jadhav, and Nikita Kulkarni. Security threats in the application layer in iot applications. In *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pages 477–480. IEEE, 2017.

[246] Yujin Tang, Nakazato Hidenori, and Yoshiyori Urano. User authentication on smart phones using a data mining method. In *Proceedings of the International Conference on Information Society (i-Society)*, pages 173–178. IEEE, 2010.

[247] Furkan Tari, Ant Ozok, and Stephen H Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the 2nd symposium on Usable privacy and security*, pages 56–66. ACM, 2006.

[248] Techtarget. bespoke. http://whatis.techtarget.com/definition/bespoke, 2017 *(Accessed on 2020-07-28)*. online web resource.

[249] Tesla. Future of driving. https://www.tesla.com/autopilot, 2019. Online web resource.

[250] IBM *(Accessed on 2020-07-28)*. Ibm tivoli federated identity manager. https://www.ibm.com/developerworks/tivoli/library/t-tfim-info/index.html, 2016 *(Accessed on 2020-07-28)*. online web resource.

[251] Julie Katherine Thorpe. *On the predictability and security of user choice in passwords*. Carleton University, 2008.

[252] James Titcomb. Hackers claim to beat iphone x's face id in one week with £115 mask. http://www.telegraph.co.uk/technology/2017/11/13/hackers-beat-iphone-xs-face-one-week-115-mask/, 2017 *(Accessed on 2020-07-28)*. online web resource.

[253] Christina-Angeliki Toli and Bart Preneel. Privacy-preserving biometric authentication model for e-finance applications. In *Proceedings of the ICISSP*, pages 353–360, 2018.

[254] Ruben Tolosana, Ruben Vera-Rodriguez, Richard Guest, Julian Fierrez, and Javier Ortega-Garcia. Exploiting complexity in pen-and touch-based signature biometrics. *arXiv preprint arXiv:1905.03676*, 2019.

[255] Issa Traoré and Ahmed Awad E Ahmed. Introduction to continuous authentication. *Continuous Authentication Using Biometrics: Data, Models, and Metrics: Data, Models, and Metrics*, page 1, 2011.

[256] Issa Traore, Isaac Woungang, Mohammad S Obaidat, Youssef Nakkabi, and Iris Lai. Online risk-based authentication using behavioral biometrics. *Multimedia tools and applications*, 71(2):575–605, 2014.

[257] Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference*, pages 159–168. ACM, 2012.

[258] Michal Trnka, Tomas Cerny, and Nathaniel Stickney. Survey of authentication and authorization for the internet of things. *Security and Communication Networks*, 2018, 2018.

[259] Uber. Always the ride you want. https://www.uber.com/us/en/ride/, 2018 *(Accessed on 2020-07-28)*. Online web resource.

[260] Uber. Engineering safety with uber's real-time id check. https://eng.uber.com/real-time-id-check/, 2018 *(Accessed on 2020-07-28)*. Online web resource.

[261] Uber. How to become an uber driver. https://www.uber.com/in/en/drive/requirements/, 2018 *(Accessed on 2020-07-28)*. Online web resource.

[262] Uber. What does the background check include? https://help.uber.com/driving-and-delivering/article/what-does-the-background-check-look-for?nodeId=ee210269-89bf-4bd9-87f6-43471300ebf2, 2018 *(Accessed on 2020-07-28)*. Online web resource.

[263] Ryan J Urbanowicz, Melissa Meeker, William LaCava, Randal S Olson, and Jason H Moore. Relief-based feature selection: introduction and review. *Journal of Biomedical Informatics*, 85:189–203, 2018.

[264] Pascal Urien and Selwyn Piramuthu. Framework and authentication protocols for smartphone, nfc, and rfid in retail transactions. In *Proceedings of the 8th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2013*, pages 77–82. IEEE, 2013.

[265] Usability. System usability scale (sus). https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html, 2020 *(Accessed on 2020-07-28)*. online web resource.

[266] USAtoday. I got taken for a ride by a fake uber driver. don't become the next victim. https://www.usatoday.com/story/tech/columnist/stevenpetrow/2016/10/12/fake-uber-drivers-dont-become-next-victim/91903508/, 2016 *(Accessed on 2020-07-28)*. Online web resource.

[267] Rubén Vera-Rodríguez, John SD Mason, Julián Fiérrez, and Javier Ortega-García. Analysis of spatial domain information for footstep recognition. *IET computer vision*, 5(6):380–388, 2011.

[268] Ruben Vera-Rodriguez, John SD Mason, Julian Fierrez, and Javier Ortega-Garcia. Comparative analysis and fusion of spatiotemporal information for footstep recognition. *IEEE transactions on pattern analysis and machine intelligence*, 35(4):823–834, 2013.

[269] Verizon. Data breach investigations report. https://enterprise.verizon.com/resources/reports/dbir/, 2019 *(Accessed on 2020-07-28)*. online web resource.

[270] VMware. Vmware identity manager documentation center. https://pubs.vmware.com/identity-manager-27/index.jsp, 2017. online web resource.

[271] Su Wang, Roland Hu, Huimin Yu, Xia Zheng, Robert I Damper, et al. Augmenting remote multimodal person verification by embedding voice characteristics into face images. In *Proceedings of the International conference on multimedia and expo workshops (ICMEW)*, pages 1–6. IEEE, 2013.

[272] David G Warnock and Carl C Peck. A roadmap for biomarker qualification. *Nature biotechnology*, 28(5):444–445, 2010.

[273] Whosdrivingyou. Fake uber drivers pose real threat. https://www.whosdrivingyou.org/blog/fake-uber-drivers-pose-real-threat, 2017 *(Accessed on 2020-07-28)*. Online web resource.

[274] Whosdrivingyou. Reported list of incidents involving uber and lyft. http://www.whosdrivingyou.org/rideshare-incidents, 2018 *(Accessed on 2020-07-28)*. Online web resource.

[275] Michael Winnick. Putting a finger on our phone obsession, 2016 *(Accessed on 2020-07-28)*. online web resource.

[276] Ian H Witten, Eibe Frank, Mark A Hall, and Christopher J Pal. *Data Mining: Practical machine learning tools and techniques*. Morgan Kaufmann, 2016.

[277] Teresa Wu, Jennifer Blackhurst, and Vellayappan Chidambaram. A model for inbound supply risk analysis. *Computers in industry*, 57(4):350–365, 2006.

[278] Hui Xu, Yangfan Zhou, and Michael R Lyu. Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. In *Proceedings of Symposium On Usable Privacy and Security, SOUPS*, volume 14568–582, pages 187–198, 2014.

[279] Yong Xu, Xiaozhao Fang, Xuelong Li, Jiang Yang, Jane You, Hong Liu, and Shaohua Teng. Data uncertainty in face recognition. *IEEE transactions on cybernetics*, 44(10):1950–1961, 2014.

[280] Junshuang Yang, Yanyan Li, and Mengjun Xie. Motionauth: Motion-based authentication for wrist worn smart devices. In *Proceedings of the International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 550–555. IEEE, 2015.

[281] Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Kwang In Kim, Ben Taylor, and Zheng Wang. Cracking android pattern lock in five attempts. *Proceedings of the Network and Distributed System Security Symposium (NDSS'17)*, 2017.

[282] Ka-Ping Yee. User interaction design for secure systems. *Information and Communications Security*, pages 278–290, 2002.

[283] Jie Zhang, Xin Luo, Somasheker Akkaladevi, and Jennifer Ziegelmayer. Improving multiple-password recall: an empirical study. *European Journal of Information Systems*, 18(2):165–176, 2009.

[284] Linghan Zhang, Sheng Tan, and Jie Yang. Hearing your voice is not enough: An articulatory gesture based liveness detection for voice authentication. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pages 57–71. ACM, 2017.

[285] Linghan Zhang, Sheng Tan, Jie Yang, and Yingying Chen. Voicelive: A phoneme localization based liveness detection for voice authentication on smartphones. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pages 1080–1091. ACM, 2016.

[286] Leah Zhang-Kennedy, Sonia Chiasson, and Paul van Oorschot. Revisiting password rules: facilitating human management of passwords. In *Proceedings of APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–10. IEEE, 2016.

[287] Nan Zheng, Kun Bai, Hai Huang, and Haining Wang. You are how you touch: User verification on smartphones via tapping behaviors. In *Proceedings of the 22nd International Conference on Network Protocols (ICNP), 2014, IEEE*, pages 221–232. IEEE, 2014.

[288] Bo Zhou, Monit Shah Singh, Sugandha Doda, Muhammet Yildirim, Jingyuan Cheng, and Paul Lukowicz. The carpet knows: Identifying people in a smart environment from a single step. In *Proceedings of the International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 527–532. IEEE, 2017.

[289] Jiang Zhu, Pang Wu, Xiao Wang, and Joy Zhang. Sensec: Mobile security through passive sensing. In *Proceedings of the International Conference on Computing, Networking and Communications (ICNC)*, pages 1128–1133. IEEE, 2013.

[290] Zhaoxia Zhu and Fulong Chen. Fingerprint recognition-based access controlling system for automobiles. In *Proceedings of the 4th International Congress on Image and Signal Processing*, volume 4, pages 1899–1902. IEEE, 2011.

[291] Zhen Zhu, Ren-Gen Huang, et al. Study on the iot architecture and access technology. In *Proceedings of the 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES)*, pages 113–116. IEEE, 2017.

[292] Thomas Zink and Marcel Waldvogel. X. 509 user certificate-based two-factor authentication for web applications. In *Proceedings of the 10th DFN-Forum Kommunikationstechnologien*, pages 51–61, 2017.

Appendix A

Hold & Tap: Demographic Survey Questionnaire

1. What is your gender?
    - Male
    - Female
    - I don't want to disclose
2. How old you are?
    - $\leq$ than 20 years.
    - >20 years and ≤ 40 years.
    - >40 years and ≤ 60 years.
    - $>$ than 60 years.
    - I don't want to disclose
3. Tell us about your nationality.
    - ________________
    - I don't want to disclose
4. Which hand(s) do you use for interacting with your smartphone?

- Right
- Left
- Both
- I don’t want to disclose

Appendix B

Step & Turn: Generic Survey Questionnaire

1. I think I can provide training samples between

   - 1 to 5
   - 5 to 10
   - 10 to 40
   - 40 to 100
   - More than 100

2. Please select your age category

   - 16 years and below
   - 17 - 25 years
   - 26 - 35 years
   - 36 - 45 years
   - 46 - 60 years
   - 60 years and above

3. Please select your gender

- Female
- Male
- Prefer not to say

Appendix C

RiderAuth Survey Questionnaire

1. I think rider authentication is essential for driverless taxis for their customers' security.
   - Strongly agree
   - Agree
   - Neutral
   - Disagree
   - Strongly disagree
2. I think I am aware of biometric-based authentication schemes?
   - Yes
   - No
3. I would rate my knowledge of biometrics as
   - Excellent
   - Good
   - Fair
   - Negligible

4. I am using biometric-based authentication schemes on smart devices?
    - Yes
    - No

5. I think I prefer to use biometrics over PIN/Password-based schemes for authentication purposes.
    - Yes
    - No

6. I think I prefer to use biometrics over smart cards for authentication purposes.
    - Yes
    - No

7. I think I can use my physiological biometric characteristics for authentication purposes
    - Yes
    - No

8. I think I am willing to use my fingerprints for authentication purposes.
    - Strongly agree
    - Agree
    - Neutral
    - Disagree
    - Strongly disagree

9. I think I am willing to use my face for authentication purposes.
    - Strongly agree
    - Agree
    - Neutral
    - Disagree
    - Strongly disagree

10. I think I am willing to use my iris/retina for authentication purposes.
    - Strongly agree
    - Agree
    - Neutral
    - Disagree
    - Strongly disagree

11. I think I can use my behavioral biometric characteristics for authentication purposes
    - Yes
    - No

12. I think I am willing to use my voice for authentication purposes.
    - Strongly agree
    - Agree
    - Neutral
    - Disagree
    - Strongly disagree

13. I think I am willing to use my handwritten signatures for authentication purposes.
    - Strongly agree
    - Agree
    - Neutral
    - Disagree
    - Strongly disagree

14. I think I am willing to use my keystroke/touch dynamics for authentication purposes.
    - Strongly agree
    - Agree
    - Neutral
    - Disagree
    - Strongly disagree

15. I think I am willing to use my gait for authentication purposes.
    - Strongly agree
    - Agree
    - Neutral
    - Disagree
    - Strongly disagree

16. I think I am willing to use my hand-movements to hold or wear smart devices for authentication purposes.

- Strongly agree
- Agree
- Neutral
- Disagree
- Strongly disagree

17. I think I can provide training samples between

    - 1 to 5
    - 5 to 10
    - 10 to 30
    - 30 to 100
    - More than 100

18. Please select your age category

    - 16 years and below
    - 17 - 25 years
    - 26 - 35 years
    - 36 - 45 years
    - 46 - 60 years
    - 60 years and above

19. Please select your gender

    - Female
    - Male
    - Prefer not to say

20. Please select the continent where you are residing at present?

    - Africa
    - Asia
    - Australia
    - Europe
    - North America
    - South America