UNIVERSITY OF THE AEGEAN

School of Engineering

Department of Information & Communication Systems Engineering

Karlovassi, Samos

Greece

Doctoral Dissertation

Συμπεριφορικές Βιομετρικές Μέθοδοι για Συνεχή Αυθεντικοποίηση: Ζητήματα ασφάλειας και ιδιωτικότητας (Behavioral Biometrics for Continuous Authentication: Security and Privacy Issues).

by

Ioannis Stylios

January 2023

Υπεύθυνη δήλωση

Είμαι ο αποκλειστικός συγγραφέας της υποβληθείσας Διδακτορικής Διατριβής με τίτλο «Συμπεριφορικές Βιομετρικές Μέθοδοι για Συνεχή Αυθεντικοποίηση: Ζητήματα ασφάλειας και ιδιωτικότητας (Behavioral Biometrics for Continuous Authentication: Security and Privacy Issues». Η συγκεκριμένη Διδακτορική Διατριβή είναι πρωτότυπη και εκπονήθηκε αποκλειστικά για την απόκτηση του Διδακτορικού διπλώματος του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων. Κάθε βοήθεια, την οποία είχα για την προετοιμασία της, αναγνωρίζεται πλήρως και αναφέρεται επακριβώς στην εργασία. Επίσης, επακριβώς αναφέρω στην εργασία τις πηγές, τις οποίες χρησιμοποίησα, και μνημονεύω επώνυμα τα δεδομένα ή τις ιδέες που αποτελούν προϊόν πνευματικής ιδιοκτησίας άλλων, ακόμη κι εάν η συμπερίληψή τους στην παρούσα εργασία υπήρξε έμμεση ή παραφρασμένη. Γενικότερα, βεβαιώνω ότι κατά την εκπόνηση της Διδακτορικής Διατριβής έχω τηρήσει απαρέγκλιτα όσα ο νόμος ορίζει περί διανοητικής ιδιοκτησίας και έχω συμμορφωθεί πλήρως με τα προβλεπόμενα στο νόμο περί προστασίας προσωπικών δεδομένων και τις αρχές Ακαδημαϊκής Δεοντολογίας.

Advising Committee

Spyros Kokolakis, Professor, Supervisor
Department of Information & Communication Systems Engineering
University of the Aegean

Sotirios Chatzis, Associate Professor, Advisor
Cyprus University of Technology

Panagiotis Rizomiliotis, Assistant Professor, Advisor
Department of Informatics and Telematics
Harokopio University, Greece

Examining Committee

Spyros Kokolakis, Professor, Supervisor
Department of Information & Communication Systems Engineering
University of the Aegean

Sotirios Chatzis, Associate Professor, Advisor
Department of Electrical Engineering, Computer
Engineering and Informatics
Cyprus University of Technology

Panagiotis Rizomiliotis, Assistant Professor, Advisor
Department of Informatics and Telematics
Harokopio University

Stefanos Gritzalis Professor, Member
Department of Digital Systems,
University of Piraeus

Georgios Kampourakis, Professor, Member
Department of Information & Communication Systems Engineering
University of the Aegean

Christos Kalloniatis, Associate Professor, Member
Department of Cultural Technology and Communication,
University of the Aegean

Kostoulas Theodoros, Associate Professor, Member
Department of Information & Communication Systems Engineering
University of the Aegean

Acknowledgements

This research has been financially supported by the General Secretariat for Research and Technology (GSRT) and the Hellenic Foundation for Research and Innovation (HFRI) (Scholarship Code: 13).

Contents

Table of Figures

List of Tables

Περίληψη

Τα συστήματα ελέγχου ταυτότητας που βασίζονται σε PINs και κωδικούς πρόσβασης ή σε φυσιολογικά βιομετρικά (π.χ. ίριδα ματιού, δακτυλικό αποτύπωμα, κ.α.) χρησιμοποιούν το μοντέλο αυθεντικοποίησης στο σημείου εισόδου (entry-point authentication model). Το μοντέλο αυτό έχει επικριθεί έντονα επειδή είναι ευάλωτο σε επιθέσεις που συμβαίνουν μετά την αρχική αυθεντικοποίηση. Ορισμένα από τα εν λόγω συστήματα αμύνονται έναντι τέτοιων επιθέσεων εκτελώντας ένα πρόσθετο βήμα ελέγχου ταυτότητας σε κρίσιμα σημεία της συνεδρίας αλλά δεν είναι δημοφιλή στους χρήστες λόγω της επαναλαμβανόμενης αυθεντικοποίησης (repetitive authentication).

Οι κινητές συσκευές και οι εφαρμογές τους χρησιμοποιούν το μοντέλο αυθεντικοποίησης στο σημείου εισόδου για τον έλεγχο της ταυτότητας των χρηστών. Ένα σημαντικό μέλημα οπότε είναι να καθοριστεί εάν η κινητή συσκευή βρίσκεται στα χέρια του γνήσιου χρήστη (genuine user) και, αντίστοιχα, εάν ο γνήσιος χρήστης είναι αυτός που χρησιμοποιεί τις ευαίσθητες υπηρεσίες κατά τη διάρκεια μιας συνεδρίας. Προς επίλυση αυτού του ζητήματος έχουν προταθεί στη βιβλιογραφία τα συστήματα Συνεχούς Αυθεντικοποίησης (Continuous Authentication – CA) με χρήση Συμπεριφορικών Βιομετρικών (Behavioral Biometrics – BB). Τα CA συστήματα αποτελούν ένα πρόσθετο μέτρο ασφαλείας που παρακολουθεί τη βιομετρική συμπεριφορά των χρηστών επαναπροσδιορίζοντας συνεχώς την ταυτότητα τους κατά τη διάρκεια μιας περιόδου σύνδεσης. Η πρακτική εφαρμογή τους είναι όμως περιορισμένης έκτασης λόγω δυο θεμελιωδών ελλείψεων. Η πρώτη έλλειψη εστιάζεται σε μη τεχνικά ζητήματα, όπως για παράδειγμα, σε αντιλήψεις σχετικές με τους φόβους και τις προσδοκίες των μελλοντικών χρηστών και σε αντιλαμβανόμενες ανησυχίες για την ιδιωτικότητα των βιομετρικών τους. Η δεύτερη έλλειψη εστιάζεται στο πρόβλημα των ψευδώς θετικών/ψευδώς αρνητικών αποτελεσμάτων, δηλαδή, σε ζητήματα ασφάλειας (security) και ευχρηστίας (usability).

Η παρούσα διδακτορική διατριβή περιλαμβάνει τέσσερα ερευνητικά στάδια. Πρόκειται για ερευνητικά στάδια ενός ενιαίου ερευνητικού έργου. Στο πρώτο ερευνητικό στάδιο παρουσιάζεται μια εκτεταμένη βιβλιογραφική ανασκόπηση που χαρτογραφεί την περιοχή της

έρευνας και αφορά στην τεχνολογία BBCA και την απόδοση των συστημάτων μηχανικής μάθησης. Επιπλέον, παρουσιάζεται μια βιβλιογραφική ανασκόπηση σχετική με τους πιθανούς φορείς επίθεσης στα συστήματα BBCA και επισημαίνονται πολλά υποσχόμενα αντίμετρα. Επίσης, πραγματοποιείται μια ταξινόμηση των συμπεριφορικών βιομετρικών (Behavioral Biometrics - BB) σε επτά κατηγορίες και μια ανάλυση των μεθοδολογιών της συλλογής και εξαγωγής των χαρακτηριστικών (feature extraction) τους. Τέλος, εντοπίζονται οι προκλήσεις, τα ανοιχτά προβλήματα και οι μελλοντικές τάσεις.

Στο δεύτερο ερευνητικό στάδιο της παρούσας διατριβής, διερευνάται η επίδραση διαφόρων παραγόντων συμπεριφορικής πρόθεσης υιοθέτησης της τεχνολογίας (Behavioral Intention – BI) μέσω μιας νέας ενσωμάτωσης του Μοντέλου Αποδοχής Τεχνολογίας (Technology Acceptance Model - TAM) και της Θεωρίας Διάχυσης Καινοτομίας (Diffusion of Innovation Theory - DOI). Επίσης, αναπτύσσεται ένα νέο θεωρητικό πλαίσιο με δομές όπως Κίνδυνοι Ασφάλειας & Προστασίας Προσωπικών Δεδομένων (Security & Privacy Risks - SPR), Ανησυχίες Ιδιωτικότητας των Βιομετρικών (Biometrics Privacy Concerns - BPC) και Αντιλαμβανόμενος Κίνδυνος Χρήσης της Τεχνολογίας (Perceived Risk Of Using the technology - PROU). Επιπλέον, χρησιμοποιήθηκαν οι δομές Εμπιστοσύνη στην Τεχνολογία (Trust in Technology - TT) και Καινοτομία (Innovativeness - Innov).

Διαπιστώθηκε ότι οι κύριοι Διευκολυντές (Facilitators) της Συμπεριφορικής Πρόθεσης Υιοθέτησης της Τεχνολογίας (Behavioral Intention - BI) είναι η Εμπιστοσύνη στην Τεχνολογία (Trust in Technology - TT), ακολουθούμενη από τη Συμβατότητα (Compatibility - COMP), την Αντιλαμβανόμενη Χρησιμότητα (Perceived Usefulness - PU) και την Καινοτομία (Innovativeness - INNOV). Η παρούσα έρευνα δείχνει επίσης ότι τα άτομα ενδιαφέρονται λιγότερο για την ευκολία χρήσης της τεχνολογίας και είναι πρόθυμα να τη θυσιάσουν για να επιτύχουν μεγαλύτερη ασφάλεια. Η Συμβατότητα και η Καινοτομία παίζουν επίσης σημαντικό ρόλο. Τα άτομα που πιστεύουν ότι η χρήση της τεχνολογίας BBCA θα ταίριαζε στον τρόπο ζωής τους και θα ήθελαν να πειραματιστούν με νέες τεχνολογίες έχουν θετική πρόθεση να υιοθετήσουν την τεχνολογία BBCA. Για τις νέες δομές που προστέθηκαν, τα αποτελέσματα υποστηρίζουν την υπόθεση ότι οι Κίνδυνοι Ασφάλειας & Προστασίας

Προσωπικών Δεδομένων (Security & Privacy Risks - SPR) είναι ένας διευκολυντής για την Αντιλαμβανόμενη Χρησιμότητα (Perceived Usefulness - PU). Επίσης, η PU ενεργεί ως διευκολυντής στην Συμπεριφορική Πρόθεση Υιοθέτησης της Τεχνολογίας (BI). Κατά συνέπεια, τα άτομα που δεν αισθάνονται επαρκώς προστατευμένα από τις κλασικές μεθόδους αυθεντικοποίησης θα εξετάσουν τη χρησιμότητα της τεχνολογίας BBCA για την πρόσθετη προστασία τους από κινδύνους. Επίσης, με τις δομές Ανησυχίες Ιδιωτικότητας των Βιομετρικών (Biometrics Privacy Concerns - BPC) και Αντιλαμβανόμενος Κίνδυνος Χρήσης της Τεχνολογίας (Perceived Risk of Using the Technology - PROU) εξετάζεται εάν οι ανησυχίες των ατόμων σχετικά με το βιομετρικό τους απόρρητο λειτουργούν ως Αναστολείς (Inhibitors) στο BI. Το συμπέρασμα που προκύπτει είναι ότι τα άτομα θεωρούν ότι τα οφέλη που σχετίζονται με την ασφάλεια των αγαθών τους (π.χ. χρήματα σε τραπεζικό λογαριασμό) από τη χρήση της τεχνολογίας BBCA είναι πολύ πιο σημαντικά από τους αντιλαμβανόμενους κινδύνους για το απόρρητό των βιομετρικών τους. Αυτό προκύπτει από το ότι η υπόθεση πως ο κύριος αναστολέας του BI είναι η δομή Αντιλαμβανόμενος Κίνδυνος Χρήσης της Τεχνολογίας (PROU) δεν υποστηρίζεται από το μοντέλο. Οι νέες δομές χρησιμοποιήθηκαν για την επέκταση του μοντέλου TAM και την αντιμετώπιση των περιορισμών του όσον αφορά στην αντιμετώπιση αντιλαμβανόμενων ζητημάτων ασφάλειας και ιδιωτικότητας. Ως εκ τούτου, προτείνεται το νέο θεωρητικό πλαίσιο να συνδυαστεί με το TAM για την έρευνα που αφορά στην υιοθέτηση τεχνολογιών βιομετρικής αυθεντικοποίησης και συνεχούς αυθεντικοποίησης.

Στο τρίτο στάδιο έρευνας της παρούσας διατριβής παρατηρήθηκε ότι μια σημαντική πρόκληση και ένα ανοιχτό πρόβλημα, για την έρευνα που αφορά στην ανάπτυξή συστημάτων BBCA, είναι η συλλογή και η τελειοποίηση ενός κατάλληλου συνόλου βιομετρικών δεδομένων συμπεριφοράς. Το ζήτημα επιδεινώνεται από το γεγονός ότι οι περισσότεροι χρήστες αποφεύγουν να συμμετέχουν σε χρονοβόρες και επίπονες διαδικασίες που συνεπάγεται η συλλογή βιομετρικών δεδομένων έρευνας. Για το λόγο αυτό, η ανάπτυξη και η δοκιμή μιας μεθοδολογίας και ενός εργαλείου συλλογής βιομετρικών χαρακτηριστικών, με τρόπο φιλικό προς τον χρήστη, αποτελεί μια άλλη μεγάλη πρόκληση. Ως απάντηση σε αυτές τις προκλήσεις, στο τρίτο στάδιο της έρευνας, παρουσιάζεται ένα νέο παράδειγμα συλλογής συμπεριφορικών

βιομετρικών δεδομένων, που ονομάζεται BioGames paradigm και ακολουθεί μία καινοτόμα προσέγγιση. Η προσέγγιση αυτή αφορά στην παιγνιοποίηση της συλλογής δεδομένων. Ταυτόχρονα αναπτύχθηκε και ένα εργαλείο συλλογής συμπεριφορικών βιομετρικών (Biogames App) που βασίζεται στο παράδειγμα BioGames. Η BioGames App χρησιμοποιεί παιχνίδια και προκλήσεις που συνδυάζουν δυναμική πληκτρολόγησης (Keystroke Dynamics) και χειρονομίες αφής (Touch Gestures).

Στο τέταρτο στάδιο, παρουσιάζεται μια έρευνα σχετική με το σχεδιασμό και την αξιολόγηση νέων προσεγγίσεων στην συνεχή αυθεντικοποίηση χρησιμοποιώντας δυναμική πληκτρολόγησης (Keystroke Dynamics) και χειρονομίες αφής (Touch Gestures). Σύμφωνα με τη βιβλιογραφία, αρκετές μελέτες χρησιμοποιούν μονοτροπικές συμπεριφορικές μεθόδους (single behavioral modality methods) για τον έλεγχο της ταυτότητας των χρηστών. Ωστόσο, οι συμπεριφορές των γνήσιων χρηστών (genuine users) μπορεί να αλλάξουν και τα συστήματα να αποτυγχάνουν όταν συμβαίνουν σημαντικές αλλαγές. Τα παραπάνω έχουν ως αποτέλεσμα να δημιουργούνται είτε ζητήματα ασφάλειας είτε ευχρηστίας (security or usability issues). Στην βιβλιογραφία, η Σύντηξη (Fusion) βιομετρικών στοιχείων χρησιμοποιείται για την επίλυση αυτού του προβλήματος και επιτυγχάνει βελτιωμένα αποτελέσματα. Στην παρούσα έρευνα εξετάζεται κάθε συμπεριφορική βιομετρική περίπτωση ξεχωριστά και διερευνάται η περίπτωση βελτίωσης των αποτελεσμάτων απόδοσης με σύντηξη χειρονομιών αφής και δυναμικής πληκτρολόγησης σε επίπεδο χαρακτηριστικών (Feature-level fusion). Στην παρούσα προσέγγιση γίνεται σύγκριση μεταξύ βαθιών νευρωνικών δικτύων (Deep Neural Networks) σχεδιασμένων για δεδομένα που συνεπάγονται σημαντικές χρονικές δυναμικές, όπως το Multi-Layer Perceptron (MLP) και βαθιών νευρωνικών δικτύων σχεδιασμένων για ανεξάρτητα κατανεμημένα δεδομένα, όπως η Μακροχρόνια Βραχυπρόθεσμη Μνήμη (Long Short-Term Memory -LSTM). Συγκρίνοντας την απόδοση των δύο συστημάτων, το MLP είναι ανώτερο από το LSTM σε αυτό το πλαίσιο. Το MLP πέτυχε Accuracy 98,3% (αύξηση 21,1%), Equal Error Rate (EER) 1% (μείωση σφάλματος κατά 23,7%), True Acceptance Rate (TAR) 99,4% (αύξηση 46%), True Reject Rate (TAR) 97,4% (αύξηση 10%), False Acceptance Rate (FAR) 2,6% (μείωση κατά 10%), και False Reject Rate (FRR) 0,6% (μειωμένο κατά 46%). Από τα αποτελέσματα της έρευνας προκύπτει ότι η σύντηξη χειρονομιών αφής και δυναμικής

πληκτρολόγησης σε επίπεδο χαρακτηριστικών βελτιώνει την απόδοση των συστημάτων και επιλύει ζητήματα ασφάλειας και ευχρηστίας.

Abstract

Authentication systems based on PINs and passwords or physiological biometrics (e.g., iris, fingerprint, etc.) establish the user identity only at the beginning of the session using the entry-point authentication model. This model has been criticized heavily for being vulnerable to attacks occurring after the authenticated session has been established. Some of these systems defend against such attacks by performing an additional authentication step at critical points of the session but are unpopular with users due to repetitive authentication.

Mobile devices and their applications use the entry-point authentication model to authenticate users. Therefore, an important concern is to determine whether the mobile device is in the hands of the genuine user, and accordingly, whether the genuine user is the one using the sensitive services during a session. To solve this issue Continuous Authentication (CA) systems using Behavioral Biometrics (BBs) have been proposed in the literature. CA systems are an additional security measure that monitors users' biometric behavior by constantly re-authenticating them during a login session. However, their practical application is limited due to two fundamental shortcomings. The first shortcoming focuses on non-technical issues, for example, perceptions related to the fears and expectations of future users and perceived concerns about the privacy of their biometrics. The second shortcoming focuses on the problem of false positive/false negative results, that is, on security and usability issues.

This doctoral thesis includes four research stages. These are the research stages of a single research project. In the first research stage, an extensive literature review is presented that maps the research area and concerns BBCA technology and the performance of machine learning systems. Additionally, a literature review on potential attack vectors on BBCA systems is presented, and promising countermeasures are highlighted. Also, behavioral biometrics (Behavioral Biometrics - BBs) are classified into seven categories and an analysis of their feature extraction and collection methodologies is carried out. Finally, challenges, open issues, and future trends are identified.

In the second research stage of this thesis, the effect of various factors on Behavioral Intention to Adopt the Technology (Behavioral Intention - BI) is investigated through a new integration

of the Technology Acceptance Model (TAM) and the Diffusion of Innovation Theory (DOI). Also, a new theoretical framework is developed with constructs such as Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC), and Perceived Risk of Technology Use (PROU). In addition, the constructs of Trust in Technology (TT) and Innovativeness (Innov) were used.

It was found that the main Facilitators of the Behavioral Intention to Adopt the Technology (BI) are Trust in Technology (TT), followed by Compatibility (COMP), Perceived Usefulness (PU), and Innovativeness (INNOV). This research also shows that people care less about the ease of use of technology and are willing to sacrifice it to achieve greater security. Compatibility and Innovation also play an important role. People who believe that using BBCA technology would fit their lifestyle and would like to experiment with new technologies have a positive intention to adopt BBCA technology. For the new constructs added, the results support the hypothesis that Security & Privacy Risks (SPR) is a facilitator of Perceived Usefulness (PU). Also, PU acts as a facilitator of Behavioral Intention to adopt the technology (Behavioral Intention – BI). Consequently, individuals who do not feel sufficiently protected by classic authentication methods will consider the usefulness of BBCA technology for their additional protection against risks. Also, the constructs Biometrics Privacy Concerns (BPC) and Perceived Risk of Using the technology (PROU) examine whether individuals' concerns about their biometric privacy act as inhibitors to BI. The conclusion drawn is that individuals consider the benefits related to the security of their assets (e.g., money in a bank account) from using BBCA technology to be far more important than the perceived risks to the privacy of their biometrics. This results from the fact that the hypothesis that the main inhibitor of BI is the construct Perceived Risk of Using the technology (PROU) is not supported by the model. The new constructs were used to extend the TAM model and address its limitations in addressing perceived security and privacy issues. Therefore, it is proposed that the new theoretical framework be combined with TAM for research on the adoption of biometric authentication and continuous authentication technologies.

In the third research stage of this thesis, it was observed that a major challenge and an open problem for research related to the development of BBCA systems, is the collection and refinement of an appropriate set of behavioral biometric data. The issue is compounded by the fact that most users avoid engaging in time-consuming and laborious processes involved in collecting biometric survey data. For this reason, developing and testing a user-friendly biometric collection methodology and tool is another major challenge. In response to these challenges, in the third stage of the research, a new behavioral biometric data collection paradigm, called the BioGames paradigm, is presented and follows an innovative approach. This approach is about gamification of data collection. At the same time, a behavioral biometric collection tool (Biogames App) based on the BioGames example was developed. The BioGames App uses games and challenges that combine Keystroke Dynamics and Touch Gestures.

In the fourth stage, research related to the design and evaluation of new approaches to continuous authentication using Keystroke Dynamics and Touch Gestures is presented. According to the literature, several studies use single behavioral modality methods to authenticate users. However, the behaviors of genuine users may change, and systems fail when significant changes occur. The above result in either security or usability issues. In the literature, Biometric Fusion is used to solve this problem and achieves improved results. In the present research, each behavioral biometric case is examined separately and the case of improving performance results by fusion of touch gestures and keystroke dynamics at the feature level (Feature-level fusion) is investigated. In the present approach, a comparison is made between deep neural networks designed for data that entail important temporal dynamics, such as Multi-Layer Perceptron (MLP), and deep networks designed for independently distributed data, such as Long Short-Term Memory (LSTM). By comparing the performance of both systems, the MLP is superior to LSTM in this context. The MLP achieved greater improvement and better performance compared to the LSTM. The MLP achieved an Accuracy of 98.3% (an increase of 21.1%), an EER of 1% (the error was reduced by 23.7%), a TAR of 99.4% (an increase of 46%), a TRR of 97.4% (increased 10%), a FAR of 2.6% (reduced by 10.5%) and an FRR of 0.6% (reduced by 46%). The research results show that the feature-level

fusion of touch gestures and keystroke dynamics improves the performance of the systems and solves both security and usability issues.

1 Introduction

For several decades, user authentication was based on the "something the user knows" paradigm referred to as the knowledge-based authentication method [139]. This method has been the most popular for authenticating an individual, but research has shown that PINs and passwords do not provide adequate protection [13, 140]. Especially when the method is used on mobile devices it is known to suffer from low user-friendliness and insufficient security [102]. Also, mobile devices are vulnerable to smudge attacks, and PINs and secret touch patterns can be revealed [65]. Hence, the theft of a device may give rise to the risk of allowing full access to critical applications and personal data. In addition, Stylios et al. [58], showed that a high percentage (24%) of smartphone users ignore privacy and security risks and store, on their mobile devices, large volumes of private information including PINs, credit card numbers, etc. Also, a high percentage of users ignore protection practices for their PINs and passwords [58, 247]. These vulnerabilities stress the need for the development and implementation of novel authentication methods. These methods are based on the "something that the user is" paradigm, which is something that characterizes the user and constitutes a unique physiological biometric feature (e.g., fingerprint, iris, etc.). Under this paradigm, authentication is performed by comparing a previously captured biometric template to a biometric feature of the person (e.g., a fingerprint) [3, 12, 44, 97, 152]. The previously captured biometric template must derive from the same person and be of the same type [141].

Whether based on PINs and passwords or physiological biometrics, these methods use the entry-point authentication model, which authenticates the user only at the beginning of the session [33]. This model has been heavily criticized since it becomes vulnerable to attacks that

occur after the initial authentication [1, 2, 5, 33, 58, 210, 211 187]. For these reasons, a new method of user authentication, also based on the “something that the user is” paradigm, has been proposed. This method uses Behavioral Biometrics (BB) and Continuous Authentication (CA) [1, 97,184, 187, 212, 213]. As mobile devices become more advanced technologically, it is abundantly clear that the incorporated sensors can be used to efficiently capture the behavior of most users, thus enabling behavioral biometric user authentication [54, 55, 84, 86, 114]. Mobile devices can enroll BB templates from their sensors [86,109,141]. BB can include walking gait, touch gestures, keystroke dynamics, hand waving, user profile, and power consumption. Continuous Authentication technology constitutes an additional security measure alongside the initial login process by monitoring user behavior and continuously re-authenticating user identity throughout a login session [1, 85, 94, 97, 116, 117, 184, 187]. The idea of continuous authentication emerged in the early 2000s [213]. This technology has gained more attention since then, both from academia and industry. The increase in attention to biometric technology is encouraged by the expected reduction of technology costs, better systems’ properties, and socio-political pressure for improved security controls [6, 191, 188]. Finally, research like the one presented in [5, 7, 8, 183] showed that users are eager to use biometric authentication methods to protect their privacy.

The rapid development of biometric technologies in several areas, however, raises some privacy concerns [187]. Personal data collected from biometric systems are of a particular nature as they relate to either the physical characteristics of an individual (e.g., fingerprints, iris, facial features, DNA, etc.) or its behavioral features (e.g., touch gestures, keystroke dynamics, walking gait, hand waving, etc.) [187]. In the conscience of individuals, biometrics are also often associated with the violation of privacy by state controls that use these new technologies [214]. Individuals' perceptions and behavior are significant elements of systems’ design because users are concerned about their privacy, security, and online identity management [207]. The identification of related non-technical issues, for example, future users’ expectations and perceptions related to the fears, is probably required when preparing a strategy to assist the adoption of a widespread innovation [147, 188, 187]. Consequently, for the success of future investments in the implementation of CA systems, there is a need to

explore the key factors that influence technology adoption. Assessing the key factors of BBCA technology adoption is essential to solving the issue of low use and reduced exploitation of the advantages of this technology.

One major challenge for behavioral biometrics research is the lack of real-world datasets for research purposes [10, 187]. The compilation and refinement of a proper set of behavioral biometrics data constitute a challenge and an open issue. The issue is aggravated by the fact that most users avoid participating in time-consuming, painstaking procedures entailed in the collection of research biometric data. For this reason, developing and testing a methodology and a tool for extracting biometric features, in a user-friendly way, constitutes another great challenge.

According to the literature [1, 9, 187, 193], most studies use single behavioral modality methods to authenticate users. However, the behaviors of genuine users may change, and systems fail when significant changes occur [187, 193]. The above result in either security or usability issues. Most BBCA systems often operate with a high False Reject Rate (FRR) at thresholds attempting to keep the False Acceptance Rate (FAR) under 0.1% [112, 113, 187, 193]. Of course, a false rejection that diminishes usability is less costly than a false acceptance that diminishes security. A higher FAR will reduce the security level of the authentication system, while a higher FRR will block a genuine user [9, 193]. However, this imbalance may make the whole system unusable. To overcome these limitations, it is crucial to maximize the performance of BBCA systems and examine how to find a balance between security and usability [9, 112, 113, 187, 193].

1.1 Research Objective

This doctoral thesis includes four research stages. In the first stage, an extensive survey is presented that maps the research area. The scope of the survey is wide, ranging from reviewing BB and CA technologies to data collection methodologies and relevant machine learning systems. The main goal of the survey is to offer a sufficient background on BBCA technology for mobile devices, of interest to both researchers and practitioners. The purpose is to present all the significant elements for enabling researchers to conduct their research. The first goal is

to present a classification of seven categories of BB and CA on mobile devices and an analysis of BB collection methodologies, and feature extraction. The second goal is to present a literature review on machine learning systems performance in seven types of BB for CA. Further, an additional review is conducted that showed the vulnerability of machine learning systems against well-designed adversarial attack vectors, and the relevant countermeasures are highlighted. Finally, a discussion extends to lessons learned, current challenges, and future trends.

In the second stage, a new model is presented to investigate the effect of various factors on behavioral intention to adopt the technology (Behavioral Intention – BI). Based on this model, a Structural Equation Modeling (SEM) research was carried out. This research is among the first in the field that examines the factors that influence individuals' decision to adopt BBCA technology. An extensive conceptual framework is provided for both existing models (Technology Acceptance Model (TAM) and Diffusion of Innovation Theory (DOI)) and the new constructs added to the model. In addition, the research explores external factors, such as Trust in Technology (TT) and Innovativeness (Innov). It has been reported in the literature that the TAM model needs additional prior factors, especially when used in the investigation of biometrics technology acceptance [188, 242]. Also, the measurements of TAM using only a few of its standard variables are clearly restrictive [188]. Therefore, the TAM was adapted to the needs of the present research. New variables are added to the TAM, while some of the original variables, which did not contribute to the present research, were extracted. In addition, significant constructs were introduced, to overcome the limitations of the TAM and to adapt it to the needs of the present research. The new theoretical framework introduced in the present research concerns the constructs of Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC), and Perceived Risk of Using the Technology (PROU). The design of the research is such as to meet the above-mentioned combination. That is the trade-off between perceived users' concern for their biometrics privacy and their protection from risks [250].

In the third stage, a new behavioral biometric data collection paradigm is presented, called the BioGames paradigm [246] and an innovative approach to the gamification of data collection

follows. At the same time, a tool for collecting keystroke dynamics and touch gestures is developed. The BioGames App is based on the Bio-Games paradigm, where users play games without participating in an exhaustive experimental process, and for each modality, the application creates all the datasets.

In the fourth stage, research related to the design and evaluation of new approaches to continuous authentication using Keystroke Dynamics and Touch Gestures is presented. The research aims to design and evaluate new approaches to CA by applying feature-level fusion of touch gestures and keystroke dynamics to solve security and usability issues. In feature-level fusion, the feature sets from multiple behavioral biometrics are unified into a single feature set [14, 187]. Our goal is to accomplish a solution that achieves better performance compared to a single modality method. First, an experimental data collection process of biometrics is applied by using mobile smartphones. For this purpose, the BioGames paradigm and the BioGames App [246] are used. In the experiment, users' keystroke dynamics and touch gestures were recorded. Second, new appropriate feature sets, for continuous authentication, of touch gestures, keystroke dynamics, and the fusion of both, were developed. Following, a comparison is made on deep networks designed for data that entail important temporal dynamics, such as Multi-Layer Perceptron (MLP), and deep networks designed for independently distributed data, such as Long Short-Term Memory (LSTM). This choice is made because there is a great corpus of research, on touch gestures and keystroke dynamics with MLP and LSTM, which has given very good results [187] and it would be easier to be compared to the approaches of this research. Each modality is examined separately and an investigation is made regarding the improvement of performance by applying feature-level fusion to solve either security or usability issues.

1.2 Research Questions

The present thesis aims to answer the following research questions:

1. Which are the challenges, the open issues, and the future trends of BBCA technology?
2. Which are the key factors of user acceptance (or reject) of BBCA technology?

3. Is there a need for the development of a new paradigm for the collection of behavior biometrics data for research purposes? Could this new paradigm be supported by an effective behavioral biometrics collection tool?
4. Does feature-level fusion of touch gestures and keystroke dynamics improve the performance of deep learning systems and address both security and usability issues?

1.3 Contribution of the Thesis

This research comprised four research stages that each addressed one of the above research questions and resulted to a relevant publication. Here, the contribution of each stage of the research is presented separately as well as the research question they address. Table 1 associates the papers to each contribution point and the corresponding research question.

Table 1: List of publications.

Contribution of thesis		
Research	**Research questions**	**Publications**
Stage 1	Which are the challenges, the open issues, and the future trends of BBCA technology?	Ioannis Stylios, Spyros Kokolakis, Olga Thanou, Sotirios Chatzis, (2021). Behavioral biometrics & continuous user authentication on mobile devices: A survey, Information Fusion, Volume 66, 2021, Pages 76-99, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2020.08.021.
Stage 2	Which are the key factors of user acceptance (or reject) of BBCA technology?	Ioannis Stylios, Spyros Kokolakis, Olga Thanou, Sotirios Chatzis, (2022). Key factors driving the adoption of behavioral biometrics and continuous authentication technology: an empirical research", Information and Computer Security, Vol. 30 No. 4, pp. 562-582. https://doi.org/10.1108/ICS-08-2021-0124
Stage 3	Is there a need for the development of a new paradigm for the collection of behavior biometrics data for research purposes? Could this new paradigm be supported by an effective behavioral biometrics collection tool?	Ioannis Stylios, Spyros Kokolakis, Andreas Skalkos, Sotirios Chatzis, (2022). BioGames: a new paradigm and a behavioral biometrics collection tool for research purposes, Information and Computer Security, Vol. 30 No. 2, pp. 243-254. https://doi.org/10.1108/ICS-12-2020-0196
Stage 4	Does feature-level fusion of touch gestures and keystroke dynamics improve the performance of deep learning systems and address both security and usability issues?	Ioannis Stylios, Sotirios Chatzis, Olga Thanou, Spyros Kokolakis (2023). Continuous Authentication with Feature-Level Fusion of Touch Gestures and Keystroke Dynamics to Solve Security and Usability Issues. Under review.

1.3.1 Contribution of research stage 1

The first stage of the research concerns a survey on Behavioral Biometrics & Continuous User Authentication on Mobile Devices.

Research contribution of this stage:

- A classification of behavioral traits on seven categories and an analysis of behavioral biometrics collection methodologies and feature extraction.
- A wide range, state-of-the-art literature review on BBCA technology and the performance of machine learning systems.
- A literature review on possible attack vectors on BBCA technology and a highlight on promising countermeasures.
- Identification of challenges, open issues, and future trends.

➢ ***Publication of stage 1:*** Behavioral Biometrics & Continuous User Authentication on Mobile Devices: A Survey.

1.3.2 Contribution of research stage 2

The second stage of the research concerns an empirical research on key factors driving the adoption of Behavioral Biometrics & Continuous Authentication Technology.

The research contribution of this stage is the following:

- It proposes a new integration of a modified TAM model and DOI theory, which examines the influence of various factors on BBCA's behavioral intent of adoption.
- A new theoretical framework is created with constructs such as Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC) and Perceived Risk of Using the Technology (PROU).
- A research model focused on BBCA technology is developed that can be used by researchers, practitioners, governments, decision-makers, and providers of BBCA technology.

➢ ***Publication of stage 2:*** Key factors driving the adoption of Behavioral Biometrics & Continuous Authentication Technology: An Empirical Research.

1.3.3 Contribution of research stage 3

The third stage of the research concerns the creation of a new paradigm and a behavioral biometrics collection tool for research purposes.

The research contribution of this stage is the following:

- Presentation of a new paradigm, named BioGames, that suggests a user-friendly and entertaining way for the collection of behavioral biometrics for users of mobile devices.
- Development of a novel behavioral biometrics collection tool, named BioGames App, which is freely available for researchers and practitioners.
- Development of new appropriate feature sets for continuous authentication of touch gestures and keystroke dynamics.
- Introduction of a convenient data collection methodology by which the behavioral biometrics of the users can be collected via BioGames.

➢ ***Publication of stage 3:*** BioGames: a new paradigm and a behavioral biometrics collection tool for research purposes.

1.3.4 Contribution of research stage 4

The fourth stage of the research concerns continuous authentication with a feature-level fusion of touch gestures and keystroke dynamics to solve security and usability issues.

The research contribution of this stage is the following:

- Development of a new appropriate feature set for continuous authentication that combines touch gestures and keystroke dynamics.
- A comparative study between MLP and LSTM on the development of a BBCA system is provided.
- Is shown that the feature-level fusion of touch gestures and keystroke dynamics improves the performance of the systems.
- Is shown that the feature-level fusion of touch gestures and keystroke dynamics solves both security and usability issues.
- Is shown that MLP is superior to LSTM in this context.

- ***Publication of stage 4:*** Continuous Authentication with Feature-Level Fusion of Touch Gestures and Keystroke Dynamics to Solve Security and Usability Issues.

1.4 Structure of the Thesis

This Thesis is structured as follows: The first section is the introduction section that includes a brief description of the Behavioral Biometrics and Continuous Authentication technology for user authentication and its challenges. Moreover, it includes the research objective, the research questions and the contribution of the Thesis. The second section is the background section, focusing on mobile devices, sensors, biometrics, performance metrics, and continuous authentication technology. Also, a classification of Behavioral Biometrics and Continuous Authentication into seven categories, is presented. In addition, an analysis of behavioral biometrics collection methodologies, feature extraction and the existing publicly available datasets is presented. The third section is the literature review section, where the performance of machine learning systems is presented. The fourth section that follows is the method of work section, where the four research stages that comprise this research and each address one of the research questions are presented. In the fifth section a new model is presented to investigate the effect of various factors on Behavioral Intention to Adopt the Technology. In the sixth section that follows, a new paradigm is proposed, named BioGames, for the extraction of behavioral biometrics conveniently and entertainingly. In the seventh section that follows, research related to the design and evaluation of new approaches to continuous authentication using keystroke dynamics and touch gestures is presented. Finally, a summary, conclusions and future work section of this research is presented.

2 *Background*

2.1 Introduction

In this section, an overview of mobile devices, sensors, biometrics, performance metrics, and continuous authentication technology is presented. Also, a classification of BB and CA into seven categories is presented. The first category is walking gait, the second category is touch gestures, the third category is keystroke dynamics, the fourth category is behavioral profiling, the fifth category is hand waving, the sixth category is power consumption, and the seventh category is fusion. Also, an analysis of behavioral biometrics collection methodologies, feature extraction and the existing publicly available datasets, is offered.

2.2 Mobile Devices and Sensors

As mobile devices become more technologically advanced, they incorporate sensors that can capture accurately most aspects of users' motional behavior, which enables behavioral biometric user authentication [186, 54, 55]. Mobile devices have a rich selection of built-in sensors. We can distinguish three types of sensors: motion, position, and environmental sensors. Forces of acceleration and rotation along three axes are measured by motion sensors. This type of sensors includes accelerometers, gravity sensors, gyroscopes, and rotational vector sensors. The physical position of a mobile device is spotted by position sensors, which include orientation sensors and magnetometers [114, 84]. Environmental parameters are measured by environmental sensors, such as barometers, thermometers, and photometers [114]. Apart from these sensors, smartphones also incorporate microphones, cameras, touchscreens, GPS, compasses, etc. Through these sensors, we can collect data that correspond to a matching behavioral modality [86].

2.3 Biometrics

Biometric methods are techniques for identifying individuals by analyzing their unique characteristics. Biometric methods can be categorized into two categories: techniques based on the analysis of physical or genetic characteristics, and techniques based on the analysis of behavior [187]. Indeed, each user interacts with his/her device uniquely and distinctively. Thus, behavioral biometrics are based on behavioral characteristics of individuals captured by mobile phone sensors, mainly through the gyroscope and accelerometer recordings, as well as touch screen recordings that capture tap, swipe, typing, etc. [86]. Some devices also have more advanced sensors, such as those that capture side squeeze. Sensors incorporated in mobile devices track various behavioral modalities, including walking gait, touch gestures, keystroke dynamics, hand waving, behavioral profile, and power consumption. Moreover, research like that presented in [140, 36, 186, 187] showed that users are willing to adopt alternative methods of authentication, such as biometrics, to protect their privacy [187].

2.4 Evaluation

In this section the performance metrics and the classifiers are presented.

2.4.1 Performance metrics

The basic metrics that are applied for evaluating an authentication system depend on the error rates. Following, a discussion on some basic evaluation metrics is made [4, 94, 127, 170, 187, 245]:

- The *Confusion matrix* is used to describe the performance of a classifier. In table 2 an example of a confusion matrix is presented where there are two possible predicted classes: "Genuine" and "Impostor".

Table 2: Confusion matrix.

		Actual Class	
		Genuine	Impostor
Predicted Class	Genuine	TA	FA
	Impostor	FR	TR

Where:

- *TA (True Acceptance)* is the number of patterns belonging to the genuine user and ranked correctly as "Genuine".
- *TR (True Reject)* is the number of patterns not belonging to the genuine user and ranked correctly as "Impostor".
- *FA (False Acceptance)* is the number of patterns not belonging to the genuine user and ranked mistakenly as "Genuine".
- *FR (False Reject)* is the number of patterns belonging to the genuine user and ranked mistakenly as "Impostor".

Based on the above, the True Acceptance Rate (TAR), False Acceptance Rate (FAR), False Reject Rate (FRR), Accuracy and Equal Error Rate (EER) are estimated as follows [127]:

- *True Acceptance Rate (TAR)* is the conditional probability of a pattern to be classified in the class "Genuine" given that it belongs to it. TAR is given by the formula:

$$TAR = \frac{TA}{TA+FR}, (1)$$

- *True Reject Rate (TRR): is the conditional probability of a pattern to be classified in the class "Impostor" given that it belongs to it. TRR is given by the formula:*

$$TRR = \frac{TR}{FA+TR} (2)$$

- *False Acceptance Rate (FAR)* is the conditional probability a pattern to be classified in the class "Genuine" given that it does not belong to it. FAR is given by the formula:

$$FAR = \frac{FA}{FA+TR}, (3)$$

- *False Reject Rate (FRR)* is the conditional probability a pattern not to be classified in the class "Genuine" given that it belongs to it. FRR is given by the formula:

$$FRR = \frac{FR}{TA+FR}, (4)$$

- *Accuracy* is defined as the probability of a correct classification of a pattern. Accuracy is given by the formula:

$$Accuracy = \frac{TA+TR}{TA+TR+FA+FR}, (5)$$

- *Equal Error Rate (EER)* is the point at which the false acceptance rate (FAR) and false rejection rate (FRR) are equal. [170].

In addition, the following metrics are often used:

- *Decision threshold:* the claimed identity is considered genuine, thus accepted, when its matching score exceeds a predefined threshold $\alpha \in (0, 1)$. In case the matching score of the claimed identity does not exceed the predefined threshold, it is perceived as an impostor, thus rejected. The formula for calculating the decision rule is the following [11]:

$$P(ui) = \begin{cases} Genuine, & P(ui) \geq \alpha \\ Impostor, & P(ui) < \alpha \end{cases}, (6)$$

  where α expresses a predefined threshold and $P(ui)$ expresses the score for a user ui authentication.

- *Receiver Operating Characteristic (ROC) Curve* demonstrates the performance based on TAR and FAR. The ideal point is represented by the top left corner where TAR equals one and FAR equals zero [11, 94]. The Area Under Curve (AUC) is used as an alternative to accuracy and the values range between 0 and 1 [11].
- *Mean Absolute Error (MAE):* the *average* of all absolute errors, described in the following formula [4]:

$$\text{MAE} = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y_i}|, (7)$$

  Where: n = the number of errors, Σ = summation, $|y_i - \hat{y_i}|$= the absolute errors.

- *Mean Squared Error (MSE):* measures the average squared error of model' s predictions. where y_i is the expected output and y_i is the prediction of model [4]:

$$\text{MSE} = \frac{1}{n}\sum_{j=1}^{n}\left(y_j - \hat{y_j}\right)^2, (8)$$

- *Root mean squared error (RMSE):* is the square root of the average of squared differences between prediction and observation [4]:

$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{j=1}^{n}\left(y_j - \hat{y}_j\right)^2}, \text{ (9)}$$

- *Half Total Error Rate (HTER):* is *equal* to the aggregation of FAR with FRR divided by 2. Decreased HTER, signifies better system performance. The HTER is calculated with the following formula [99]:

$$HTER = \frac{FAR + FRR}{2}, \text{ (10)}$$

- *Manhattan distance (Rectilinear distance L1):* is the sum of the lengths of the projections of the line segment between the points onto the axes of coordinates [107]:

$$d(a, b) = \sum_{i=1}^{n} |a_i - b_i|, \text{ (11)}$$

- *Euclidean distance L2:* is the length of the line segment connecting *points* a and b ($\overline{ab}$) [107]:

$$d(a, b) = \sqrt{\sum_{i=1}^{n} (a - b)^2}, \text{ (12)}$$

- *Dynamic Time Warping (DTW) distance metric:* It can shortly be described as an algorithm that can align temporal sequences and measure their similarities. More information can be found in the work of Zhao et al. [171].

2.4.2 Classifiers and machine learning algorithms

The purpose of this thesis is not to analyze each classifier; they are solely reported with a citation, in case someone is seeking for more information to easily find it. The algorithms that encountered are: Random Forests [61], Support Vector Machines (SVM) [62], Bayesian Networks [63], J48 tree [63], Multi-layer Perceptron (MLP) [63], Naïve Bayes [63], Instance-Based Learning Algorithms [48], Dynamic Time Wrapping (DTW) [66], k-Nearest Neighbors (kNN) [135], Long Short-Term Memory (LSTM) [88], Logistic Regression used as a classifier [136], Cycle detection [132], Manhattan method [107], isolation Forest [26], Hidden Markov Model (HMM) [27], Convolutional Neural Networks (CNNs) [106], Feed Forward Neural Network (FFNN) [28]], Generalized Regression Neural Networks (GRNNs) [40], Least Squares Anomaly Detection (LSAD) [42], Radial Basis Function networks (RBF) [46], Modified Edit-Distance algorithm (M-ED) [119], Ordinary Least Squares

regression (OLS) [130] and Strangeness-based Outlier Detection algorithm (strOUD) [86].

2.5 Classification and analysis

In this section, a classification of BB and CA on mobile devices into seven categories is presented. The first category is walking gait, the second category is touch gestures, the third category is keystroke dynamics, the fourth category is behavioral profiling, the fifth category is hand waving, the sixth category is power consumption, and the seventh category is fusion. Also, an analysis of behavioral biometrics collection methodologies and feature extraction and the existing publicly available datasets is provided. All behavioral traits can be categorized in these seven categories:

2.5.1 Walking Gait

This recognition technique is comparatively new and is based on the measurement and analysis of an individual' s manner of walking or running by using the acceleration signals produced by his/her mobile device. The characteristic of gait is amenable to smartphones due to their incorporated sensors, namely accelerometer, gyroscope, and magnetometer. The main advantage of this technique is that it can be applied to CA of users without requiring their intervention. However, factors such as the changing orientation of the device during walking [132], uneven ground, possible injuries, footwear, fatigue, personal peculiarities, etc. can affect its accuracy [86].

- *Data Collection:* The accelerometer is used to collect data when subjects are walking in normal, slow, and fast speeds. For estimating the smartphone's orientation in the participants' pocket, gyroscope data is used. Finally, the combination of accelerometer, gyroscope and magnetometer data allows for calculating the motion patterns of the human body [86].
- *Feature extraction:* The features used in the literature of walking gait analysis are speed, orientation, and human body motion patterns. The sensors in use are the accelerometer, the magnetometer and the gyroscope which respectively measure along the local X, Y, Z axes

of the device the acceleration in m/s2, the ambient geomagnetic field in μTesla and the rate of rotation in rad/s [86,94,103].

2.5.2 Touch Gestures

The touch gestures are shapes drawn by hand on the mobile devices touch screen that comprise of a single, or multiple strokes. Each stroke is a series of successive numerical coordinates. Features such as touch direction and the touch duration, the velocity and acceleration of movement are analyzed and measured solely or in combination with each other.

- *Data Collection:* The smartphone touch screen sensor is used for collecting touch data. Actions of input associated with parameters such as speed, velocity, size, length, direction or pressure, are converted into a gesture output template. These parameters are different between users and indicate the behavior of each, thus consisting the basis of the touch gesture authentication systems [86].
- *Feature extraction:* The collected data from users are extracted and analyzed to identify each user by his distinctive set of features. When the finger touches the mobile device screen whether it strokes or swipes it produces a series of touch data as shown in the following formula [84]:

$$S_i = (x_i, y_i, t_i, p_i, A_i, O_i^f, O_i^{ph}), i = \{1, 2, \dots, N\}, \textit{(13)}$$

where x_i, y_i are the location points, t_i are the time stamps, p_i is the finger pressure on screen, A_i is the finger blocked area, O_i^f is the finger orientation and O_i^{ph} is the device orientation (portrait or landscape) and *N* represents the total number of swipes.

2.5.3 Keystroke dynamics

The procedure of recording the typing keyboard inputs of an individual on a mobile device and the effort to identify him via an analysis based on his tapping habits is called keystroke dynamics [11,16].

- *Data collection:* Some researchers on keystroke dynamics collect data from predefined texts, for example during the typing of a text message, or during the log-in session when

entering passwords [40, 41,43,110,111]. Others conduct their research by collecting data not restricted on predefined sentences or passwords [42,44]. In both cases the results are of high accuracy.

- *Extracted features:* Duration, latency, pressure and location are the features used in the literature of keystroke analysis as explained following [105,110]:
    - *Duration* is also called hold time and corresponds to the period of time elapsed between the action of pressing and the action of releasing a key.
    - *Latency* is also called inter-key time and is expressed by the time period elapsed between the action of releasing a pressed key until pressing the next key.
    - *Pressure* is the pressure on a key.
    - *Location* are the finger location points (x_i, y_i) or the finger area on screen.

Also, Kambourakis et al. [256], introduced touchstrokes adding the features of distance and speed as input data. For data collection they used a predefined password and a predefined phrase. The extracted features were:

- *Distance,* which is the distance in pixels between two successively pressed virtual buttons.
- *Speed,* which is calculated as the quotient of the distance between two successively pressed virtual buttons divided by the inter-time for this event to complete.

2.5.4 Behavioral profile

The usage data of a mobile device can be employed for the behav- ioral authentication of individuals on the basis that they usually follow a specific pattern when using their phones to interact with applications and digital services [2]. The behavioral profile of a user can be built either based on his interaction with a network or with a host. In the first case the behavior of users is monitored regarding their patterns of connecting to Wi-Fi networks, service providers, etc., while in the sec- ond case the monitoring refers to the usage manner of

applications at different locations and time [94].

- *Data Collection:* Device usage data can be used in several combinations for the profiling of users. For example, Anjomshoa et al. [115] have used a self-developed behaviometric mobile application, namely TrackMaison to collect usage data resulting from the inter- action with five social network services such as location and session duration and usage frequency. Neil et al. [50] have used Wi-Fi, Bluetooth and application usage data. Fridman et al. [118] used the device location, applications used, the text entered, and the websites visited. Ashibani et al [156] used the interaction patterns of users while connecting to their home network, via a hub, to access and control IoT devices from their smartphones. Their model authenticated users based on the Android applications' access logs. In another study of Ashibani and Qusay [169] they authenticated users based on the events of mobile device application access in a smart home environment. Lee et al. [157] used SmarterYou, a system that combined three devices, a smartphone, a smartwatch, and an authentication server in the cloud. The smartwatch was used to monitor the raw data from the accelerometer and the gyroscope sensors and send the information to the smartphone via Bluetooth. The server in the cloud was used for computations and protection of data. Acien et al. [158], used the combination of touch gestures, keystrokes, applications usage data, WiFi, and GPS location while users interacted naturally with their smart- phones. They examined two scenarios depending on the number of sessions. The first scenario included one session (One-Time Authentication), while the second scenario included multiple sessions (Active Authentication).

- *Feature extraction:* In the work of Anjomshoa et al. [115] the Track Maison application collected spatiotemporal information regarding the usage of social network services. In addition, when TrackMaison was recording a session, it utilized the incorporated GPS of the device and recorded the location coordinates where the session initiated. Periodically it updated users' location. In the dataset used by Neil et al. [50] all data types included the date and time of data capture and the identification number of users. For the application

usage data, the available information additionally included the name of the accessed application. For the Bluetooth usage data, the available information further included the name of the sighted Bluetooth de- vice, the Received Signal Strength (RSSI - dBm) and the MAC address. For the Wi-Fi usage data the available information addi- tionally included the SSID (network name), the Received Signal Strength (RSSI – dBm) and the Access Point's MAC address. Regarding the four modalities studied by Fridman et al. [118], they counted the action's instances related to each modality of TEXT, APP, WEB and Location. Ashibani et al. [156] concentrated on the usage patterns of Android applications which consisted of the length and time of activity when users were accessing the network. Ashibani and Qusay [169] used the smart home hubs to collect the application access history including user id, timestamp, and name of the package. Lee et al. [157] used the accelerometer and the gyroscope sensors of the smartphone and the smartwatch to record the walking patterns and the manner of holding the smartphone. Regarding the application usage data, WiFi, and GPS location, Acien et al. [158] used timestamps and the frequency of the events, while for touch gestures they used the data of *x, y,* and *z* coordinates of the gyroscope and the acceleration vector from the accelerometer in each time stamp. For keystroke dynamics, they used hold time, press-press latency, and press-release latency.

2.5.5 Hand waving

The waving pattern of the wrist of an individual, while interacting with his mobile phone or just holding it, for identifying users has recently gained attention. This method does not require any additional action by the user besides holding the device. Several features can be used such as wrist twisting, speed, waving range and frequency. Individuals can be distinguished since the waving of their hand is different [97].

- *Data Collection:* Sitová et al. [38] captured Hand Movement, Orientation, and Grasp (HMOG) by recording the readings from the accelerometer, gyroscope and magnetometer sensors. They captured the device orientation and subtle movement deriving from the manner an individual taps on the smartphone after grasping and while holding it. Yang et

al. [100] selected the three-axis accelerometer sensor to measure the phone's acceleration during the waving action. Buriro et al. [98] collected the movement patterns of hand(s) resulting from the accelerometer, gyroscope, magnetometer, orientation and gravity sensors to profile users.

- *Feature extraction:* The features of grasp resistance and grasp stability can be extracted when users tap on the screen [38]. The resistance of a hand holding the device during a tap is measured by the grasp resistance features while the amount of time elapsed for the influence of movement caused by the tap to disappear is measured by the grasp stability features. The grasp resistance and grasp stability features can be extracted from the accelerometer, the gyroscope, and the magnetometer sensors (magnitude, x, y, and z axes). Also, some common features in hand waving extracted from each sensor are median, mean, standard deviation, mean absolute deviation, unbiased standard error of the mean, unbiased skewness and kurtosis [98].

2.5.6 Power Consumption

The fact that patterns of user behavior are highly correlated to the patterns of power consumption constitute the basis of this approach [129]. Power consumption is not used as a single identifier on biometric systems but in combination with other biometrics [86].

- *Data Collection:* Murmuria et al. [86] measured the power consumption resulting from the activities performed by the user by using the incorporated sensors of the battery driver of mobile devices namely the voltage and current sensors. In another work of Murmuria et al. [130], they collected information regarding the power usage from the power suspend driver. They recorded the power usage of the CPU, display, graphics, audio, microphone, Wi-Fi, and GPS.
- *Feature extraction:* The voltage is reported by the sensors to the kernel of the operating system in units micro-volts (uV) and the current in micro-Ampere (uA). The battery charge is reflected on the voltage readings while the quantity drawn by the Operating System is reflected on the current readings and depends on the kind of activities performed [86]. The

power-management module of the operating system reported the use of each subsystem's time shares. Based on these measurements, they calculated the power consumption of each application [130].

2.5.7 Fusion

In this section an analysis of the fusion achieved by a single sensor using multiple instances of a biometric and the fusion achieved by multiple sensors is made. The focus will be made on multimodal behavioral biometrics fusion. The purpose of multimodal systems is to access multiple sources of information from different modalities and improve the authentication accuracy [23]. Several researchers have used multi-modal behavioral biometrics traits, such as touch gestures, hand waving, behavioral profile, keystroke dynamics, walking gait, etc., to authenticate users [1,24,25]. According to Sanderson and Paliwal [14] fusion levels are divided into two categories:

a. **Pre-classification or fusion before matching:** Pre-classification refers to fusion at the sensor level (or raw data) and the feature level.
    - Sensor-level fusion is the unification of raw data obtained using multiple sensors or multiple instances of a biometric using a single sensor.
    - In feature-level fusion, the feature sets originating from multiple biometric algorithms are unified into a single feature set.
b. **Post-classification or fusion after matching:** Post-classification refers to fusion at the match score, rank and decision levels.

In match score-level fusion the combination of the match scores output resulting from multiple biometric matchers generates a new match score, which is thereafter used by the authentication system to achieve a decision. When a biometric system operates, the ranking of the enrolled identities constitutes the system's output. This output expresses the sorting of all possible sets of matching identities in decreasing order of confidence. In decision level fusion the majority voting approach is mostly used where the input of a biometric sample is attributed to that

identity on which the majority of the matchers agree [20]. There is a large corpus of research works referring to fusion. More information can be found in the following works: [17–22,90,108].

2.6 Publicly available datasets

There are some publicly available datasets like the one in the work of Mahbub et al. [166] that can be used for research purposes. This dataset was designed for biometric identification and it contains smartphone sensor signals collected from 48 volunteers over a period of 2 months. The data collected include the front-facing camera, touchscreen, gyro- scope, accelerometer, magnetometer, light sensor, GPS, Bluetooth, WiFi, proximity sensor, temperature sensor, and pressure sensor. The authors also stored the timing of screen lock and unlock events, start and end timestamps of calls, currently running foreground applications, etc. Another publicly available dataset is the itekube – 7 touch gestures dataset which was created from Debard et al [106] and it contains 6591 touch gestures of 7 different interaction classes.

Other publicly available datasets can be found in the works of Reyes- Ortiz et al. [164] and Casado et al. [165] which, although were not initially intended for biometric identification they could be used for that purpose. The dataset of Reyes-Ortiz et al. [164] was originally proposed for the recognition of human activity and it contains raw data from the inertial sensors (accelerometer and gyroscope) of a smartphone when carried by 30 different users. The dataset provided by Casado et al. [165] contains raw data from the accelerometer, gyroscope, and magnetometer of a mobile device when carried by 77 different people.

2.7 Conclusion

One major challenge for BB research is the small number of real-world datasets and the availability of a public behavioral biometrics database for research purposes [10]. There are some available datasets as in the work of Mahbub et al. [166] and Debard et al [106] that can be used for research purposes. Other publicly available datasets can be found in the works of Reyes-Ortiz et al. [164] and Casado et al. [165] which, although were not initially intended

for biometric identification, could all be used for that purpose. Also, many users avoid participating in time consuming, painstaking procedures for the collection of biometric features. This results in not fulfilling the data collection procedure. For this reason, the testing of a methodology for extracting biometric features, in a user-friendly way, constitutes an open problem. Also, BBCA technology is of limited extent due to some fundamental deficiencies, as, the Biometrics Privacy Concerns (BPC) of users [1]. There are two approaches to data collection and data processing. In the first approach, which is device-centric, data is collected and processed in the device itself, while in the second approach, data is sent to a central online server. Users may be concerned about their sensitive information and thus, research should focus on ways to preserve user privacy. This can be achieved by processing behavioral measurements on the user's mobile and that sensitive information is not sent to the online service. Also, in the work of Shila et al [102], it was shown that the device-centric implementation of authentication outperformed the cloud-based authentication in terms of classification accuracy and detection latency. In addition, particular attention should be given to the anonymization of behavioral biometrics data when these are collected for research purposes. If reliable and effective anonymization is not achievable, then specific permission or consent should be obtained, in accordance with applicable law.

In systems developed to provide security services, we aim for a small FAR and we can sacrifice the FRR to achieve low FAR. In systems that we are interested in friendliness, we want the opposite. TAR is actually the reverse of FAR. EER and Accuracy are more generic metrics that show the overall performance of the algorithm. EER is the error rate that is achieved by tuning the system's detection threshold thus much that FAR and FRR are equal. Accuracy is the percentage of samples that are classified accurately [170]. There are more specialized indicators such as ROC, MAE, HTER, RMSE, etc. The ROC curve demonstrates the dependency between the FAR, FRR, and detection threshold of the system. It is used to show how threshold values affect the overall accuracy of the algorithm. The Half Target Error Rate (HTER) is the average between the FAR and FRR at a random threshold. MAE measures the average magnitude of the errors in a set of predictions, without considering their direction. It is used as a combined metric of FAR and FRR. RMSE is the square root of the average of

squared differences between prediction and observation [4]. It is used to estimate how the model fits the data and it is an alternative for MSE which is used for the same purpose. Research works should include at least the FAR, TAR, FRR, EER, and Accuracy when evaluating the performance of their approach. In this way, a comparison between the different approaches will be feasible. Finally, when an authentication approach is evaluated, researchers should also weight and report the amount of data from each user that is necessary for each approach to be effective, the computational and communication cost, and the usage of battery, memory, and CPU. Future research should also measure those aspects to enable the comparison.

3 *Literature Review*

3.1 Introduction

Behavioral biometrics authentication techniques are built based on an individual's behavioral characteristic such as walking gait, touch gestures, keystroke dynamics, behavior profiling, hand waving, power consumption and fusion. A plethora of research works have been published. A literature review focusing on the performance of machine learning systems is presented. Each technique is evaluated separately, but a comparison based on performance metrics cannot be made, as not all researchers use the same metrics. However, for each system, there is at least one of the five basic metrics, namely FAR, TAR, FRR, EER, and Accuracy.

3.2 Relevant surveys

Recently published surveys, such as Crawford [87] and Yampolskiy & Govindaraju [89], refer to a single behavioral biometric. More specifically Crawford refers to keystroke dynamics and Yampolskiy & Govindaraju to behavioral profiling. Similarly, Ashbourn [91] refers to keystroke dynamics. Ferrag et al. [154] present electrocardiographic signal (ECG), keystroke and touch dynamics while Rui et al. [155] also consider voice recognition. Jain et al. [92] name two modalities used in CA, that is walking gait and keystroke dynamics, while Rogowski et al. [93] also consider the modality of touch gestures. Meng et al. [9] present four CA behavioral biometrics and also refer to morphological bio- metrics or behavioral biometrics not used for CA. Mahfouz et al. [11] present touch and keystroke dynamics, behavioral profiling and gait recognition. Finally, Abdulaziz and Kalita [94] provide a more extensive list of CA behavioral biometrics, including walking gait, touch gestures, keystroke dynamics, hand waving, and behavioral profiling.

The existing aforementioned surveys are quite old; thus, they contain very few references to recent literature. In addition, there is no reference to attack points on behavioral biometrics and countermeasures except for the work of Meng et al. [9]. Therefore, there is a striking lack of an up-to-date, thorough, exhaustive, and focused survey on CA and BB that would include the previously mentioned issues. The survey attacks exactly these topics focusing on BB and CA approaches amenable to mobile devices. The goal is to cover all BB for CA categories, attack vectors and defense techniques.

3.3 Walking Gait

Feng et al. [29] investigated the application of two different verification methods the Trajectory Reconstruction and the Statistic Method. They extracted certain features and identified users from the motion data. Users executed the movement of picking up their phone while sitting/standing stationary or walking. They concluded that user movements (walking) strongly affect the accelerometer data and the verification performance. They used an SVM classifier and achieved 7.09% Equal Error Rate when sitting/standing stationary and 6.13% while walking by the Trajectory Reconstruction and the Statistic Method respectively. They concluded that user movements (walking) strongly affect the accelerometer data and the verification performance.

Muaaz and Mayrhofer [132] used a self-developed android application to collect gait data (from tri-axis accelerometer data) from a smartphone that was placed in the trouser pocket of 35 individuals while they walked with normal pace. To compensate the orientation error produced by the movement of the device during walking, they modified the data processing steps and employed magnitude data, in addition to wavelet-based de-noising modules. Furthermore, they used a modified version of a cycle length estimation algorithm as it was one of the fundamental prerequisites of automatic cycle detection employed in their work. Their method achieved 7.05% EER for a walking session.

Al-Naffakh et al. [30] used the accelerometer and gyroscope of a smartwatch to collect data from 10 individuals while walking during two five-minute sessions on a flat surface on two different days with their natural walking speed. Users also chose on which arm they would

wear the smartwatch. They observed that test subjects had different patterns of movement and, thus, walking gait could be used to transparently and continuously authenticate individuals. In an antecedent research using smartwatches, Al-Naffakh et al. [31], presented two experiments on Same, Mixed, and Cross Day situations. Their results showed that the technology is sufficient to discriminate individuals by their gait characteristics. With data from the Same day they achieved 3.12% and 0.13% EER for gyroscope and accelerometer respectively, while in the evaluation of the Cross Day situation they achieved 7.97% and 0.69% for the same sensors. Simultaneously, Kork et al. [101] collected gait data from 50 individuals by using five wearable sensors that were placed to different areas on the body in addition to a smart- phone held in hand. Data were collected while users performed slow, normal and fast walking paces. In these three different walking scenarios the Equal Error Rate ranged from 0.17% to 2.27% for the wearable sensors, while for the smartphone the Equal Error Rate ranged from 1.23% to 4.07%.

Shila et al. [102] developed dCASTRA (deep CASTRA), a user verification service which was device-centric and constituted an improved version of a previous service named CASTRA built by the same authors. They extracted gait features for user classification by employing Long Short-Term Memory (LSTM) Recurrent Neural Networks. They also extracted segments of walking by using the Google Activity Recognition Service API. For their experiments, they used data from 15 individuals while they walked from the accelerometer and gyroscope sensors. Their system achieved the identification of users in less than 6 seconds with greater than 99.95% accuracy. In addition, they reported that for learning an efficient model the required amount of data was 60K samples using a 50Hz sampling rate and the minimum duration was 20 minutes.

Baek et al. [159], developed a gait- based authentication framework, named LiSA-G which successfully authenticated and identified 51 users by using the accelerometer and gyroscope sensors of a smartwatch. They applied two scenarios, where, in the first scenario users walked normally towards a smart home system and in the second scenario they walked normally towards a smart car system. Their framework extracted the walking gait and movement of

arms and achieved 8.2% EER by using the Random Forest classifier, while they needed fewer features and less amount of sensor data, specifically they needed 37 features and 100 data samples respectively, in comparison to other works [95,160,161] for authentication.

Table 3: Walking gait modality research works.

Method	Publications	Platform	Classification	Performance (%)	
				Accuracy	EER
Walking gait	[29] in 2013	smartphone	SVM		6.13
	[132] in 2014	smartphone	Cycle detection		7.05
	[31] in 2017	smartwatch	MLP		0.13
	[101] in 2017	wearable-smartphone	Manhattan method		0.17
	[102] in 2018	smartphone	LSTM	99.95	
	[159] in 2019	Smartwatch	Random Forest		8.2

3.4 Touch gestures

On the issue of user authentication based on touch gestures, Saevanee et al. [32] used finger pressure and keystroke dynamics (hold-time and inter-key) to investigate the behavioral input manner of users. They used a notebook touch pad to collect data and made analysis by the k-NN classification method. The finger pressure achieved 1% EER, the hold-time 30% and the inter-key 35%. Later, Frank et al. [33], used natural navigation gestures on the touchscreen of a smartphone such as up-down and left-right scrolling, to investigate whether these gestures could be used for continuous authentication. They extracted 30 touch features and used a Gaussian RBF kernel support vector machine and a k-nearest neighbor classifier to train user profiles. For inter-session authentication they achieved 2%-3% median equal error rate, while for intra-session authentication they achieved 0%. In the case where they carried out the authentication one week after the enrollment the equal error rate achieved was below 4%. Their method could be implemented to extend screen-lock time or to constitute a part of an authentication system based on multi-modal biometrics.

Later, Li et al. [34] designed a system to continuously re-authenticate smartphones users based on biometrics. They divided participants in 25 target users and in 47 non-target users and selected 8 sliding and tap features. Finger and touch movements of the owner were compared with the current user's finger movement patterns for verification. For classification they used a Support Vector Machine. The highest accuracy achieved was 95.78% for the sliding up gesture. Also, they measured the computation time for their system to make the classification, which was 17 milliseconds. Meanwhile, Zhao et al. [35], used shapes and intensity values of movement and pressure respectively, that were represented by a feature of their own design named Graphic Touch Gesture Feature (GTGF). They used six commonly used touch gestures divided into three datasets. Their method was proven effective since it achieved 2.62% Equal Error Rate when the six gestures were combined. At the same time Serwadda et al. [148], compared 10 classification algorithms based on their performance for touch gestures. They collected data by two self-developed Android applications while users scrolled/swiped back and forth in landscape and portrait orientation of the screen and computed 28 features to represent a stroke. The logistic regression classifier achieved the lowest mean EER of 10.5%, whereas the J48 tree classifier achieved the highest mean EER of 42% across population.

Afterwards, Bo et al. [36] designed SilentSense which was a software-based decision mechanism for smartphones. This mechanism obtained information regarding the usage of applications and the interacting behavior with each application performed by the user from the system API and measured the device's reaction by using the motion sensors. The user was identified as the owner, or a guest based on his actions and the corresponding reaction of the device. The performance of SilentSense was evaluated in walking and static scenarios and achieved over 99% identification accuracy. Both false rejection (FRR) and false acceptance rates (FAR) were lower than 1% after collecting only 10 actions. In addition, they achieved significantly low error rates for user identification when they combined touch signatures with walking patterns. At the same time, Xu et al. [37] used the keystroke, slide, handwriting and pinch operations on the touchscreen of a smartphone to authenticate users. The best performance achieved by their system was lower than 1 % EER for the slide operation, while for all operations it achieved an EER lower than 10%. Simultaneously,

Feng et al. [66] presented an application named TIPS, for the authentication of users based on the location of touch, and the length and curvature of swipe on the touchscreen of three different brands of smartphones. For classification they combined Dynamic Time Warping (DTW) with the One Nearest Neighbor (1NN) classifier and achieved approximately 90% accuracy. Apart from the performance evaluation of their touch- based authentication application they also calculated its power consumption which was 88 mW on average and the battery usage was approximately 6.2%.

Following, Buriro et al. [39] built a system that profiled the user based on his/her finger movements on the touchscreen while signing or writing and the movements of the device. They tested their mechanism on a dataset of 30 volunteers and achieved a True Acceptance Rate (TAR) of 95% with a False Acceptance Rate (FAR) of 3.1% by using a Multilayer Perceptron (MLP). Also, they measured the power consumption and the required time for authentication of their system which was approximately 1000mW and 0.215 0.250s, respectively. Filippov et al. [96] built an authentication system using the data resulting from the interaction of twenty-one users with the touch screen of a smart- phone. They gathered 2000 features from seven different gesture types of swipe while users interacted with the smartphone. Their system was evaluated with the use of the Isolation Forest method and achieved values of FRR and FAR equal to 6.4% and 7.5%, respectively. Moreover, their system was able to detect the illegitimate user in seven performed actions.

Shen et al. [104] collected touch data from 102 subjects during three different operation scenarios. More specifically participants hold the smartphone and performed touch actions while sitting, standing still or walking, or they used one hand for the touch operations while the smartphone was placed on a desktop. The best performance among all three operation scenarios was achieved when participants hold the smartphone and performed touch actions while sitting or standing still. More specifically, the FAR was 3.98%, the FRR 5.03%, and the EER 4.71%. They also evaluated the battery, memory, and computation cost of their application and reported that it consumed less than 4.5% of battery per-day, 5.6 Mbytes of memory and it took approximately 110 ms to authenticate a user. Debard et al. [106] proposed

the Convolutional Neural Networks, which used 2D filters for the recognition of touch gestures on a touch surface. They used a dataset of 6591 touch gestures from 27 individuals. They compared the performance of their method to the performance of the methods provided by Hochreiter et al [172] and Liu et al [173] who used the LSTM classifier. The Convolutional Neural Networks classifier used by Debard et al. [106] achieved 89.96% accuracy while the LSTM classifier achieved 73.10% and 87.72% in the works of Hochreiter et al [172] and Liu et al [173], respectively.

Yang et al. [126] used behavioral biometrics of touch and based on anomaly detection they developed a CA method for security-sensitive mobile applications named BehaveSense. Their study was based on the fact that only a few applications contain sensitive data. They used touch gestures of click and slide. They collected 250,000 touch operations in total while 45 participants used the application "WeChat". For classification they used Isolation Forest and One-class SVM Method. For the sequence of touch operation their method achieved an average accuracy of 95.85% when considering 9 touch operations. They also calculated the energy consumption of their method which was 6.82 mAh, while the average calculating time was less than 0.01 seconds.

Alqarni et al. [181] used the accelerometer and gyroscope sensors of a smartphone to collect data resulting from keystroke dynamics, touch gestures, and hand waving. They divided their data into two groups, namely short-term activities and gestures. Data from the short-term activities included the data collected while participants were using a smartphone and executed specific typing and hand waving tasks. Data from gestures included data that were collected while participants were holding the smartphone in their hand and performed predefined swiping, drawing, and hand waving gestures. They evaluated their method by using 3 different classifiers, namely SVM, Random Forests, and Bayes Net. Regarding the group of short-term activities, the best performance was achieved while participants typed a predefined sentence. More specifically, they achieved 76.20% accuracy, and 0.133 RMSE, by using the Random Forest classifier. Regarding the group of hand gestures, the best performance was achieved while participants performed two different gestures. The first

gesture was the drawing of a circle with their right hand and the second was the drawing of a triangle with their right hand. In the first gesture, they achieved 92.81% accuracy, and 0.1218 RMSE, while in the second gesture, they achieved 92.81% accuracy, and 0.1178 RMSE. In both gestures, they used Random Forest for classification.

Table 4: Touch gestures modality research works.

Method	Publications	Classification	Performance (%)					
			FAR	TAR	Accuracy	FRR	EER	RMSE
Touch gestures	[32] in 2008	k-NN			99		1	
	[33] in 2012	k-NN & SVM					<4	
	[34] in 2013	SVM			>88.28			
	[35] in 2013	L1 distance					2.62	
	[148] in 2013	logistic regression					10.5	
	[36] in 2014	SVM	<1		99	<1		
	[37] in 2014	SVM					<1	
	[66] in 2014	Combination of DTW with 1NN			90%			
	[39] in 2016	MLP	3.1	95				
	[96] in 2018	Isolation Forest	7.5			6.4		
	[104] in 2018	HMM	3.98			5.03	4.71	
	[106] in 2018	CNNs			89.96			
	[126] in 2019	Isolation Forest			95.85			
	[181] in 2020	Random Forest			92.81			0.1178

3.5 Keystroke dynamics

Most techniques are based on a specific context with predefined text. Clark and Furnell [40] authenticated users based on the user's patterns of typing when entering text messages and telephone numbers. By using Multi-Layer Perceptron (MLP), Radial Basis Functions (RBF) and General Regression Neural Network (GRNN) classifiers, they achieved an average EER of 12.8%. In another study, Feng et al. [41] asked participants to enter 4-digit passwords during the log-in session and a predefined sentence of 20 characters during the post-login session. The keystrokes were collected by an Android application. The authentication performance during

the log-in session achieved an FRR approximately 11.0% using Bayes Net. In the post-login stage, the Random Forest algorithm outperformed the other two (8.93% vs 19.78% and 14.26%FAR). Simultaneously, Draffin et al. [44] collected keystrokes from 13 participants in a real-world study in a three weeks period. They did not intervene and collected 86000 keystrokes not restricted to passwords or predefined sentences. By using Feed Forward Neural Network for classification they achieved 86% accuracy after 15 keypresses with 14% FAR and 2.2% FRR.

Later, Buschek et al. [42] asked 28 participants to type 20 times 6 different passwords in non-specific order and in three different hand postures. By using the Least Squares Anomaly Detection, they achieved 17% EER when combining pressure with spatiotemporal features. Following, Zhang et al. [110] collected time and pressure-related data from 10 students while they typed the same password by using a self-prepared Android App. Their user authentication model was based on an RBF network and achieved 10.3% false positive rate and 91.7% true positive rate.

Kambourakis et al. [256], collected data from 12 individuals in two scenarios. In the first scenario, participants typed a predefined password where no mistakes were allowed. In the second scenario they typed a predefined phrase and mistakes were allowed. In both scenarios, the input process was repeated for 12 times for each individual. For the first scenario, the best results were achieved with Random Forest while for the second scenario, the best results were achieved with KNN. More specifically, the average FAR%, FRR%, and EER% values for the first and second scenarios were 12.5, 39.4, 26 and 23.7, 3.5, 13.6, respectively.

Darren and Inguanez [111] collected data from the input of 15 predefined sentences during four different typing scenarios. Participants could choose one of the four scenarios: One Handed Stationary, Two handed Stationary, One Handed Moving, Two handed Moving. All 4 activities had to be completed by the smartphone owner. All their results, using a Least Squares SVM classifier with RBF kernel, achieved around 1% EER, with one-handed scenario being the best at 0.44% EER, 100% accuracy, 0% FAR and 1 % FRR Krishnamoorthy [43] classified users based on keystroke dynamics, by applying machine learning concepts. Participants typed

a specific password to record their typing characteristics. She effectively identified each of 94 users who participated achieving an identification accuracy of 98.44% when using the random forest classifier.

Table 5: Keystroke dynamics modality research works.

Method	Publications	Classification	Performance (%)				
			FAR	TAR	Accuracy	FRR	EER
Keystroke Dynamics	[40] in 2006	MLP, RBF, GRNNs					12.8
	[41] in 2013	RF	8.93				
		J48	19.78				
		Bayes	14.26			11.0	
	[44] in 2013	FFNN	14		86.0	2.2	
	[42] in 2015	LSAD					17.00
	[110] in 2016	RBF		91.7		10.3	
	[256] in 2016	Random Forest	12.5			39.4	26
		KNN	23.7			3.5	13.6
	[111] in 2018	SVM	0		100	1	0.44
	[43] in 2018	RF			98.44		2.2

3.6 Behavioral profiling

Neal et al. [50] developed a method to profile users based on Blue- tooth sightings, Wi-Fi access points and application usage. To produce matching scores, they utilized a categorical nearest-neighbor classifier. They achieved 80% identification rate when using Bluetooth, 93% when using Wi-Fi, 77% when using applications and 85% when combining the features. Following, Anjomshoa et al. [115] presented TrackMaison, a mobile application tool, which kept track of the manner smartphone users made use of five social network services via the usage of data, the usage frequency, the location and session duration. By using their tool, they conducted a study on several user profiles in Instagram and showed that users which are highly active can be identified with 3% FAR.

Fridman et al. [118] suggested an authentication method that regards the user's application and website logs, the keystroke dynamics and the location of the device as defined from the Wi-Fi or the GPS. Their data collection involved behavioral biometrics from 200 participants

who used their smartphone for 30 days. They used the support vector machines (SVMs) and the equal error rate (ERR) achieved by their authentication system was 1% after 30 minutes of interaction and 5% after 1 minute.

Later, Mahbub et al. [119] used unique application usage data and handling the unexpected events in the data. They collected data for approximately six months, from 218 participants. These data included the device location, the installed, removed or updated applications, the currently running foreground application, etc. They divided their dataset into three categories, namely: *"all observations"* category, *"all except the ones with unknown applications"* category and *"all without un-foreseen observations"* category. The number of training samples that they used were 500. By using the M-ED algorithm their method achieved an EER of 34.31% in the *"all observations"* category, 42.47% in the *"all except the ones with unknown applications"* category and 43.29% in the *"all without unforeseen observations"* category. Moreover, their method detected an intrusion in 2.5 minutes of application use.

Alotaibi et al. [162] employed the usage patterns of specific applications to identify and verify users on mobile phones. More specifically, they collected data from 100 individuals while they used their device as usual, and employed the applications of Phone Call, SMS, Download, YouTube, WhatsApp, Browser, Google Play, Email, Viber, Google Photo, Camera, and Yahoo mail. Each individual participated in the data collection procedure for one month. Their approach succeeded in successfully identifying users by their behavioral profiling, with 26.98% average EER and the Gradient Boosting Classifier.

Pang et al [180] developed an application to collect data from seven modalities from a smartphone, namely, LOCATION, ACTIVITY, APP, BLUETOOTH, WiFi, CALL, and SMS. They evaluated the performance of their approach by using different classifiers. The best results were achieved with the MineAuth method which was 98.5% accuracy. The authors also measured the running time, the power consumption, the CPU, and memory usage of their approach. They reported that the total running time was 90.601 ms. More specifically, the running time for behavior construction was 87,759 ms, for habits mining and authenticator it

was 2310 ms, while for the decisionmaker it was 532 ms. The total power consumption was 0.37%. More specifically, the power consumption for behavior construction was 35% MB, for habits mining and authenticator it was 0.01%, while for the decisionmaker it was 0.01%. The total CPU usage was 46.85%. More specifically, the power consumption for behavior construction was 15.30%, for habits mining and authenticator it was 16.10%, while for the decisionmaker it was 15.45%. The total memory usage was 186,29MB. More specifically, the memory usage for behavior construction was 75.10 MB, for habits mining and authenticator it was 60.2 MB, while for the decisionmaker it was 50.99 MB.

Table 6: Behavioral profiling modality research works.

Method	Publications	Classification	Performance (%)		
			FAR	Accuracy	EER
Behavioral profiling	[50] in 2015	Categorical Nearest-Neighbor		93	
	[115] in 2016	KNN	3		
	[118] in 2017	SVMs			1
	[119] in 2018	M-ED algorithm			34.31
	[162] in 2019	Gradient Boosting			26.98
	[180] in 2019	MineAuth method		98.5	

3.7 Hand waving

Sitová et al. [38] used Hand Movement, Orientation, and Grasp (HMOG) to continuously authenticate smartphone users. They used readings from the accelerometer, gyroscope, and magnetometer sensors to capture orientation features and subtle micro-movement as the user grasps, holds, and taps on the smartphone. They evaluated their mechanism by collecting data under both walking and sitting circumstances. They achieved 7.16% EER when walking and 10.05% when sitting by combining HMOG, keystroke features and tap. Also, they measured the energy consumed by their system to compute the 18 HMOG features from the magnetometer, accelerometer and gyroscope sensor readings which was 0.08 joules.

Yang et al. [100] employed the waving patterns to lock and unlock the smartphone in a system named OpenSesame. They collected data from 200 subjects and used an SVM classifier. The result from their experiment achieved 15% mean FAR while the FRR <8%.

Later, Buriro et al. [98] developed an authentication mechanism by using the micromovements of the user's hand(s) within a few seconds after unlocking his smartphone. They collected data from the smart- phone sensors and more specifically from the gyroscope, the accelerometer, the gravity, the orientation and the magnetometer. On a dataset of 31 volunteers their mechanism achieved a 96% TAR at 4% EER using the Random Forest classifier.

Table 7: Hand waving modality research works.

Method	Publications	Classification	Performance (%)			
			FAR	TAR	FRR	EER
Hand waving	[38] in 2015	SVM				7.16
	[100] in 2015	SVM	15		8	
	[98] in 2017	Random Forest		96		4

3.8 Power consumption

Zhang et al. [15] presented Power Tutor, a power consumption monitoring model on electronic devices which utilized the battery sensors. The absolute average error rate achieved by their model was lower than 10%. Murmuria et al. [130] showed that the operation state of a smartphone's device driver affects its power consumption. They succeeded in attributing power consumption to applications with lower than 4% error rate by using the Ordinary Least Squares regression analysis. More specifically for the applications Logger, Music, Sound Recorder and GPSTracker the EERs were 3.69 %, 1.27 %, 0.74 % and 3.68% respectively.

Shye et al. [129] presented a model to estimate power that was tested on 20 users for more than a week. They used a self-developed logger application to record the activity of users and showed that power consumption patterns are differentiating greatly among users. They found

that this approach was not effective since they could not profile users on the basis of power consumption patterns.

Murmuria et al. [86] used a machine learning based approach that involved three different modalities: power consumption, physical movement and, touch gestures to continuously monitor users. They collected data from 73 participants while they used facebook and chrome. They applied the Strangeness-based Outlier Detection algorithm for each modality and achieved an EER that ranged from 6.1% to 6.9% depending on training times that varied between 20 and 60 minutes and sufficient data. They deployed their approach and created the kryptowire system which is available on the market [51]. This application employs the embedded sensors of mobile devices including power consumption, physical movement and, touch gestures to identify users based on the way they interact with their device and within the context of each mobile application.

Table 8: Power Consumption modality research works.

Method	Publications	Classification	Performance (%)
			EER
Power Consumption	[15] in 2010	PowerTutor model	>10
	[130] in 2012	OLS	>4
	[86] in 2015	StrOUD	6.1

3.9 Fusion

Saevanee et al. [24] conducted a study where they first employed behavior profiling, keystroke dynamics and linguistic profiling as single modalities to discriminate users and achieved error rates of 20%, 20% and 22% respectively. Following, they combined behavior and linguistic profiling with keystroke dynamics by applying matching-level fusion and increased the reliability of continuous authentication systems with an overall EER of 8% with MLP classifier.

Later, Zheng et al. [52] combined four features for a PIN typing action on a smartphone touch screen (acceleration, pressure, size, and time). They collected tapping data from

more than 80 users and they first evaluated the performance of the modalities as single modalities and following they measured the results of fusing these modalities. The fusion achieved better results in comparison to the single modalities results. More specifically, the size modality, as a single modality achieved 27% EER, the pressure modality achieved 16% EER, the time modality achieved 14% EER, and the acceleration modality achieved 10% EER. When they combined the modalities of size, time and acceleration they achieved 3.65% EER with k-NN classifier.

Buriro et al. [53] used features collected from 26 participants while they unlocked a smartphone before answering a call. They collected features of slide swipe, the manner of moving the arm while carrying the device towards the ear and recognition of voice. They first evaluated the modalities as single modalities and achieved 22.28% FAR and 4.84% FRR for the slide modality, 26.69% FAR and 6.19% FRR for the pickup modality and 63.92% FAR and 12.69% FRR for the voice modality. In their multimodal system they incorporated the features of slide and pickup and enhanced the unimodal result, with 11.01% FAR and 4.12% FRR while the final HTER was 7.57% using the BayesNet classifier. The computation time required for the same classifier was 64, 762 and 205 ms for the slide, pick up and voice modalities respectively.

Kumar et al. [134] investigated if arm movements while walking can be used for user authentication. In their experiments, they used the accelerometer and the gyroscope sensors of a smartwatch to extract 32 acceleration and 44 rotation features respectively. They used the rotation and acceleration of arms and their fusion at the feature level to build three different continuous authentication designs. They implemented these designs by four classification algorithms resulting in twelve authentication mechanisms and tested these mechanisms in three different environments where participants wore the smartwatch on their wrist and walked naturally. They first evaluated the performance of the modalities as single modalities and achieved a mean dynamic FAR of 2.6% and a dynamic FRR of 4.3% for the acceleration modality and 4.2% dynamic FAR and 10.5% dynamic FRR for the rotation modality. Following they deployed score level fusion at the feature level with the k-NN classifier and

the best results achieved were 2.2% dynamic FAR and 4.2% dynamic FRR in the inter-phase environment. The authors also reported the number of features vectors that were in the training data set which was 156 for both the authentic and impostor users.

Shrestha et al. [64], applied a multi-modal walking biometrics approach, namely Walk Unlock ZIA(WUZIA) on a Zero-Interaction Authentication (ZIA) system. ZIA is a paradigm where a legitimate user caries a prover device and walks towards a verifier device which unlocks automatically [49]. They used the accelerometer, gyroscope and magnetometer of a smartphone and a smartwatch to collect data from 18 individuals. The smartphone was placed in their pocket to record hip movement and the smartwatch was worn on their wrist to record hand movement. Participants walked towards the verifier device which would unlock and respond to the prover device only after it detected the legitimate user' s walking patterns. First, they evaluated the performance of the watch which achieved 0.46% FRR and 0.63% FAR and the phone which achieved 0.18% FRR and 0.36% FAR. Following they combined the watch with the watch and achieved the almost error free FRR of 0.2% and FAR of 0.3% on average with the Random Forest classifier. Their results showed that their approach detected with high accuracy a legitimate or a non-legitimate user when using both of the aforementioned devices. ZIA systems are already deployed in several real-world applications like BlueProximity [174], Keyless-Go [175], PhoneAuth [176], and access control systems based on wearable devices like the iWatch [177]. BlueProximity [174] enables the unlocking of a computer screen when the user approaches the computer and holds a mobile device. Keyless-Go [175], allows users to start and lock their car just by having the key with them. PhoneAuth [176], is deployed based on the scenario where users, for example, walk towards an Internet kiosk to navigate to a web page and they type their username and password to log in. Following, PhoneAuth stores the cryptographic credentials on the user's phone. If the phone is present when the user logs into a site, then it will ascertain the user's identity via Bluetooth with the computer's browser. The iWatch [177] when it is in close range to iPhones and Macs it allows the legitimate user to log in without using a pin or a password. Hence, WUZIA can be implemented in a traditional ZIA system such as BlueProximity [174], Keyless-Go [175], PhoneAuth [176], and the

iWatch [177]. More specifically WUZIA can be implemented in BlueProximity [174] simply by changing the app and without changing the terminal software. WUZIA can also be implemented on systems like Keyless-Go [175] where the key has incorporated RF capability and processor.

Haq et al. [121] applied micro-environment sensing to build a three-class smartphone user classification scheme based on physical activity recognition. They employed time and frequency domain features to recognize physical activities such as walking, running, etc. They used a probabilistic scoring model to recognize the activity patterns and subsequently classify users as authenticated, restricted access user or guest user (supplementary) and impostor. Their scheme granted full access to authenticated users, restricted access to supplementary users and zero access to impostors. For their experiments they used a dataset created by Shoaib et al. [120,123]. To enhance their authentication scheme, they took into account the work of Yang et al. [124] regarding the smartphone's position sensitivity issue and incorporated micro-environment sensing, meaning the awareness of the smartphone's close surroundings. For this purpose, they selected five different body positions to place the smartphone while users performed physical activities. The body positions were the wrist, the upper arm, the waist, the left and right thigh, and were considered as the smartphone's close surroundings. Their authentication model was trained not only to sense the smartphone's position on the human body but to also combine it with the performed physical activities of each user. First, they evaluated the modalities as single modalities and reported that they achieved an average accuracy of 97.55% when the smartphone was placed to the waist, 98.57% when the smartphone was placed to left thigh, 98.01% when the smartphone was placed to right thigh, 95.45% when the smartphone was placed to the upper arm, and 96.85% when the smartphone was placed to the wrist. Following, they combined data from the accelerometer, gyroscope and magnetometer sensors and achieved an average accuracy rate of 97.38% by the Bayes Net classifier where the average error rate was 0.027 MAE and 0.086 RMSE. They also reported that the best TAR achieved was 0.95 for the impostor with the smartphone placed in his waist and the best FAR was 0.03 and achieved for the supplementary user when the smartphone was place on his waist and his left thigh. They also measured the energy

and storage cost of their application and reported that it consumed between 5% and 11.2% of energy depending on how frequently the users were moving and maximum 1.8 MB of storage per day. In addition, they measured the required time for the BayesNet classifier to perform authentication and reported that it was 5.61 seconds.

Li and Bours [122] developed a mobile application authentication method in which they collected and analyzed data from four resources: gyroscope and accelerometer sensors, Bluetooth, and Wi-Fi. With the scores from the aforementioned resources they performed a score-level fusion. The 321 participants who joined the experiment were free to choose when and where they would open the App while performing seven different activities and carrying the smartphone at a different position. For the gyroscope features the EER achieved was 28.12% while for the accelerometer features the EER achieved was 36.11%. The best EER achieved by their method was 9.67% for the score-level fusion with data from all four resources and Random Forest classifier.

Later, Buriro et al. [125] built an authentication mechanism named AnswerAuth that was based on the behavioral biometrics of smartphone users. More specifically, AnswerAuth utilized the manner users slide the screen's lock button to unlock the smartphone and bring it close to their ear. Data were recorded by using the incorporated sensors of the smartphone, i.e., touchscreen, accelerometer, gyroscope, gravity and magnetometer. Their dataset derived from 85 individuals while they unlocked the smartphone in three different positions, namely walking, standing, and sitting. They reported that the best results achieved were the fusion of the slide operation with the bringing the device towards to the ear while users were standing. Specifically, they achieved a TAR of 99.35% and 98.98% accuracy by using the Random Forest (RF) classifier.

At the same time, Volaka et al. [178] used the touch-screen data(scroll), and data from the accelerometer and the gyroscope sensors from the HMOG dataset, as provided in the work of Sitova et al. [38]. First, they evaluated only the touch-screen data using the LSTM classifier and achieved an average accuracy of 88%, an average TAR of 78-79%, and an EER of 16%. Following, they evaluated the combination of touch-screen data and data from the

accelerometer and achieved an average accuracy of 89%, an average TAR of 79%, and an EER of 16%. Next, they evaluated the combination of touch-screen data and data from the gyroscope and achieved an average accuracy of 89-90%, average TAR of 80-81%, and an EER of 14%. Finally, they evaluated the combination of touch-screen data and data from the gyroscope and the accelerometer and achieved an average accuracy of 88%, an average TAR of 78%, and an EER of 15%.

Simultaneously, Lamiche et al. [179] used the gait patterns resulting from the accelerometer and the keystroke dynamics while 20 users walked and typed a predefined sentence. They evaluated their method under four different scenarios, by using different classifiers, and by applying a feature level fusion method to profile users by using both modalities of walking gait and keystroke dynamics. In the first scenario, users walked naturally while the smartphone was placed in the pocket of their trouser and achieved 96.54% accuracy and 9% EER with the Random Forest classifier. During the second scenario, users walked naturally while they were holding the device on their hand and they achieved 97.34% accuracy and 6% EER by using the Random Forest classifier. In the third scenario, users answered a phone call while they were walking and achieved 98.1% accuracy and 0.3% EER with the Random Forest classifier. During the fourth scenario, users typed a predefined sentence while they were walking and they achieved 99.11% accuracy, 0.684% average FAR, 7% FRR, and 1% EER by using the Multilayer Perceptron (MLP) classifier.

Following, Abuhamad et al. [182] presented a continuous authentication method based on deep learning, named AUToSen. The performance of their method was evaluated by using LSTM on four different sets of data. The data collected included touch screen data such as sliding or tapping while participants interacted with their smartphones, and sensor data from the accelerometer, the gyroscope, the magnetometer, and elevation, while the individuals performed various physical activities. These data were divided into four groups. The first group included data from the accelerometer, the gyroscope, the magnetometer, elevation, and touch screen data. The second group included data from the accelerometer, the gyroscope, the magnetometer, and elevation. The third group included data from the accelerometer, the

gyroscope, and the magnetometer, while the fourth group included data from the accelerometer and the gyroscope. The authors showed that their method achieved 0.41% EER, 0.95% FAR, and 6.67% FRR, by using sensory data of one second, from only three sensors, namely the accelerometer, the gyroscope, and the magnetometer.

Table 9: Fusion research works.

Method	Publications	Classification	Performance (%)							
			FAR	TAR	Accuracy	FRR	EER	MAE	RMSE	HTER
Fusion	[24] in 2011	MLP					8			
	[52] in 2014	k-NN					3.65			
	[53] in 2015	BayesNet	11.01			4.12				7.57
	[134] in 2016	k-NN	DFAR 2.2			DFRR 4.2				
	[64] in 2016	Rand. Forest	0.3			0.2				
	[121] in 2017	Bayes Net	0.03	0.95	97.38			0.027	0.086	
	[122] in 2018	Random forest					9.67			
	[125] in 2019	Random Forest		99.35	98.98					
	[178] in 2019	LSTM		78	88		15			
	[179] in 2019	MLP	0.684		99.11	7	1			
	[182] in 2020	LSTM	0.95			6.67	0.41			

3.10 Discussion on behavioral biometrics

In this section, a discussion on the machine learning and deep learning models that were previously presented is made. Of course, there are corresponding interesting research works in the field of IoT Environments as well as for wearable devices, e.g. [252, 253, 254], but which will not be presented in detail since they are outside the research area of this thesis. Unfortunately, a comparison of the performance of machine learning algorithms cannot be

made given in the literature because researchers use different evaluation criteria and different kinds of data to evaluate machine learning algorithms. However, the best results achieved in each category are presented. Moreover, a summary of some advantages and disadvantages of the Methods is made as shown in table10. A discussion on each modality follows:

- *Gait:* As shown above, the walking gait modality can be efficiently used to transparently and continuously authenticate individuals as this modality sufficiently discriminates different users by their gait characteristics [31]. An accuracy of 99.95% was achieved by using the Long Short-Term Memory (LSTM) Recurrent Neural Networks classifier [102]; while an EER of 0.17% and 0.13% was achieved by applying the Manhattan method [101], and the MLP classifier [31] respectively. In addition, the walking gait modality can work without user intervention or additional hardware apart from the smartphone embedded components. However, movements of users while walking, for example the MDP motion (the movement of picking up their phone to the ear), strongly affects the accelerometer data and the verification performance [29].This is due to Einstein's principle of equivalence [45] according to which the acceleration data incorporates the effect of motion acceleration as well as the gravity acceleration. To solve this, Feng et al. [29] removed the accelerometer data and emphasized on gyroscope and magnetometer data and increased the performance result. An additional disadvantage is that the accuracy can be negatively affected due to the uneven ground, possible injuries, footwear, fatigue, personal peculiarities, etc. [86]. As highlighted in the work of Shila et al. [106] machine learning techniques are used in the design of walking biometrics and current methods are either based on feature extraction for model training or they cannot learn the time series data. Thus, they constitute a major challenge, leading to an increased number of false positives and false negatives. To extract temporal features and successfully classify users, they used a deep learning architecture, namely LSTM (Long Short-Term Memory) Recurrent Neural Net- works. In the same work, they also compared the performance of LSTMs to CNNs and reported that while both achieved an excellent performance, the latter are more difficult to train since they required four hours while the former only thirty minutes.

- *Touch gestures:* The touch gestures modality combines several touch operation patterns and achieves very good results. The k-NN and the SVM classifier achieved 99% accuracy in the works of [32] and [36] respectively, while SVM and Isolation forest classifiers achieved an average accuracy of 95.85 [126]. Subsequently, touch biometrics hold much promise as a method for the passive and continuous authentication of individuals [37]. Moreover, for the collection of data no additional equipment is required except for the incorporated device sensors. When an individual performs touch gestures the dynamic nature of this action results in a test sample that can in part noticeably vary from prior training samples of the same individual. For this reason, an authentication system might reject the testing sample, in case it expects an individual to perform the gestures in the same manner [137]. A dataset that contains millions of samples is necessary to realistically evaluate the performance of an authentication system based on touch gestures [11]. So far, the biggest sample comprises of 250,000 touch operations [126]. Debard et al [102] mentioned the issue of sequential data classification in touch gestures that present different sums of data per time. They used Convolutional Neural Networks (CNN) and improved the recognition rate in comparison with the commonly used Recurrent Networks. More specifically, Debard et al. [106] achieved 89.96% accuracy while the LSTM classifier achieved 73.10% and 87.72% as reported in the works of Hochreiter et al. [172] and Liu et al [173], respectively.
- *Keystroke:* The authentication of users with the use of keystroke dynamics modality requires no additional equipment apart from the built-in sensors of the device. In addition, it is non-intrusive and efficient in capturing the users' patterns without disturbing them. Moreover, the results of the authentication of users with the use of keystroke dynamics modality are of high accuracy. The SVM and the Random forest classifier achieved an EER of 0.44% and 2.2% in the works of [111] and [43] respectively; while the RBF classifier achieved 91.7% TAR [110]. A disadvantage of an authentication system based on keystroke dynamics is the inconsistent performance if users perform inconsistently.
- *Behavioral profiling:* The behavioral profiling approach is based on the assumption that the majority of users tend to perform similar tasks due to their habitual nature [77].

Thus, in case users interact inconsistently with their mobile phones results in unreliable performance which constitutes a major deficiency [11]. Nevertheless, the results of the authentication of users with the use of behavioral profiling are of high accuracy. The SVM classifiers achieved 1% EER in the work of [118], while in the work of [180] the MineAuth method achieved 98.5% accuracy. The KNN achieved 3% FAR. The CNN achieved 93% accuracy and the M-ED algorithm achieved an EER of 34.31%. Finally, this method does not require any additional hardware apart from the embedded smartphone components.

- *Hand-waving:* Regarding the hand-waving modality very little research is conducted. The random forest classifier has achieved 4% EER in [98]. This approach does not involve any user interaction. For the collection of motion data, no additional equipment is necessary except for the incorporated device sensors.
- *Power consumption:* The power consumption modality cannot be used to efficiently profile users as a single modality [129], but only in combination with other behavioral biometric modalities [86]. The measurement of power consumption resulting from the user's activities does not require any additional equipment apart from the incorporated sensors of the device's battery driver [15]. An EER smaller the 4% was achieved by using the OLS classification [130].
- *Fusion*: A plethora of combinations is used for the authentication of individuals with the fusion of biometrics, which achieves improved results compared to single modality methods [24,52,53,64,122, 134]. For example, in [24] the behavior profiling, the keystroke dynamics and the linguistic profiling as single modalities achieved error rates of 20%, 20% and 22% respectively. When combined by applying matching-level fusion the reliability of the system increased with an overall EER of 8%, with MLP classifier. In [52] the modalities of size, pressure, time and acceleration achieved EERs of 27%, 16%, 14%, and 10% respectively as single modalities and when they were combined, the EER was 3.65% with k-NN classifier. In the work of [53] when they evaluated the modalities as single modalities, they achieved 22.28% FAR and 4.84% FRR for the slide modality, 26.69% FAR and 6.19% FRR for the pickup modality and 63.92%

FAR and 12.69% FRR for the voice modality. When they incorporated the features of slide and pickup into their multimodal system, they enhanced the unimodal result, with 11.01% FAR and 4.12% FRR using the BayesNet classifier. In the work of [134] the performance of the modalities as single modalities achieved a mean dynamic FAR of 2.6% and a dynamic FRR of 4.3% for the acceleration modality and 4.2% dynamic FAR and 10.5% dynamic FRR for the rotation modality. When the authors deployed score level fusion at the feature level with the k-NN classifier they achieved 2.2% dynamic FAR and 4.2% dynamic FRR in the inter-phase environment. In the work of [179] they achieved 99.11% accuracy, 0.684% average FAR, 7% FRR, and 1% EER by using the Multilayer Perceptron (MLP) classifier, while users were walking and typed a predefined sentence. In the work of [64] the evaluation of the performance of the watch achieved 0.46% FRR and 0.63% FAR, while the phone achieved 0.18% FRR and 0.36 % FAR. When they combined the watch with the watch, they achieved the almost error free FRR of 0.2% and FAR of 0.3% on average with the Random Forest classifier. In the work of [122] the gyroscope and the accelerometer features achieved EERs of 28.12% and 36.11%, respectively. When the author applied score-level fusion with data from all four resources and Random Forest classifier they achieved 9.67% EER. The only work where a single modality achieves better results in comparison with fusion results is the work of Haq et al. [121]. Specifically, when the authors evaluated the modalities as single modalities they reported that average accuracy achieved was 97.55% when the smartphone was placed to the waist, 98.57% when the smartphone was placed to left thigh, 98.01% when the smartphone was placed to right thigh, 95.45% when the smartphone was placed to the upper arm, and 96.85% when the smartphone was placed to the wrist. When they combined data from the accelerometer, gyroscope and magnetometer sensors they achieved an average accuracy rate of 97.38% by the Bayes Net classifier. As it is shown, the single modalities of the smartphone being to the upper arm or when it is placed to the wrist achieved better results. The random forest achieved 99.35% TAR in [125]. The random forest classifier also achieved very good results in the deployment of WUZIA [64] scoring 0.2% FRR and 0.3% FAR on average. A drawback of the WUZIA approach is that it incorporated the use of a smartwatch as an

additional token. The collection of data requires no additional equipment apart from the built-in sensors of the device. Compared to unimodal biometric systems these systems are evoking interest regarding their implementation in large scale authentication systems even though they involve more computational cost, they take higher processing time and require more storage [138, 139].

Table 10: Advantages and disadvantages of each method.

Methods	Advantages	Disadvantages
Walking Gait	Continuous Authentication. Can work without user intervention. Doesn't need additional hardware.	The verification performance is greatly affected by Mobile Device Picking-up (MDP) motion of users. Accuracy can be negatively affected due to uneven ground, possible injuries, footwear, fatigue, personal peculiarities, etc.
Touch Gesture	Continuous Authentication. A promising method. Doesn't need additional hardware.	Noticeable variations in the testing sample Research is conducted on small-scale samples.
Keystroke dynamics	Continuous Authentication. Doesn't need additional hardware. Doesn't disturb users. High accuracy of results.	Doesn't work well if users perform inconsistently.
Behavioral profiling	Continuous Authentication. Doesn't need additional hardware.	Doesn't perform well if users perform inconsistently.
Hand waving	Continuous Authentication. Does not require any interaction. Doesn't need additional hardware.	Very little research is conducted.
Power consumption	Continuous Authentication. Doesn't need additional hardware.	Cannot profile users solely on this basis.
Fusion	Continuous Authentication. Achieves improved results. Doesn't need additional hardware.	Require more storage. More processing time. Higher computational and power cost.

As it is shown, most of the works presented in this chapter are using the zero-effort evaluation approaches to test the performance of their authentication systems. The zero-effort attack is based on the sufficient similarity of the templates between the attacker and the legitimate user and relates to the uniqueness property of a biometric characteristic. It does not involve any sophisticated action by the adversary. An adversary attack involves sophisticated action by

the attacker to successfully impersonate a legitimate user. The level of sophistication strongly depends on the available resources such as digital or physical means, time, and information regarding the biometric system and the victim [95]. Therefore, there is a need to shift from the zero-effort to high-effort evaluation approaches to see the actual performance of the systems under the spectrum of today's possible threats. In addition, user behaviors and habits may change over time, thus authentication systems should be able to adapt to these changes. A paradigm that could be employed towards this direction is Continual Learning [163, 167, 168]. This framework can train successfully deep discriminative models as well as deep generative models in complex continual learning scenarios where new tasks appear, and existing tasks change over time.

Also, most researchers employ commonly used machine learning techniques, and only a few used deep machine learning. Debard et al. [106] employed CNNs in the category of touch gestures and Shila et al. [102] used LSTMs and CNNs in the category of walking gait. Therefore, it is impossible to make a comparison between them since they are only a few and they belong to different categories of behavioral biometrics. In the work of Shila et al. [102] they showed that LSTMs are faster to train that CNNs but they both performed excellently.

Finally, there are several additional aspects of machine learning on mobile devices that should be taken into consideration when evaluating an authentication approach. These aspects include the amount of data from each user that is necessary for each approach to be effective, the computational and communication cost, and the usage of battery, memory, and CPU. However, most researchers do not measure these aspects in their works. Still, a presentation of all the research work that measure these aspects their results is made in table 11, that follows. Future research should measure those aspects to enable a comparison of each method based on these aspects. Moreover, researchers should at least weight and report the FAR, TAR, FRR, EER, and Accuracy when evaluating the performance of their approach. Also, they should measure and report additional aspects of machine learning such as the amount of data from each user that is necessary for each approach to be effective, the computational and communication cost, and the usage of battery, memory, and CPU. In this way, it will be feasible to make a comparison between the approaches.

Table 11: Research works that measured additional aspects of machine learning.

Method	Publications	Classification	Performance							
			Computation time for authentication	Memory usage	CPU usage	Battery consumption	Necessary amount of data for training	Necessary duration of training	Necessary amount of features for authentication	Necessary amount of data samples for authentication
Walking gait	[102] in 2018	LSTM					60K samples	20 minutes		
	[159] in 2019	Random forest							37	100
Touch gestures	[34] in 2013	SVM	17 ms			88 mW on average				
	[66] in 2014	DTW with 1NN				≈ 6.2%				
	[39] in 2016	MLP	0.215-0.250s			1000mW				
	[104] in 2018	HMM	110 ms	5.6 Mb		4.5%				
	[126] in 2019	Isolation Forest	0.01 s			6.82 mAh				
Behavioral profiling	[119] in 2018	M-ED algorithm					500 samples			
	[180] in 2019	MineAuth method	532 ms	186,29Mb	46.85%	0.4%		87,759 ms		
Power consumpti	[86] in 2015	StrOUD						20 - 60 min		
Fusion	[134] in 2016	k-NN							156	
	[121] in 2017	BayesNet	5.61 s							

3.11 Possible attack vectors on BBCA systems

As mentioned previously, there is a need to shift from the zero-effort to high-effort evaluation approaches to see the actual performance of machine learning and deep learning models under the spectrum of today's possible threats. In this section a review on possible attack vectors on CA systems is made.

3.11.1 Practical attack techniques

A behavioral biometric system could face several threats such as malware and a form of shoulder surfing attacks, mimic, impersonation, spoofing, replay, statistical, algorithmic, robotics, etc. These attacks can be divided into two general categories zero-effort or passive

attacks and adversary or active attacks. The zero-effort attack does not involve any sophisticated action by the adversary. It is based on the sufficient similarity of the templates between the attacker and the legitimate user and relates to the uniqueness property of a biometric characteristic. An adversary attack involves sophisticated action by the attacker to success- fully impersonate a legitimate user. The sophistication level of an adversary attack strongly depends on the available resources such as digital or physical means, time, and information regarding the biometric system and the victim [95].

Biometric researchers focus more on mimicry attacks since they do not involve any modification of the authentication system or the device and can be launched easily and unnoticeably on any biometric-based authentication system. Three kinds of mimicry attacks can be launched in authentication systems that are based on behavioral biometrics namely, the zero-effort, the minimal-effort, and the high-effort mimicry attacks. In a zero-effort mimicry attack, imitators are randomly selected by the attackers either from or outside the database since they do not possess any information regarding the legitimate user. In minimal-effort mimicry attack, imitators are selected by the attackers according to specific criteria since they possess information regarding the legitimate user. In high-effort mimicry attacks, imitators are intensively trained to successfully mimic the legitimate user [134]. Following practical attacks and threats on walking gait, keystrokes and touch gestures are shown.

3.11.2 Attacks on walking gait

A number of studies examine the vulnerability of authentication based on the gait patterns of an individual. The studies presented here refer to passive zero effort impostor attacks, active impostor mimic at- tacks including minimal effort impersonation attacks [142] and attacks after training of the adversary [60,64,95]. The aforementioned attacks can be divided in two general categories passive or zero-effort attacks and active or adversary attacks. In an active attack the attackers try to be accepted by the authentication system. They use two ways either by changing their biometric in order to match another targeted person or by selecting a victim based on information, for example the closest in the database, to verify themselves against the template of this targeted person. Apparently, the attackers can combine both ways.

Gafurov et al. [142] set two different scenarios, namely a friendly and a hostile scenario and evaluated the performance of a gait authentication system based on wearable sensors. In both scenarios, they collected gait patterns by placing a wearable accelerometer sensor to the hip of test subjects. This method has been suggested, from the authors, for the unobtrusive authentication of users on mobile devices. During the friendly scenario, they experimented by launching a passive (zero-effort) attack. This means that individuals submitted their biometric characteristics as if they were trying to successfully verify themselves against their own templates, but in fact, their biometric characteristics were compared with a nonself template. Participants walked in their customary way and an EER of about 13% and a recognition rate of 73.2% was obtained by employing the averaged cycle method. During the second part they launched a minimal-effort impersonation attack where participants tried to imitate the walking manner of another individual after observation. Based on FAR error analysis the probabilities for impostors being successfully allowed access did not increase. Within the third part, they launched an attack based on the hypothesis that attackers were aware of their closest individual in the database. This means that attackers selected an individual whose gait was the most similar to theirs, which resulted in them becoming a great threat to the system.

Mjalaand et al. [133] extended the work of Gafurov et al. [142] by performing three differently structured scenarios, namely a friendly, a short-term and a long-term hostile that involved 50 individuals. The system's baseline performance within the friendly scenario was 6.2% in terms of EER. During the short-term hostile scenario, they selected seven individuals whose gait templates had a small distance between them. One of the participants acted like a victim while the other six tried to imitate him individually. The attackers' training lasted two weeks watching videos with the walking manners of the victim. The comparison between the gait templates of the victim and the attacker was made by employing the distance metric Dynamic Time Warping (DTW). Regarding the long-term hostile scenario, while the training was the same as in the short-term hostile scenario it was addressed to only one attacker and lasted six weeks. The conclusion on this part of the work was that the attacker's ability to learn how to walk like the victim does not improve even if he is long-term trained.

Kumar et al. [60] incorporated a digital treadmill in an attack scenario over a "baseline gait-based authentication system (GBAS)". First, they collected accelerometer readings to capture walking pattern from 18 individuals by using a smartphone. Then, they tested the performance of the GBAS on their dataset by using five different machine learning algorithms. The use of random forest achieved the best results, specifically the FAR was 6% and the FRR was 3%. Afterwards, they investigated the performance of the GBAS after three attack attempts. They trained impostors to imitate their victims by using a digital treadmill to control gait characteristics. Their attacks degraded GBAS' s performance significantly and achieved an increase in mean FAR regarding all attacks on all users for all classification algorithms. More specifically the increase in mean FARs were 544% for logistic regression, 549% for Bayes network, 580% for multilayer perceptrons, 590% for SVM and 742% for random forest. The random forest classifier had the most degraded performance where the FAR of 6% increased to 44.5%.

Muaaz and Mayrhofer [95] evaluated gait recognition security under a realistic imitation attack scenario. Five specialists in body movement mimicking acted as attackers and four smartphone users acted as victims. Attackers and victims were paired according to physical similarities such as age, weight, height, etc. The attack scenario was conducted in two different phases, the reenact and the coincide phase. During the reenact phase victims walked in normal pace with the smartphone placed inside their trousers pocket while attackers observed them. Following, attackers walked along with their paired victims to observe them more closely, and finally, they tried to mimic their victim's walking manner. During the coincide phase, the authors made an analysis on the attackers' imitation skills improvement while they Table walked close to their victims. In both phases the False Acceptance Rate achieved was 0% showing that attackers could not achieve sufficient scores and be allowed access to the system. Moreover, when attackers imitated the walking style of their target person, they lost their steps pace and impersonation became much more difficult in 29% of the attempts.

Shrestha et al. [64] conducted a three-fold evaluation of the use of walking patterns for addressing the vulnerability of a Zero Interaction Authentication (ZIA) system. First, they

designed and implemented a ZIA authentication system that used the sensors of a smartphone and a smartwatch to extract walking characteristics and authorize access. Then, they evaluated their authentication system under an imposter and a treadmill attack scenario. In the imposter attack scenario, the imposter possessed the legitimate user's smartphone and smartwatch and tried to mimic his walking pattern and fool the authentication system. In the treadmill attack scenario, the attacker used a treadmill to control gait characteristics and match the extracted features from the walking pattern of the legitimate user. Their results showed that when both devices were used, both attacks became hard to execute, achieving on average 4.55% FAR, even if the attacker's capabilities were high. Kumar et al. [134] in the authentication mechanism described previously evaluated the performance under the zero-effort or random attack without launching active attacks. The training of four classifiers included both genuine and impostor samples. In the intra-session environment, a 0% mean dynamic FAR and a 0% dynamic FRR was achieved by all mechanisms of authentication. In the inter-session environment, the best error rates achieved were 2.2% mean dynamic FAR and 4.2% dynamic FRR by the design based on feature level fusion with the k-NN classifier. In the inter-phase environment, the DFAR and DFRR were increased from 5.68% and 4.23% to 15.03% and 14.62% respectively by the deployment of the design based on fusion at feature level and k-NN classifier.

3.11.3 Attacks on keystroke dynamics

Several studies examine the vulnerability of authentication systems based on keystrokes. In this section a presentation of four types of attacks is made including the Frog-Boiling attack [151], the Algorithmic attack [150], Mimic attacks [83,146], and the Snoop-forge-replay attack [131]. Studies that use virtual screen keyboards are included [146,150,151] as well as physical keyboards [83,131] because they are similar and exhibit very interesting findings.

The Frog-Boiling attack systematically alters the templates of target uses by poisoning them via the template update mechanism to effectively direct them to a template which is selected by the attacker [47, 151]. The Frog-Boiling attack was used by Wang et al. [151]

to exploit a template update mechanism and poison the keystroke dynamics system user templates. The attack increased the verifiers' EERs from between 9.9% and 18.9% to between 19.1% and 63.6% as it transformed well-performing users into ill-performing users. Attackers with weak destination templates caused higher EER increases compared to attackers with strong templates.

Serwadda and Phoha [150] investigated how a keystroke-based authentication system performed when exposed to synthetic attacks that were mimicking the legitimate user. They statistically analyzed keystroke data collected from more than 3000 users over 2 years to mimic the target user. Based on the observed statistical traits they designed and executed algorithmic attacks over three keystroke verification systems that used a password. The attack synthetically generated the keystroke sequence that corresponded to the target user's profile. Their algorithmic attack increased the Z-score, Scaled Manhattan and Naïve Bayes verifiers mean EERs by between 28.6% and 84.4% in comparison with the zero-effort attacks which are commonly used to evaluate the keystroke-based biometric systems performance.

Negi et al. [146] executed a scenario where an attacker gained access to the leaked authentication information of a website (username and password). Then the attacker tested if this authentication information could be used on a banking website that incorporated a keystroke dynamics-based security layer. They experimented with two adversarial agents of their own design: Targeted K-means++, and Indiscriminate K-means++, on various datasets, and multiple state of the art classification algorithms. For Targeted K-means++ timing information about a given password was obtained simply by asking users on a paid crowdsourcing platform (Amazon Mechanical Turk) to type the specific password. Indiscriminate K-means++ was designed based on the idea that given the username and password timing vectors can be generated if general population timing data for each key is available. Timing data can be obtained from unsuspecting users by botnets and keyloggers. Their experiments demonstrated that their attack algorithms were effective across different settings. With Targeted K-means++ they succeeded within ten attempts to

compromise the security in 40-70% of users. The Indiscriminate K-means++ compromised the security in 30-50% of users. Moreover, they showed that the K-means++ generalized well to touch screen swiping data.

Meng et al. [83] used an interface named mimesis which provided feedback to train impostors in imitating another individual' s typing patterns through the adjustment of their typing patterns. They conducted their experiment with 84 individuals acting as impostors. They set a prerequisite that the impostors obtained the victim's typing patterns by two different ways, either by extracting them from a compromised database or by capturing keystroke samples as the victim authenticated using a keylogger. They used 2 eight-digit passwords of different difficulty, and the false acceptance rate (FAR) of the difficult and easy password increased from 20% and 24% respectively (before training), to 42% and 63% (after training with partial information of the victim). With full information of the victim, the FAR increased to 99% for both passwords for the 14 best attackers, showing that when a victim's typing pattern is known, imitation is possible.

Rahman et al. [131] presented an attack on continuous verification systems based on keystroke, named snoop-forge-replay. The attack's execution involves three steps: 1) stealing timing information of keystroke from a target user using a keylogger, 2) using the stolen keystroke timing information to forge a typing sample, and 3) replaying the forged typing sample in the continuous verification system. They launched the snoop-forge-replay attacks by replaying stolen samples into the authentication system. The average EERs achieved by the attack were between 0.487 and 0.912 depending on the number of stolen keystrokes. The attack increased EERs from between 69.33 to 2730.55% since the baseline EERs of the zero-effort attacks were between 0.03 and 0.285.

3.11.4 Attacks on touch dynamics

A considerable amount of research [33,34,149,255] has argued that an authentication system based on touch encounters two main threats, namely, shoulder surfing and malware. Specifically, [255] elaborates on the potential dual use of touch loggers, i.e., either offensively as a keylogging malware or benignly as a continuous authentication application. Regarding

shoulder surfing attacks Frank et al. [33] argued that an individual cannot learn the touch behavior of another individual simply by looking over his shoulder. Also, the aforementioned research has shown evidence that touch-based authentication systems hold a lot of promise for zero effort attacks [57] because the illegitimate user that gains access to the device is prevented by the mismatch between touch patterns. However, these attacks do not represent the entire field of threats the system could face for two reasons [59]:

a) Users' behavioral biometrics show a wide variance and overlapping between users [56,153]. In case we extract statistics from a database with large population records they could be used to generate forgeries and increase error rates [82,150].
b) The gestures on which continuous authentication is based can be easily implemented using commercially available robotic devices.

Serwadda et al. [59] demonstrated the efficient use of a "Lego" robot in creating forgeries that accomplish disturbingly high penetration rates over touch-based authentication systems when guided by input deriving from swiping statistics of the general population. They investigated the attack's impact by utilizing the best touch-based authentication classification algorithms and discovered that it augmented the classifiers' EERs by between 339% and 1004% depending on factors such as the failure-to-enroll threshold and the touch stroke type that the robot created. Their work raises doubt about the performance evaluating approach employed in touch-based authentication systems, namely the zero-effort impostor approach. In another study by Serwadda et al. [144] they used a robotic attack based on both population statistics and patterns of a specific user. For the attack driven by population statistics, they used patterns extracted from a large users' population, while for the attack towards a specific user they used stolen samples of a specific individual. By using seven verification algorithms they demonstrated that in both attacks the performance of a touch-based authentication system degrades significantly. For the algorithm that was the least affected, the population attack caused a greater than 70% increase in FAR.

In Table 12 a presentation of the type of attacks and system performance after the attack is made. In some cases, the minimum and maximum of EER is presented while in others the

minimum and maximum of FAR and FRR. There are cases where the highest system error or the percentage of error increase after the attack are presented. Finally, in some cases compromise of the security of users is also presented.

Table 12: Practical attack techniques on behavioral biometrics.

Biometrics	Works	Attacks	Performance (%)				
			FAR	Increase of system errors	Compromise of security of users	EER	FRR
Walking gait	Gafurov [142]	Imitation				13	
	Mjalaand [133]	Imitation				6,2	
	Kumar [60]	Imitation	44.5				
	Muaaz [95]	Mimic	0				
	Shrestha [64]	Mimic	4.55				
	Kumar [134]	Zero effort	DFAR2.2				DFRR4.2
	Wang [151]	Frog-Boiling				19.1,63.6	
	Serwadda & Phoha [150]	Algorithmic		84.4% MEER			
Keystroke dynamics	Negi [146]	Mimic			40-70, 30-50		
	Meng [83]	Mimic	99				
	Rahman [131]	Snoop-forge-replay				48.5-91.2	
Touch dynamics	Serwadda [59]	Robotic		1004%EER			
	Serwadda [144]	Robotic		70% FAR			

3.11.5 Discussion on practical attacks

A discussion on practical attacks follows:

3.11.5.1 Walking Gait

As previously shown, the attacks on gait refer to mimic attacks including impersonation attacks of minimal effort and attacks after the adversary training. Research results on accelerometer-based authentication systems demonstrated that the impersonation attack of minimal effort on gait biometric will not increase the impostor odds of being accepted [142]. Moreover, even when attacks are launched after the long- term training of the adversaries, their ability to learn the target user' s walking manner does not improve [133]. Imitation is a difficult task and even when professional actors who are specialists in body motions and body language mimicking and are of the same gender and other physical characteristics with the victim are trained as impostors, they fail in being accepted by the authentication system [95]. On the contrary, in the research of Gafurov et al. [143], it was reported that it is higher likely an impostor to be accepted when being of the same gender with the victim. In addition, attackers who knew who their nearest person in the database is became a threat to the authentication system [142]. Also, Kumar et al. [60] by launching a treadmill imitation attack increased the average FAR from 5.8% to 43.66% and characteristically report that: "The authentication systems based only on accelerometer readings are vulnerable to imitation attacks". Of course, works like for example Shrestha et al. [64] and Kumar et al. [134], suggest a multi-modal gait biometrics solution using the accelerometer and the gyroscope. These two works use sensors which are placed at several parts of the body and authenticate users based on their walking patterns. They also showed that the fusion of these modalities improves the overall performance of the system and adds an additional layer of defence against mimicry attacks of high-effort. These two works provide serious evidence that they are a solution to the previous issue, but further research is necessary.

3.11.5.2 Keystroke

On keystroke-based authentication systems the following types of attacks were shown: The Frog-Boiling attack [151], the Algorithmic attack [150], Mimic attacks [83,146], and the Snoop-forge-replay attack [131]. Although, the performance of a biometric system is enhanced when the templates of users are often updated, little research has been conducted on attacks towards such update mechanisms. The Frog-Boiling attack is a synthetic attack that secretly

exploits the update mechanism of users' templates to poison them. The attack not only is hard to detect but also has a great impact because it transforms users from well performing into ill performing and the error rates increase. In fact, it not only allows illegitimate access to the account of the victim, but the adversary also weakens the victim's template. This aspect makes the specific attack important, as the biometric system becomes vulnerable to intrusion from many impostors and for a long time [151].

The foundation for the employment of keystroke biometrics in authentication systems lays in the uniqueness property of typing patterns. A large body of research suggests that such patterns are unique and hard to imitate, thus the research effort in this area has focused on detection techniques to differentiate legitimate users from impostors. However, the imitation of the legitimate user's keystroke patterns can be done successfully by an impostor [83,146]. More specifically, impostors can be trained to imitate another individual through the adjustment of their typing pattern by using a training interface, given that they possess information on the victim's typing pattern. This information can be obtained either by a leaked database or by installing a keylogger [83].

In case an attacker wants to mimic a target user's typing pattern he can gather information in other ways, for example by collecting samples from other individuals rather than the target individual. Indeed, based on the hypothesis that the unique typing style of an individual belongs to a greater group of similar styles; the set of keystroke timing patterns can be clustered into a small number of clusters. Practically, this means that users with similar typing styles can be grouped to the same cluster. By gathering information from the general population using keyloggers or a crowdsourcing platform all such clusters can be created and mimic the typing patterns of the targeted individual [146]. The mimicking of a target user can also be done by an algorithmic attack that statistically analyses the keystroke data to synthetically generate the keystroke sequence that corresponds to the target user's profile [150]. Finally, in the case of snoop-forge-replay attack only a small amount of the victim's stolen timing information using keyloggers was necessary to create forgeries and make the attack effective [131]. From the above stems the fact that attackers can easily obtain a lot of keystroke data and extract the

statistics of keystroke feature in many different ways. Indeed, they can use bots, crowdsourcing platforms, unsuspecting users by fooling them or extracting statistics of feature directly from keystroke datasets that are publicly accessible. As shown, these attacks are highly effective and consequently, there is a need for research on technologies that can defend against the previously mentioned attacks.

3.11.5.3 Touch gestures

Several studies [33,34,149] have shown evidence that touch-based authentication systems are much promising regarding zero effort and shoulder surfing attacks. The installation of a malware application on the user's device could result in a more effective attack if the attacker has information on how to compute the features, since the malware can obtain and reveal the legitimate user's touch patterns to the attacker [33]. The case of a malware attack is quite likely to be addressed by using an anti-malware software. However, if the user does not have anti-malware, this attack is quite dangerous for the authentication system. Also, an adversary accessing population statistics could gain much information on the patterns of a particular user without needing a malware for monitoring him. In addition, sophisticated adversaries that can use advanced robots, may render the attack even more successful.

Due to the attacks, several privacy issues are emerging. Some of these issues relate to the behavioral biometrics themselves, for example, the leakage of biometrics from a malware, a statistical, a robotic, etc., attacks. Apart from that, additional privacy issues emerge when attacks are successful and users' personal data are exposed. For the above reasons, research on technologies that can defend against attacks that are based on population statistics as well as robotic attacks should continue.

3.12 Possible countermeasures on practical attacks on BB

There are three keyways for the enhancement of security in behavioral biometrics authentication:

3.12.1 Adding features

Various features from the user's behavior are possible to be extracted and used for the enhancement of security in behavioral biometrics authentication systems. Feng et al. [149] extracted data of touch from smartphones equipped with a touchscreen from 40 users and obtained approximately 7.5% FAR at approximately 8% FRR using the random forest verifier. Afterwards, a digital glove was worn by users that provided additional information on their hands' movement. With the use of the digital glove they reduced FAR at 4.66% and FRR at 0.13% and enhanced security. Several studies showed that pressure features are extremely hard for an impostor to imitate. Zhao et al. [35] combined pressure features with six touch traces for mobile devices authentication and achieved an EER of 2.62%. Wolf et al. [128] combined data from the accelerometer, the touch screen and the keyboard and identified individuals at 83% by using a simple normal distribution method. In a study of Tasia et al. [67] where they combined several features, they concluded that the best results in user authentication were achieved when combining pressure with time features. Kumar et al. [145] experimented on fusing typing patterns, swiping gestures and the corresponding patterns of phone movement on a 28 users dataset. An accuracy of 93.33% was achieved by fusing patterns of swipe and the corresponding movement patterns of the phone at feature level. An 89.31 % accuracy was achieved by fusing behaviors of typing and the corresponding movement patterns of the phone at score-level.

3.12.2 Combination with other biometrics

Several combinations of behavioral biometrics with physiological biometrics are possible. Bigun et al. [68] evaluated the combination of fingerprint and voice data and achieved 0.94% EER. Morris et al. [69] applied the combination of voice, face and signature data and achieved an EER of 1%. Kim et al. [70] used voices and teeth images and had 2.13% EER. In another

experiment, Kim et al. [71] combined face, teeth and voice and they achieved an EER of 1.64% confirming the improved performance of combining modalities in comparison to single modalities authentication methods.

3.12.3 Combination with non-biometrics

Approaches that combine behavioral biometrics with password or token-based authentication enhance the authentication accuracy and are thoroughly investigated in the literature. De Luca et al. [72] examined the shape of the users input, and more specifically unlocking the screen and password input, in combination with the way they performed the input. Their method achieved 77% accuracy resulting in an increased security. Sae-Bae et al. [73] used multi-touch gestures which included palm position, fingertip movement and fingertip dynamics. They achieved a 90% accuracy rate by using single gestures and discovered that the accuracy improved significantly when multiple gestures were performed in sequence. In a study of Shahzad et al. [74] they combined the velocity of the finger, the device acceleration, and the stroke time to examine how users perform the input, even when attackers saw what gesture a user performed, through shoulder surfing or smudge attacks, they could not reproduce his behavior. Their method achieved 0.5% average EER. Ohana et al. [75] built a key/lock system for the mobile phone and its charger, thus making the phone useless when separated from its power source. This system, in combination with biometrics would discourage the theft of the mobile phone. Sun et al. [76] used curves as passwords inputs in combination with the way that the inputs are performed by the legitimate user. Their system achieved an accuracy rate of 97.5%.

The above methods improve the performance of authentication systems but have not been tested against trained imposters. All the data presented in Table 13 relate to the known system performance indexes FAR, FRR etc., but they do not show the improvement of systems resistance to real attacks.

Table 13: Possible countermeasures.

Method	Works	Combination	Performance (%)			
			FAR	**FRR**	**Accuracy**	**EER**
Adding features	Feng et al. [149]	Touch data and hand movement.	4.66	0.13		
	Zhao et al. [35]	Six touch traces with pressure features.				2.6
	Wolf et al. [128]	Accelerometer, touch screen, keyboard.			83	
	Tasia et al. [67]	Keystroke by adding the features of pressure and size.				
	Kumar et al. [145]	Swiping gestures, Typing patterns & Phone movement.			93.33 89.31	
Combination with other biometric characteristics	Bigun et al. [68]	Fingerprint and voice.				0.94
	Morris et al. [69]	Voice, face and signature.				1
	Kim et al. [70]	Teeth image and voices.				2.13
	Kim et al. [71]	Face, teeth and voice.				1.64
Combination with non-biometrics	De Luca et al. [72]	Screen pattern and password.			77	
	Sae-Bae et al. [73]	Palm position, fingertip movement and dynamic.			90	
	Shahzad et al. [74]	Finger velocity, device acceleration, and stroke time.				0.5
	Ohana et al. [75]	Built a key/lock system for the mobile phone and its charger.				
	Sun et al. [76]	Passwords inputs in combination with the way that the inputs are performed by the legitimate user.			97.5	

3.12.4 Discussion on countermeasures on practical attacks

As it is previously shown in Table 13 the performance of authentication can be improved by incorporating additional biometrics in the authentication system, i.e. the use of multimodal biometrics. Multimodal biometrics-based authentication produces more consistent and higher

authentication accuracy in comparison with the single biometrics-based authentication and achieves upgraded performance [24]. Many research works and practical implementations widely adopted the multimodal-based framework since the reliable authentication of a high level cannot be guaranteed by the single biometric [5,9]. A plethora of studies has emphasized the superiority of multimodal biometric approaches to single biometric methods [77–81]. Since multimodal biometrics is performing better a well-built authentication mechanism is necessary to ensure the successful implementation of multimodal user authentication.

3.13 Lessons Learned

Behavioral biometrics and CA technology advantages: CA technology is a promising method with many advantages. It can perform without user intervention, it doesn't require additional hardware, and it presents high accuracy for zero-effort evaluation approach.

Inconsistent behavior of the legitimate user: a major deficiency that results from the inconsistent interaction of users with their mobile phones is the unreliable performance [11]. In addition, a physical injury or a panic situation may result in behavioral changes, which can lead to inconsistent reactions by the legitimate user. Therefore, the appropriate management of unexpected situations must be established [52].

Changes in user behavior and habits: User behaviors and habits may change over time; thus, authentication systems should be able to adapt to these changes. The paradigm of Continual Learning [163,167,168] can train successfully deep discriminative models as well as deep generative models in complex continual learning scenarios where new tasks appear, and existing tasks change over time. Therefore, this paradigm could be employed towards this direction.

Research data collection procedure: Many users avoid participating in time consuming, painstaking procedures for the collection of biometric features. This results in not fulfilling the data collection procedure.

Security in behavioral biometrics authentication: The primary threat is that the legitimate user's behavior can be mimicked directly or indirectly by an impostor. Security in behavioral

biometrics authentication can be improved if features are added or behavioral biometrics are combined with other biometrics or with non-biometrics.

3.14 Challenges and open issues

3.14.1 Technology acceptance

Factors of users' acceptance: Users' perception and behavior constitute important considerations when designing systems since security, privacy and online identity management issues often trouble users. A study aimed at identifying non-technical issues, for example perceptions about the fears and expectations of future users, may be necessary for developing a strategy to support the acceptance of an innovation [150]. For these reasons, the assessment of technology acceptance determinants is crucial for addressing the problem of reduced use and utilization of the BBCA technology benefits.

3.14.2 Behavioral Biometrics collection and feature extraction

Need for a user-friendly BB collection methodology: A major challenge is the design of a methodology for collecting behavioral biometrics, in a way that makes it user-friendly. The selection and optimization of a proper set of behavioral biometrics constitutes a challenge and an open issue.

Lack of real-world datasets: Another great challenge is the small number of real-world datasets. Thus, the provision of a public behavioral biometrics database for research purposes is necessary [10].

3.14.3 Systems evaluation

Maximizing accuracy: As examined in the literature most studies implement approaches using machine learning algorithms but very few use deep machine learning. The accuracy of an authentication system based on behavioral biometrics must be tested with deep machine learning algorithms to examine if the performance can be increased.

3.14.4 Security and usability

Balance between security and usability: Behavioral biometrics continuous authentication is subject to limitations, such as risk of false positives/false negatives, i.e., balance between security and usability, which result to its limited applicability. To overcome these limitations, it is crucial to maximize accuracy and examine how to find a balance between security and usability [112,113].

3.15 Conclusion

The review of a large corpus of research in the field of BBCA technology has shown that CA technology can provide high authentication accuracy. Behavioral biometrics are promising but also vulnerable to practical attack schemes. The incorporation of additional biometrics in the authentication system, i.e., the use of fusion authentication, is shown to improve security and guarantee reliable authentication. The superiority of fusion biometric approaches to single biometric methods is emphasized in a plethora of studies. These approaches must be further tested in real-world datasets. Also, the use of behavioral biometrics authentication is of limited extent due to some major shortcomings such as the risk of false positives/false negatives, i.e., the balance between security and usability [1]. To overcome these shortcomings, it is critical to maximize accuracy and investigate how to balance security with usability. Also, evaluating users' technology acceptance factors is vital to addressing the problem of reduced use of BBCA technology. Finally, a major challenge is the testing of a methodology for extracting biometric features, in a way that makes it user friendly, because many users avoid participating in time consuming, painstaking procedures for the collection of biometric features.

4 *Method of Work*

4.1 Introduction

This research comprised of four research stages that each addressed one of the research questions. This chapter presents a general summary description for each stage of the research.

4.2 Research design and methodology

Following, a presentation of the methodologies of the four research stages is made.

4.2.1 Research Stage 1

The first stage of the research concerns a survey on Behavioral Biometrics & Continuous User Authentication on Mobile Devices. The methodology is based on the collection of selected published sources relevant to the subjects of Continuous Authentication using Behavioral Biometrics. Moreover, annotation, critical analysis of content and opposition, in some cases, of the main conclusions of each work is carried out. A prerequisite of systematic search for suitable publications is the definition of indexing terms. In order to increase the efficiency of search, combined indexing operators with the relevant terms were used, e.g., continuous authentication, behavioral biometrics, mobile phones, etc., The results were grouped in 5 main sections, examining: walking gait, touch gestures, keystroke dynamics, behavioral profile, hand waving, power consumption, and fusion.

4.2.2 Research Stage 2

The second stage of the research concerns an Empirical Research on key factors driving the adoption of Behavioral Biometrics & Continuous Authentication Technology. In this regard, an investigation on the effect of various factors of behavioral intention through the new incorporation of a modified Technology Acceptance Model (TAM) and Diffusion of Innovation Theory (DOI), is made. Also, a new theoretical framework with constructs such as Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC), and Perceived Risk of Using the Technology (PROU), is created. A Structural equation modeling (SEM) empirical research is conducted. The research is designed in such a way to respond to the trade-off between perceived users' concern for their biometrics privacy and their protection from risks. To be able to answer the questions asked, in the context of this research, there is a need to first develop a sample of people with knowledge of the biometric methods that are under consideration. For this reason, participants in this study first followed an online five-minute course (mini-seminar) on behavioral biometric methods and CA systems. The sample of the research consists of 545 individuals and is composed of different groups of working people and university students of the European Union (EU), United States of America (USA), and Canada. To collect the data, the method of submitting questionnaires via the Amazon MTurk was used. A detailed description of the methodology is detailed in chapter 5.

4.2.3 Research Stage 3

The purpose of this stage is to present a new paradigm, named BioGames, for the extraction of behavioral biometrics (BB) conveniently and entertainingly. The BioGames paradigm suggests a user-friendly methodology for the collection of behavioral biometrics. The users simply play games without participating in an experimental painstaking process. To apply the BioGames paradigm, a BB collection tool for mobile devices named BioGames App is developed. The BioGames App is an Android application for collecting mobile devices sensor values and it sends the biometrics data in a database. The database is designed to allow multiple users to store their sensor data at any time. Thus, there is no concern about data separation and synchronization. BioGames App is GDPR compliant, as it collects and processes only

anonymous data. Moreover, the behavioral data collected are not publicly observable, they can only be recorded when a person uses the application. The BioGames App collects keystroke dynamics and touch gestures data and create datasets for research purposes.

4.2.4 Research Stage 4

In this stage, research related to the design and evaluation of new approaches to continuous authentication using touch gestures and keystroke dynamics, is presented. In the data collection process, the BioGames App is installed on the mobile devices of 39 participants. Users play the games in their everyday environment, and the various hardware components collect the biometrics. The BioGames App sends to the database all the data for each modality. The process of touch gestures and keystroke dynamics data collection has 16 sessions, where each session lasts approximately 2 minutes. Of the 39 participants in the sample, 38 are considered impostors, and one person is considered genuine. Regarding fusion, the feature-level fusion of keystroke dynamics and touch gestures is applied, and their unification into a single feature set consists of 39 individuals and 1488 Instances. Of the 39 participants in the sample, 38 are considered impostors, and one person is considered genuine. Lastly, a comparison of the performance of Multi-Layer Perceptron (MLP) and Long Short-Term Memory (LSTM), is made. Each modality is examined separately and an investigation is made regarding if there can be an improvement of the performance by applying feature-level fusion of biometrics to solve either security or usability issues. A detailed description of the methodology is presented in chapter 7.

4.3 Conclusion

In this chapter, the summary of the methodology that was followed in this doctoral thesis is presented. The methodology consisted of four research stages that each addressed one of the research questions. These are the research stages of a designed single project. Firstly, an extensive systematic literature review is presented that maps the research area and identifies the challenges, open problems, and future trends. Then, a new theoretical framework is presented to investigate the key factors that show us the user requirements that influence the

adoption of BBCA technology. In the third stage, a new paradigm (BioGames paradigm) and a new tool (BioGames App) for collecting behavioral biometric data, are presented. Finally, an experimental data collection process of keystroke dynamics and touch gestures is applied by using smartphones. For this purpose, the BioGames paradigm and the BioGames App are used. Also, a comparison is made between Multi-Layer Perceptron (MLP) and Long Short-Term Memory (LSTM). Each modality is examined separately and an investigation is made regarding the improvement of performance by applying feature-level fusion of keystroke dynamics and touch gestures to solve either security or usability issues.

5

Key factors driving the adoption of Behavioral Biometrics & Continuous Authentication Technology: An Empirical Research

5.1 Introduction

In this chapter, a new model is presented to investigate the effect of various factors on Behavioral Intention to Adopt the Technology (Behavioral Intention – BI). Based on this model, a Structural Equation Modeling (SEM) research was carried out. In this regard, an investigation on the effect of various factors of behavioral intention through the new incorporation of a modified Technology Acceptance Model (TAM) and Diffusion of Innovation Theory (DOI), is made. Also, a new theoretical framework with constructs such as Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC), and Perceived Risk of Using the Technology (PROU), is created. In addition, the research explores external factors, such as Trust in Technology (TT) and Innovativeness (Innov). The addition of exogenous factors to the basic research model has allowed the study of their impact on the intention of users to adopt BBCA technology. This research provides several useful insights and new knowledge for researchers, practitioners, governments, and providers of BBCA technology.

5.2 Theoretical Background

In this section a presentation of the theoretical framework is made.

5.2.1 DOI and TAM models

In this research, the most acknowledged theoretical frameworks proposed in the literature for

the behavioral intention to adopt new technology is used. Specifically, the TAM model [196] and the DOI theory [215]. The DOI Theory investigates the reactions of individuals towards new products or processes, and the reasons why some innovations diffuse while others do not. According to the research conducted on the field of the DOI Theory, various factors affect the formation of an individual's attitude and subjective norms towards his/her reactions to new products [218]. The above Theoretical Technology Acceptance Framework demonstrates that when innovative technology is displayed to users, several factors impact their choice on how and when to utilize it.

The Technology Acceptance Model (TAM) has been constantly studied and developed. The most significant improvements are the TAM 2 [200, 216] and the Unified Theory of Acceptance and Use of Technology (UTAUT) [191]. TAM 2 proposes that users form perceptions regarding the usefulness of the system based on its relevance between the important goals at work and the consequences of performing job tasks using the system [244]. Also, a TAM 3 has been suggested on e-commerce which incorporates the impacts of trust and perceived risk on system employment [217]. The TAM has been demonstrated to be especially valuable in examining the intention to embrace new technologies in a wide range of cases [219, 220, 221, 222]. A product or an idea gains impetus and diffuses (or spreads) across a particular population or social system. Regarding the editions of the TAM model, the original TAM fits best with this research. TAM is a simple model comprising the fundamental constructs that explain technology acceptance and, thus, it is expandable and can be adapted for use in specific technology areas. TAM 2 adds several variables to the TAM model to increase the model’s capacity to explain Intention to Use. Instead of the generic variables of TAM 2, variables are added that are more specific to behavioral biometrics. Thus, TAM being a basic model formed the basis for the development of a model more relevant to the specific technology under study.

5.2.2 Limitation of the TAM model

The cause driving the acceptance of biometrics adds important constructs like the variables that are connected with privacy and security issues [188, 242]. These variables cannot be individually clarified or sufficiently addressed with the present frameworks or adoption

models. The TAM model appears to omit several factors that could affect individuals regarding the acceptance of biometrics technology [188]. Therefore, new variables must be added in addition to a unifying view of technology acceptance prior factors. The relevant constructs of technology acceptance best practices and theories could be combined to create a new framework that can be utilized to assess biometrics technology acceptance facilitators and inhibitors [188, 242].

5.2.3 Theoretical framework

To address the limitation of TAM it is extended by adding three new constructs, namely, Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC) and Perceived Risk of Using the Technology (PROU), resulting in a new theoretical framework. The modifications of TAM were designed to overcome the limitations of the model and to adapt it to the needs of the present research so that its impact could be measured more effectively. The construct SPR concerns the security and privacy risks of individuals. The meaning of risks includes both the probability of access control breach and the value of the protected data or assets (e.g., money in a bank account). So, when there is a high SPR, then the chances of violations seem high because the value of our assets is great. Consider that our mobile phones are used for important tasks, such as mobile banking, e-payments, accessing email, and social media accounts. The SPR is considered as a facilitator in the Perceived Usefulness (PU) of the TAM model and following in the Behavioral Intention to adopt the Technology (BI). The BPC construct concerns biometrics Privacy issues. Individuals may be concerned about their biometrics which are sent to a central online server; therefore, this research should concentrate on this [187]. Since BBCA technology operates mainly with a central online server, individuals will consider BBCA technology to be risky for their biometrics privacy. For this reason, BPC is expected to act as a facilitator in the PROU and that PROU acts as an inhibitor in the BI of TAM model. The design of the research is such as to meet the above-mentioned combination. That is the trade-off between perceived users' concern for their biometrics privacy and their protection from risks.

5.3 Model development

The research model examines the factors that influence the adoption of BBCA technology. It consists of both pre-existing models (TAM, DOI) and new constructs added to explore the perceived intent of adopting BBCA technology. The new constructs added are Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC) and Perceived Risk of Using the Technology (PROU). Also, new variables to the TAM are added where its impact could be measured more effectively. Moreover, the constructs Trust in Technology (TT) [202], Innovativeness (Innov) [189], Compatibility (COMP) [225] are used, and the Perceived Risk of using the technology (PROU) is adapted to the need of this research which was based on the works [188], [240].

5.3.1 A Modified Technology Acceptance Model (TAM)

New variables to the TAM model are added, where its impact could be measured more effectively. Also, some original variables were extracted from TAM. The constructs variables are presented in table 14. In the literature, it is suggested that PU [193, 194, 195] and PEOU determine the intent of adopting a technology [196, 197]. Also, it was shown by empirical evidence that the ease of use has an impact on the user's intention to use [198, 199, 200]. From this point of view, the same to be valid in the case of BBCA technology is expected.

H1. The greater the perceived usefulness (PU), the greater the intention of adopt the technology (BI).

H2. The greater the perceived ease of use (PEOU), the greater the intention of adopting the BBCA technology (BI).

5.3.2 The impact of DOI variables

In studies like Koenig-Lewis et al. [227] and Miltgen et al. [188], compatibility was recognized as a significant precedent for perceived ease of use and perceived usefulness. For this reason, based on the aforementioned literature, it is considered that this construct is a contributing addition to the TAM model. For this reason, only this construct is selected from the DOI theory to be included in this research model.

5.3.2.1 The impact of Compatibility (COMP) variables

Compatibility (COMP) [225] is an important variable defining technology adoption [208, 204, 209, 189] and has also been reported to contribute remarkably to accurately predicting the adoption intent [203]. In the present research, it is considered that individuals who believe that the usage of the BBCA technology would fit well with the way they want to secure their personal data and accounts (e.g., bank accounts, e-mail, etc.) have a higher intent to adopt this technology. Moreover, individuals who believe that BBCA would fit into their lifestyle have a higher appraisal of ease-to-use and perceived usefulness. From the above reports the following hypotheses arise:

H3. The higher the perceived Compatibility (COMP), the greater the intent of adopting the BBCA technology (BI).

H4. The higher the perceived Compatibility (COMP), the more likely it is that an individual will perceive a BBCA technology as easy to use (PEOU).

H5. The higher the perceived Compatibility (COMP), the more likely it is that an individual will perceive a BBCA technology as useful (PU).

5.3.3 Perceived Risk of Using the technology (PROU)

Miltgen et al. [188] investigated the hypothesis that Perceived Risk (PR) [240], will be higher for biometrics technology and will decrease consumer intention to use this technology. Of course, a highlight must be made on Miltgen et al. [188] who investigated their hypothesis in an entry point authentication technology, which was directly comparable to similar traditional knowledge-based authentication systems [223]. In this research, the perceived risk in association with BBCA technology is examined to see if and how it will affect the behavioral intention to adopt this technology. The perceived risk (PR) is modified to the needs of the present research, and the construct Perceived Risk of Using Technology (PROU) is created as the main inhibitor to BI. The hypothesis is as follows.

H6. The greater the Perceived Risk of Using the technology (PROU), the lower the Behavioral Intention of Adopting the BBCA technology (BI).

5.3.4 Prior Factors

5.3.4.1 The impact of Innovativeness (Innov) variables

Yi et al. [189] and Miltgen et al. [188] confirm that the mood for innovation directly determines three characteristics: perceived usefulness, ease of use and compatibility. Also, it associates with the behavioral intention to adopt a technology. The higher the personal innovation, the more likely there would be a positive perception of the technological characteristics, such as: (a) Compatibility (COMP), (b) Behavioral Intention to Adopt the Technology (BI), (c) Perceived Usefulness (PU) and (d) Perceived Ease of Use (PEOU).

H7. Individuals with higher personal innovativeness will positively recognize the technological features of (a) Compatibility (COMP), (b) Behavioral Intention to Adopt the Technology (BI), (c) Perceived Usefulness (PU) and (d) Perceived Ease of Use (PEOU).

5.3.4.2 The impact of Trust in Technology variables

Trust in technology has the effect of reducing uncertainty and creating a sense of security [201], [202]. Carter and Bélanger [203], and Kim et al. [206] have also assumed that trust is important in shaping the intent of consumer regarding the use of a specific technology. Wu and Chen [207] report that trust has a direct impact on the behavioral intent of adoption. Finally, Kim et al. [205] have shown that as confidence grows, it is likely that consumers perceive less risk (likewise [203], [204]). Based on the above the following hypotheses are formed:

H8. Individuals' trust in technology has a positive impact on the: (a) Perceived Ease of Use (PEOU), (b) Behavioral Intention to Adopt BBCA Technology (BI), (c) Perceived Usefulness (PU) and (d) a negative impact on Perceived Risk of Using the Technology (PROU).

5.3.5 Theoretical background of the new constructs

In this section, the theoretical background, and the hypotheses from the new constructs (SPR and BPC) added to the model are presented.

5.3.5.1 The impact of Security and Privacy Risks (SPR) variables

Laux et al. [232], in their study, showed that a banking organization would adopt biometric technology because it considers it a competitive advantage, in the sense that the bank advertises to its clients that they secure their money from theft due to biometric technology. There will be look back on this issue from the user side. That is, in view of the fact that due to the biometric technology the user enhances his/her security and privacy from potential dangers. The technologies used by users so far offer entry-point authentication, which is exposed to attacks that take place past the initial authentication. Therefore, individuals will realize the necessity of a BBCA system and, thus Security and Privacy Risks (SPR) is positively correlated to the construct of Perceived Usefulness (PU) of the TAM model. The concept of risk includes both the possibility of a violation of the access control mechanism (e.g., by stealing the PIN) and the value of the protected data or assets (e.g., personal data, money in a bank account). This includes the perceived risk of exposure or loss of personal data and concerns about the security of their assets considering a possible breach of the security mechanism. So, when we have a high SPR, then the chances of violations seem high because the value of our assets is great. Thus, the following hypothesis arises:

H9. The greater the Perceived Security and Privacy Risks (SPR), the greater the Perceived Usefulness (PU) of BBCA technology.

5.3.5.2 The impact of Biometrics Privacy Concerns (BPC) variables

Given that BBCA technology inherently requires personal biometric data, users may have concerns that the technology may entail risks to their biometrics privacy. Data can be collected and processed in the device, or it can be sent to a central online server [187]. Since BBCA technology mainly operates with a central online server, it is expected that individuals will be concerned about specific issues. These issues are if users' biometrics may be sent to third parties and if mobile phone companies and other providers that require biometric authentication, possess, may collect and process their biometric information. As a result, it is expected that their biometrics privacy concerns (BPC) positively correlate with their perceived risk of using BBCA technology.

H10. Individuals with higher Biometric Privacy Concerns (BPC) will perceive the use of BBCA technology as riskier (PROU).

5.3.6 The research model

By considering other relevant instruments [188, 189, 190, 196, 202, 223, 224], a pool of variables has been created. New variables to the adoption of technology models are added. Finally, the new factors added are included in the constructs Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC) and Perceived Risk of Using the Technology (PROU). In figure 1 the research model is presented.

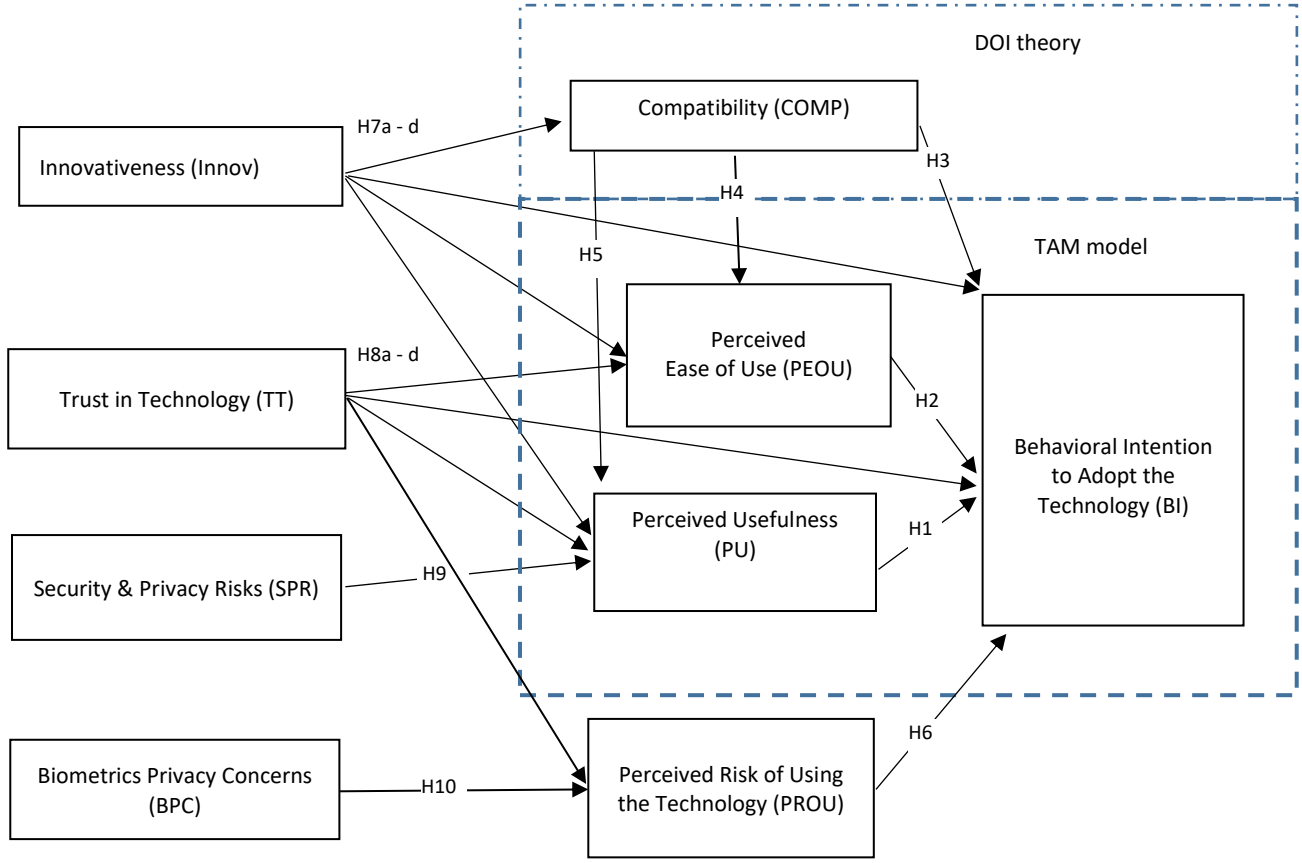


Figure 1: The research model.

5.3.7 The variables of constructs (Questionnaire)

The constructs variables of the model are presented in table 14.

Table 14: The variables of constructs.

Contructs	Authors	Item	Questions
Innovativeness (Innov)	Yi, et al. [189]	I1	I am among the first to try out new technologies.
	-‖-	I2	When I hear about a new technology, I look for ways to adopt it.
	-‖-	I3	I like to experiment with new technologies.
Trust in Technology (TT)	Pavlou [202]	TT1	I would trust the BBCA technology.
	-‖-	TT2	I think the BBCA technology would be reliable.
Security & Privacy Risks (SPR)	Self-developed	SPR1	It is likely that someone may get access to my bank account by stealing my phone and/or violating its access control mechanism.
	-‖-	SPR2	It is likely that someone may break into my social media and e-mail accounts.
	-‖-	SPR3	It is likely that someone may use my mobile for e-payments.
	Bélanger [240]	SPR4	I may get unauthorized charges on my bank account.
	Self-developed	SPR5	It is likely that someone may steal my device and gain access to my personal data, photos and videos stored in it.
Biometrics Privacy Concerns (BPC)	Self-developed	BPC1	I am concerned about my biometrics.
	-‖-	BPC2	My biometrics may be sent to third parties.
	-‖-	BPC3	Mobile phone companies and other providers that require biometric authentication possess may collect and process my biometric information.
Compatibility (COMP)	Vijayasarathy [225]	COMP1	Using this BBCA technology would fit into my lifestyle.
	-‖-	COMP2	I think using this BBCA technology would fit well with the way that I want to secure my personal data and accounts (e.g., bank accounts, e-mail, etc.).
Perceived Ease of Use (PEOU)	Davis [196]	PEOU1	BBCA technology will require little effort.
	-‖-	PEOU2	Learning to use BBCA technology would be easy for me.
	-‖-	PEOU3	I would find this BBCA technology easy to use
Perceived Usefulness (PU)	Davis [196]	PU1	This BBCA technology would enable access control (e.g., bank account) more securely.
	-‖-	PU2	This BBCA technology would make it easier to control my access to online services.
	-‖-	PU3	This BBCA technology would provide a valuable service.
	Self-developed	PU4	This BBCA technology would protect my bank accounts of access control breach.
	-‖-	PU5	This BBCA technology would protect my social media, e-mail, etc., accounts.
	-‖-	PU6	No one could gain access to my personal data in case my device is stolen.
Perceived Risk of Using the BBCA Technology (PROU)	Self-developed	PROU	BBCA technology maybe be risky for my biometrics privacy.
Behavioral intention to use the BBCA technology (BI)	Davis [196]	BI1	I should apply this BBCA technology as soon as possible.
	-‖-	BI2	I should use this BBCA technology soon after it is launched.
	-‖-	BI3	I should get detailed information before subscribing.

5.4 Methodology

To be able to answer the questions asked, in the context of this research, there is a need to first develop a sample of people with knowledge of the biometric methods that are under consideration. For this reason, participants in this study first followed an online five-minute course (mini seminar) on behavioral biometric methods and CA systems. At the mini seminar, individuals could see authentication systems in slides and examine a specific online banking scenario. During the seminar a short, on-line lecture was made where the following were presented:

- The issues of entry-point authentication model.
- The vulnerabilities of PINs and passwords.
- Vulnerabilities due to smudge attacks.
- Issues of entry-point authentication that remain even when morphological biometrics are used.
- BBCA technology, BBCA advantages, BB privacy issues, new "privacy-by-design" technologies.
- A short video on how continuous authentication works using behavioral biometrics.
- A scenario for access to mobile banking with BBCA technology.

In technological studies, and particularly in studies on technology adoption, the use of hypothetical scenarios is quite common [188]. In the seminar, individuals were also informed about privacy and BBCA usability issues.

For designing the questionnaire, the following methodology was followed. A preliminary questionnaire was given for review, to neutralize the subjectivity factor, to faculty members of the Aegean University's ICSE Department with extensive field research experience. Thus, each item was included in both the model and the questionnaire when it was adopted by the absolute majority. Based on the received suggestions, a modified version was designed and evaluated through a small-scale pre-test field involving 30 subjects. A 7-point Likert scale was employed

ranging from “Strongly disagree” (1) to “Strongly agree” (7) and the results were used to revise, remove, and rewrite certain questions. The questions were formulated in a fully understandable way so that they can be completed correctly. The logical continuity and clear distinction of the questionnaire’s sections were established by using titles and explanations to indicate each group of questions (constructs).

The research sample consists of 545 individuals and is composed of different groups of working people and university students of the European Union (EU), United States of America (USA), and Canada. According to Hair et al. [243] the sample size should be ten times the largest number of structural paths directed at a particular latent construct in the structural model. In the research, the requirement of sample size was exceeded. The sample represents the general public from the western developed countries. A stratified random sampling approach was followed, where the population was divided into categories based on certain features, i.e., smart phone-mobile device users, geographic area, occupation, and then random sampling was applied. In this way, all categories are represented by the selected attributes. To collect the data, the method of submitting questionnaires via the Amazon MTurk was used. This method was chosen among others due to its accuracy and the high level of participation it achieves. Written instructions were also provided when completing the questionnaires.

5.5 Results

In this section the descriptive analysis and the results of this research are presented.

5.5.1 Descriptive analysis

The research sample consists of 545 individuals. The respondents were from 18 to 65 years old, 58% were male, while 42% were female. Moreover, 57.72% of respondents hold a Bachelor's degree, 21.32% a Master's degree, while 5.51% hold a Ph.D. 8.46% have completed Secondary Education, and 6.99% holds a Higher National Diploma. Of the sample, 24.26% were employers or entrepreneurs with salaried employees, 22.61% were employed, 19.3% were self-employed, 3.13% were employers or entrepreneurs without employees, 19.49% were university students, 4.23% were unemployed, and 0.92 were retired. On average, it took 15

minutes to complete the survey.

5.5.2 Measurement model

There is no normal distribution in all items of the model (Kolmogorov–Smirnov's test ($p < 0.01$)). Therefore, the most-adequate method is the Partial Least Squares (PLS) [188, 206, 241]. To test the research hypotheses the bootstrapping method was applied [236]. SmartPLS version 3.0 [236] was used for the analysis, and as suggested by Hair et al. [233] and Nikou [237], there was a reliance on the path coefficients and their significance. Table 15 presents the correlations between the constructs.

Table 15: Correlation matrix.

	BI	**BPC**	**COMP**	**Innov**	**PROU**	**PEOU**	**SPR**	**PU**	**TT**
BI	-	0.148	0.799	0.590	0.026	0.593	0.346	0.750	0.807
BPC		-	0.196	0.183	0.617	0.327	0.364	0.202	0.101
COMP			-	0.554	0.031	0.640	0.320	0.783	0.796
Innov				-	0.133	0.484	0.237	0.512	0.528
PROU					-	0.163	0.299	0.041	-0.021
PEOU						-	0.273	0.576	0.559
SPR							-	0.328	0.309
PU								-	0.731
TT									-

To examine the internal consistency Cronbach's alpha, composite reliability, and the average variance extracted (AVE) were employed. In table 16, below, the following measurements are presented: Mean, Std. Dev., PLS factor loadings, average variance extracted (AVE), composite reliability (CR), and Cronbach's alpha. All items have loadings greater than 0.7, apart from BI3 which is near to these cutoff criteria (0.502). All constructs have alphas and CRs above the recommended value of 0.7 [235] which indicates good reliability. To estimate the discriminant validity, the Fornell-Larcker criterion was used [234]. The Fornell-Larcker criterion assumes that the AVE's square root must be greater than the correlations between the construct [234]. The square roots of the AVEs (diagonal elements) are greater than the correlation between each pair of constructs, as shown in Table 17.

Table 16: Measurement and internal validity.

Contructs	Item	Mean	Std. Dev.	Loadings	AVE	CR	Alpha
Innovativeness (Innov)	I1	5.200	1.533	0.904	0.817	0.930	0.888
	I2	5.053	1.514	0.923			
	I3	5.428	1.438	0.884			
Trust in Technology (TT)	TT1	5.189	1.457	0.935	0.881	0.937	0.865
	TT2	5.296	1.384	0.942			
Security & Privacy Risks (SPR)	SPR1	4.989	1.718	0.871	0.725	0.929	0.905
	SPR2	5.244	1.596	0.856			
	SPR3	4.822	1.843	0.861			
	SPR4	4.719	1.845	0.836			
	SPR5	5.336	1.640	0.832			
Biometrics Privacy Concerns (BPC)	BPC1	5.314	1.492	0.823	0.738	0.894	0.822
	BPC2	5.039	1.648	0.885			
	BPC3	5.259	1.564	0.868			
Perceived Ease of Use (PEOU)	PEOU1	5.222	1.385	0.833	0.733	0.892	0.818
	PEOU2	5.553	1.256	0.851			
	PEOU3	5.493	1.279	0.885			
Compatibility (COMP)	C1	5.469	1.313	0.909	0.826	0.905	0.789
	C2	5.282	1.468	0.908			
Perceived Usefulness (PU)	PU1	5.504	1.259	0.829	0.671	0.924	0.902
	PU2	5.621	1.157	0.833			
	PU3	5.388	1.403	0.797			
	PU4	5.586	1.180	0.849			
	PU5	5.513	1.272	0.840			
	PU6	5.301	1.502	0.764			
Perceived Risk of using the Technology (PROU)	PR1	4.890	1.553	1	1	1	1
Behavioral intention to use the technology (BI)	BI1	5.042	1.587	0.939	0.655	0.843	0.709
	BI2	4.934	1.641	0.912			
	BI3	5.851	1.254	0.502			

Table 17: Discriminant validity (diagonal values show AVE square root).

	BI	**BPC**	**Comp**	**Innov**	**PROU**	**PEOU**	**SPR**	**PU**	**TT**
BI	**0.809**								
BPC	0.148	**0.859**							
Comp	0.799	0.196	**0.909**						
Innov	0.590	0.183	0.554	**0.904**					
PROU	0.026	0.617	0.031	0.133	**na**				
PEOU	0.593	0.327	0.640	0.484	0.163	**0.856**			
SPR	0.346	0.364	0.320	0.237	0.299	0.273	**0.851**		
PU	0.750	0.202	0.783	0.512	0.041	0.576	0.328	**0.819**	
TT	0.807	0.101	0.796	0.528	-0.021	0.559	0.309	0.731	**0.938**

Note: na — AVE are not applicable to the single-item constructs.

Also, the value of standardized root mean square residual (SRMR) to show the assessment of model fit as well as the Normed Fit Index (NFI) were used [226]. SRMR values vary between 0 and 1, and those which are lower than 0.08 are considered a good fit [238, 239]. In the analysis, the SRMR value is 0.057. The NFI value in the analysis is 0.817. The closer the NFI is to 1, the better the fit [236].

5.5.3 Structural model and hypotheses testing

Respondents answered to Likert-scale questions on which one-sample t-tests were applied. The results are presented in Table 18 showing the t-values for each correlation between the variables. The t-value indicates whether there is a difference between the hypothesis H0 (i.e., there is no correlation) and the hypothesis H1 (the two variables correlate). For each correlation, there is an interest primarily in three values: Direct effects β, t-value, and p-value. The t is interested in being greater than 0, and p <= 0.05. In the case where there is an indirect effect in BI, then for each correlation, there is an interest primarily in three values: specific indirect effects β, t-value, and p-value.

Table 18 summarizes the results of the Bootstrapping estimation with 500 resamples and figure 2 the structural model result. The model explains 74.9% of behavioral intention to adopt the

technology's (BI) and H1, H3, H7b, H8b cases are supported, while H2 and H6 cases are rejected. The model explains 65.3% of perceived usefulness (PU) as all assumptions: H5c, H7d, H78c, and H9 are supported. The model explains 43.7% of perceived ease of use (PEOU), like all H4, H7c cases are supported while H8a is rejected. The model explains 38.8% of the Perceived Risk of Using the BBCA Technology (PROU) and supported by H8d: Trust in technology (TT) and H10: Biometrics privacy concerns (BPC). The model explains 30.7% of Compatibility (Comp) as H6a: Innovativeness (Innov) is supported. In total, out of the 10 assumptions made, 16 if the sub-assumptions are counted, 13 are supported by the model.

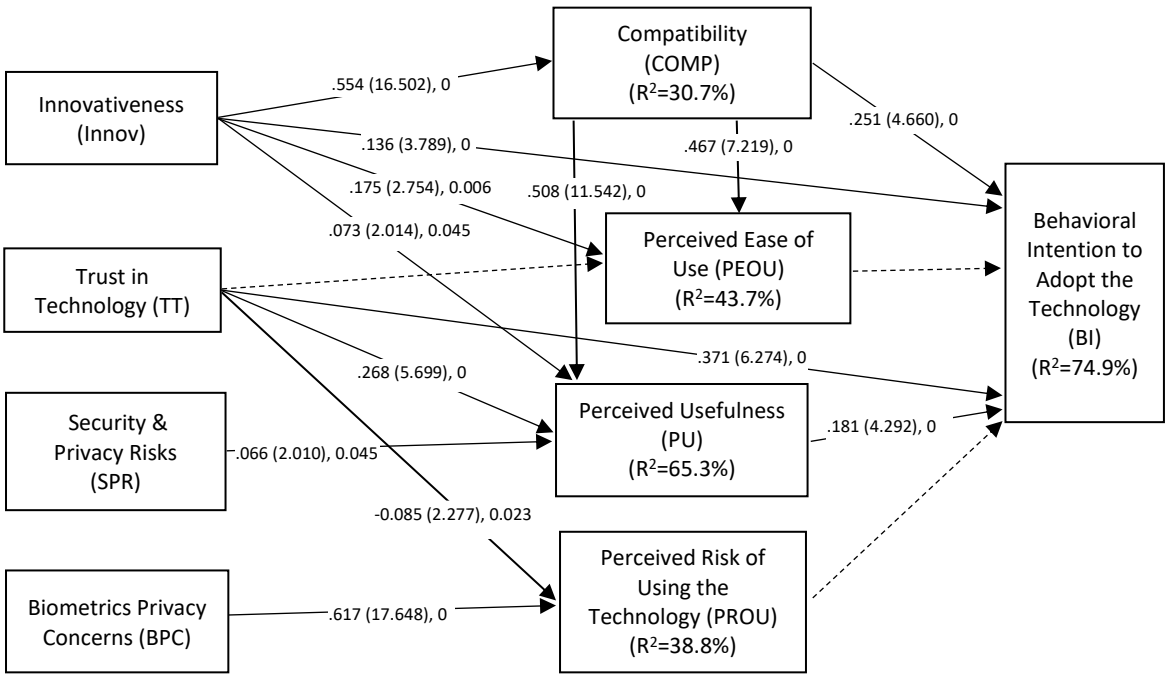
The purpose of the research is to understand the key factors that drive individuals towards the adoption of BBCA technology. Therefore, the analysis will be now focused on the main factors of adoption. The main facilitators of BI are Trust in Technology (TT) (β=0.371, t=6.274, p=0), followed by Compatibility (COMP) (β=0.251, t=4.660, p=0), Perceived Usefulness (PU) (β=0.181, t=4.292, p=0) and Innovativeness (β=0.136, t=3.789, p=0). Moreover, the results show that Trust in Technology (TT) also has a specific indirect effect, via PU (β=0.048, t= 3,172, p=0.002), on the BI, because it has a positive effect on Perceived Usefulness (PU), thus H8c (β=0.268, t=5.699, p=0), is supported by the model. Also, TT has a negative direct effect on PROU (β=-0.085, t=2.277, p=0.023) thus H8d is supported by the model.

Innovativeness (Innov) not only has a significant direct effect on BI but it also has a significant direct effect on COMP (β=0.554, t=16.502, p=0), PEOU (β=0.175, t=2.754, p=0.006) and PU (β=0.073, t=2.014, p=0.045), therefore H7a, H7c, and H7d are supported by the model. Innovativeness (Innov) has also specific indirect effects on the BI, but the effects go only via the COMP (β=0.139, t=4.499, p=0) and via Compatibility (COMP) and PU (β=0,051, t=4.190, p=0). COMP has also a specific indirect effect on BI via PU (β=0.092, t=4.196, p=0). The construct Security & Privacy Risks (SPR) has a positive direct effect on PU (β=0.066, t=2.010, p=0.045), thus H9 is supported by the model. Finally, the construct Biometrics Privacy Concerns (BPC) (β=0.629, t=17.648, p=0) positively correlated with Perceived Risk of Using a BBCA System (PROU) but the hypothesis that the major inhibitor of BI is PROU is not supported by the data.

Table 18: Direct effects, total indirect, and total effects β of determinants of intention to use BBCA technology.

Path	Direct effects **β**	Total Indirect effects **β**	Total effects **β**	**t-Value**	**R^2**	**Hypothesis confirmations**
Behavioral Intention (BI)					0.749	
H1: Perceived Usefulness (PU)	0.181		0.181	4.292		Supported
H2: Perceived Ease of Use (PEOU)	0.056		0.056	1.502		Rejected
H3: Compatibility (Comp)	0.251	0.118	0.369	4.660		Supported
H6: Perceived Risk of Using the Technology (PROU)	-0.008		-0.008	0.372		Rejected
H7b: Innovativeness (Innov)	0.136	0.228	0.364	3.789		Supported
H8b: Trust in Technology (TT)	0.371	0.054	0.425	6.274		Supported
Perceived Usefulness (PU)					0.653	
H5: Compatibility (Comp)	0.508		0.508	11.542		Supported
H7d: Innovativeness (Innov)	0.073	0.282	0.355	2.014		Supported
H8c: Trust in Technology (TT)	0.268		0.268	5.699		Supported
H9: Security & Privacy Risks (SPR)	0.066		0.066	2.010		Supported
Perceived Ease of Use (PEOU)					0.437	
H4: Compatibility (Comp)	0.467		0.467	7.219		Supported
H7c: Innovativeness (Innov)	0.175	0.259	0.434	2.754		Supported
H8a: Trust in Technology (TT)	0.095		0.095	1.312		Rejected
Perceived Risk of Using the Technology (PROU)					0.388	
H8d: Trust in Technology (TT)	-0.085		-0.085	2.277		Supported
H10: Biometrics Privacy Concerns (BPC)	0.629		0.629	17.648		Supported
Compatibility (Comp)					0.307	
H7a: Innovativeness (Innov)	0.554		0.554	16.502		Supported

Note: All effects are significant at $p < 0.001$ except for H9 and H7d: at $p<0.05$, H7c: $p<0.01$ and H8d: $p=0.023$



Note: in figure presented direct effects β, (t-value) and p-value. The dotted lines are non-significant.

Figure 2: Structural model result.

5.6 Discussion

The research examined the factors that affect the adoption of BBCA technology by using a modified TAM and DOI model by adding three new constructs. Thus, the model consists of both pre-existing models (TAM, DOI) and three new constructs that were added. The new constructs are Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC) and Perceived Risk of Using the technology (PROU). Moreover, the constructs Trust in Technology (TT) [202] and Innovativeness (Innov) [189] were used.

The main facilitators of BI are Trust in Technology (TT), followed by Compatibility (COMP), Perceived Usefulness (PU), and Innovativeness (Innov). These results reveal that the most significant driver for explaining BI of BBCA technology adoption comes from the construct TT, which is positively correlated with BI. TT also has an indirect effect on BI via PU. Therefore, it seems that trust in technology has the effect of reducing uncertainty and creating a sense of security that ultimately leads to the intention to adopt BBCA technology. These

results are consistent with the literature [188], [201], [202], [203], [206], [207], that have also confirmed that trust is important in shaping the intention of individuals to use a specific technology. Finally, research such as [203], [204] [205] has shown that as trust in technology increases, consumers are less likely to perceive risk. The findings are consistent with this claim as TT is negatively related to the PROU. In addition, despite the development of new "privacy-by-design" technologies, users are still seriously concerned about their biometrics privacy. In any case, the model measures users' Biometrics Privacy Concerns (BPC). Even if the perception of risk is not justifiable, it still affects the Perceived Risk of Using the Technology (PROU). However, although BPC positively correlated with PROU it does not seem to significantly affect individuals' intention to use these technologies. The hypothesis that the major inhibitor of BI is PROU is not supported by the findings. This probably happened because individuals consider that the benefits of using BBCA technology (e.g., the protection of their privacy and the security of their assets) are more important than the perceived risks for their biometrics privacy.

The benefits of using BBCA technology, on the part of the user, stem from the fact that users realize that authentication only at the beginning of the session, i.e., with entry-point authentication technology, is exposed to attacks that take place past the initial authentication. This leads to concerns about the security of their assets (e.g., personal data, money in a bank account) from a possible breach of the security mechanism. This may explain why Security and Privacy Risks (SPR) have a positive correlation with the PU of the TAM model.

In the literature, it is suggested that PU determines the intent to use a technology [188, 193, 194, 195, 196, 197]. This hypothesis is also confirmed by the model, since, as mentioned above, individuals are aware of the need for a BBCA system, so they understand its usefulness. On the other hand, research has also shown that PEOU has an impact on the BI [188, 198, 199, 200]. This hypothesis is not confirmed by the model probably because individuals are willing to sacrifice their ease for more security.

In studies like [188, 189, 204, 203, 208, 209, 227] compatibility was recognized as a significant precedent for perceived ease of use and perceived usefulness and has also been reported to

contribute remarkably to accurately predicting the adoption intent. The research is in line with the literature as the constructs Compatibility (COMP) are positively related to PU, PEOU, and BI. COMP has also an indirect effect on BI, via PU. So, compatibility is another factor that must be taken seriously for the success of future investments.

Finally, Yi et al. [189] and Miltgen et al. [188] confirm that the mood for innovation directly determines PU, PEOU, COMP and BI. The research, is in line with the aforementioned research since Innovativeness (Innov), not only has a significant direct effect on BI, but also has a significant direct effect on COMP, PEOU, and PU. Innovativeness (Innov) also has indirect effects on the BI, via COMP and PU. Finally, the constructs Innov and COMP, that were included in the model to explain BI, appear to be more significant than the PEOU used in the TAM model.

5.6.1 Limitations

The research has some limitations that should encourage further research in this field from other researchers as well. First, the research focused only on behavioral biometrics and continuous authentication on mobile devices. Future research could be carried out by extending to desktops or even to the Internet of Things (IoT) devices. In addition, many external factors need to be explored in future research such as consumer traits [228], situational factors [229], product characteristics [230], and previous experiences [231]. Finally, even though the sample represents the general public of the western developed countries there is the limitation that the research was conducted via the Amazon MTurk. Further research could be conducted in a wider sample.

5.7 Conclusion

This research is one of the first that examines the factors that influence the decision to adopt BBCA technology (BI). It is found that the main facilitators of BI are Trust in Technology (TT), followed by Compatibility (COMP), Perceived Usefulness (PU), and Innovativeness. The research also shows that individuals are less interested in the ease of use of the technology and are willing to sacrifice it to achieve greater security. Compatibility and Innovativeness also

play a significant role. Individuals who believe that the usage of the BBCA technology would fit into their lifestyle and would like to experiment with new technologies have a positive intention to adopt the BBCA technology.

The new constructs added are Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC) and Perceived Risk of using the technology (PROU). The results support the hypotheses that SPR is a facilitator to PU and PU acts as a facilitator to BI. Consequently, the hypothesis that individuals do not feel adequately protected by classical methods will consider the usefulness of the BBCA as a technology for their extra protection against risks is confirmed by the model. Also, with the constructs BPC and PROU an examination is made regarding if individuals' concerns regarding their biometrics privacy act as inhibitors in the BI. The conclusion is that individuals consider that the benefits of using BBCA technology are much more important than the risks for their privacy since the hypothesis that the major inhibitor of BI is PROU is not supported by the model. The new constructs were used to extend the TAM model and address its limitations with regard to addressing security and privacy issues. Therefore, it is suggested that this new theoretical framework should be combined with the TAM on biometrics and authentication research.

6

BioGames: A new Paradigm and a Behavioral Biometrics Collection Tool for Research Purposes

6.1 Introduction

One major challenge for Behavioral Biometrics (BB) and Continuous Authentication (CA) research is the lack of actual behavioral biometrics datasets for research purposes. The compilation and refinement of an appropriate set of behavioral biometrics data constitute a challenge and an open problem. The issue is aggravated by the fact that most users are reluctant to participate in long, demanding procedures entailed in the collection of research biometric data. As a result, they do not complete the data collection procedure, or they do not complete it correctly.

In response to these challenges, a new paradigm is proposed, named BioGames, for the extraction of behavioral biometrics conveniently and entertainingly. To apply the BioGames paradigm a behavioral biometrics collection tool for mobile devices, named BioGames App was developed. All it takes is simply to play a few games and the application creates all the datasets for each behavioral modality. BioGames App sends the behavioral biometrics data to an API interface, which then undertakes their storage in an online MySql database. This chapter contains and defines the requirements, specifications, and how BioGames App has been developed. BioGames code and the API interface code (MySql database connection) are available on Github[1] and contain relevant documentation and instructions. The BioGames is released as an open-source App, with an MIT License, under the following terms: Distribution,

[1] BioGames App code is available on Github (link: https://bit.ly/3vhK9zT).

Modification, Private use, Commercial use, License, and copyright notice. Finally, instructions are provided on how; researchers and practitioners can collect behavioral biometrics by using the BioGames App in their research and connect it with their database.

6.2 Current Behavioral Biometrics Collection Technologies

Meng et al. [54] built an application to collect and process keystroke data using a modified version of the Android OS based on CyanogenMod. They recorded input data from the touchscreen including the pressure of touch, the coordinates, the timing, and the type of the input (e.g., press down, press up).

Murmuria et al. [130] built a system to authenticate users based on the modalities of power consumption, touch gestures, and physical movement. Their Data Collection Tool had 4 services running to collect the power consumption data, touchscreen events, gyroscope and accelerometer sensor data, and user activity on the device. Their data collection tool, as well as their dataset, have not been released.

Bo et al. [36] obtained the user's application usage and interacting behavior with each application from the system API and made use of the motion sensors to measure the device's reaction. Their SilentSense tool has not been released.

Papamichail et al., [185] built an application named BrainRun which incorporates a tool for capturing and recording tapping and swiping gestures of users. They released their application on Google Play Store and Apple App Store and created a dataset that contains gestures and sensors data for more than 2000 different users and devices. This dataset is distributed under the Creative Commons license and can be found at the EU Zenodo repository. Even though the application is released on Google Play Store and Apple App Store, its source code is not publicly for researchers and practitioners.

In Table 19 a comparison of behavioral biometrics tools is made to show the gaps in this area. The comparison is made to show which modalities are used by each tool, which tool integrates most of the modalities, and which tool is freely available.

Table 19: Comparison with other tools.

BB Collection Tools	Behavioral Biometrics with Continuous Authentication					Released
	Gait	Touch Gestures	Keystroke	Behavioral profile	Power consumption	Freely available
Meng et al. [54]			v			v
Murmuria et al.	v	v		v	v	
Bo et al. [36]		v				
Papamichail et al.,		v				

It is noticed that there are no tools that combine keystroke and touch gestures modalities. Also, although some tools can collect data for several behavioral biometrics they are not freely available. As a result, researchers are unable to adapt them to their research needs. Therefore, there is a need for an application that collects various behavioral modalities, such as keystroke dynamics and touch gestures in an enjoyable manner. Moreover, it should be publicly available for researchers and practitioners to use and create their datasets for research purposes. BioGames App addresses these gaps, as it combines keystroke dynamics and touch gestures and it is publicly available. Also, it is based on the BioGames paradigm which suggests a user-friendly way of behavioral biometrics data collection. Finally, even though the application has many similarities with the BrainRun application, it should be noted that BrainRun only collects swiping gestures and its source code is not available for researchers and practitioners.

6.3 BioGames

In this section, the BioGames application, a behavioral biometrics collection tool, and the BioGames paradigm are presented. The BioGames paradigm suggests a user-friendly way for the collection of behavioral biometrics. All it takes is simply to play a few games and the BioGames App creates all the datasets for each behavioral modality. The BioGames App is an Android application for collecting mobile devices sensor values and it sends the biometrics data in a database. The database is designed to allow multiple users to store their sensor data at any time. Thus, there is no concern about data separation and synchronization. BioGames App is GDPR compliant, as it collects and processes only anonymous data. Moreover, the behavioral data collected are not publicly observable, they can only be recorded when a person

uses his/her smartphone. The games and challenges are presented in detail in the following section.

6.3.1 BioGames Description

In fig. 3a the BioGames App home page is shown. The user can click on any of the 2 buttons (1 for each modality) leading to the corresponding next page. Each category has 4 sessions and each session 4 games where the levels are becoming more difficult to complete. In fig. 3b, the BioGames page for the touch gestures modality is shown.

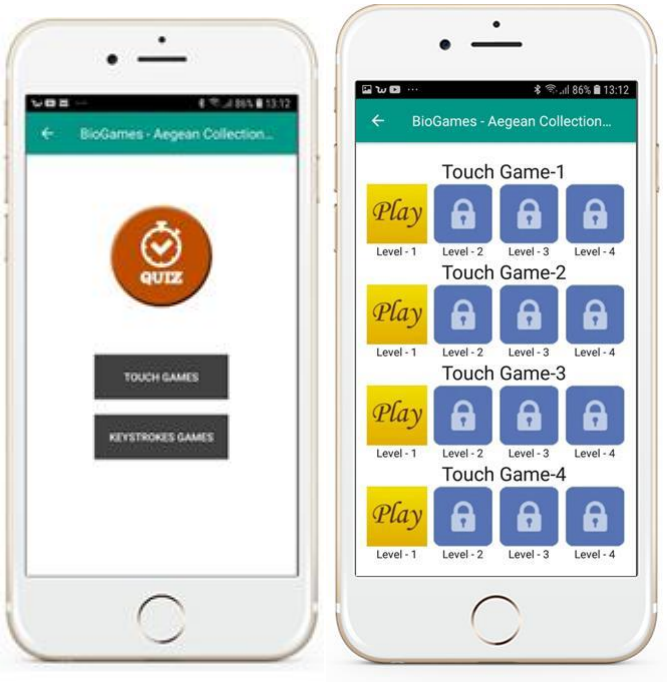


Figure 3, a, b: The BioGames App.

6.3.2 User Interface

In the beginning, the user has access only to Game 1 of Session 1. Following, the user must complete all 4 games of session 1 to unlock the first game of the next session. If the user successfully completes game 1 and within the given timeframe, then the next game unlocks until the user successfully completes all 4 games in each session. The games for each modality are as follows:

- ***Touch Gestures***

Here, there is a list of interactive games. Each game has a timer that shows how much time remains for the user to successfully complete the game (countdown).

➢ Games categories:

- Session 1 – In this session the challenge is to answer to simple mathematical statements by swiping left for correct and swiping right for wrong.
- Session 2 – In this session the challenge is to memorize a set of displayed images and then answer by swiping up or down whether a currently shown image was included in the displayed set of images or not.
- Session 3 – In this session the challenge is to pop the displayed balloons. The user must touch the screen to pop the balloons by a single or by multiple fingers touches simultaneously.
- Session 4 – In this session the challenge is to turn on the switches. The user must swipe up or down to turn on the switches.

These types of games are used because gestures such as swipe left/swipe right, swipe up/ swipe down which are widely used are collected. Also, some special gestures are collected such as single or multiple fingers touches and swipe up or down in a specific area, because they can be used for continuous authentication.

- ***Keystroke Dynamics Games***

Within the framework of these games, it is possible to record behavioral data in multiple sessions and within multiple records. Here, for example, a list of simple questions will be given which must be answered, with a slight increase in difficulty per level.

➢ Types of questions:

- Session *1* – Write the numbers. In this game a number is displayed on the screen. The user needs to write that number in text and submit his/her answer. The same is repeated for as long as the game lasts.

- Question: 8 (is displayed on the screen for a few seconds).
- Answer: Eight

- Session *2* - Write in text the numbers you have just seen. Here, for a few seconds, a list of numbers is displayed that the user must memorize and write in order to win.
  - Question: 1, 13, 37, 54 (they are displayed for a few seconds).
  - Answer: one, thirteen, thirty-seven, nine.

- Session *3* - Write the words you have just seen. Here, for a few seconds, a list of words is displayed that the user must memorize and write in order to win.
  - Question: carrot, blouse, watermelon (displayed for a few seconds).
  - Answer: carrot, blouse, watermelon.

- Session *4* – Write in text the word you see. In this game a string is displayed on the screen for a few seconds. Users need to memorize it, write it and submit their answers. The same is repeated for as long as the game lasts.
  - Question: hello! (displayed for a few seconds).
  - Answer: hello! (non-sensitive in lower case letters).

These types of games are used because all the data suggested in the literature are collected [187]. Also, in each game played the time limit decreases to collect typing data at different typing speeds. Finally, the typing games that are used are based on something that the user must recall from his/her memory, like a password, and games that are based on something that the user sees and types, like a captcha.

6.4 Data Collection and Features Extraction

BioGames collects data and creates features in the ways described below.

6.4.1 Keystroke dynamics

When a user types on the keyboard of a smartphone the keyboard inputs are recorded and analyzed in order to identify him based on his tapping habits [187]. The BioGames application

extracts the duration and latency of the pressure on keys and the location points of the finger as described following [187, 108, 113]:

- *Duration:* is the time period between pressing and releasing a key.
- *Latency:* is the time period between releasing a pressed key until pressing the next key.
- *Pressure:* is the pressure on a key.
- *Location:* are the finger's location points (x_i, y_i) on the screen.

6.4.2 Touch Gestures modality

The gesture of touch is a single or multiple strokes or a swipe on the touch screen of the mobile device made by the finger. The BioGames application extracts the direction and duration of touch, the velocity, and acceleration of movement, which are analyzed and measured solely or in combination with each other [84, 87, 89]. A stroke or a swipe on the touch screen is a series of touch data when the finger is in contact with the mobile device screen [84]. Each of them can be encoded as a series of vectors [187, 87]:

$$S_i = (x_i, y_i, t_i, p_i), i = \{1, 2, \dots, N\}, \textit{(5)}$$

where x_i, y_i are the location points, and $t_i, p_i$are the time stamps and the pressure on screen, respectively. Here, N is the total number of swipes.

6.5 Discussion

In this research, a new paradigm and a new behavioral biometric data collection tool, called BioGames paradigm and BioGames App, respectively, are proposed. The BioGames App uses games and challenges that combine keystroke dynamics and touch gestures. In touch gestures, the types of games that are used collect gestures that are widely used. Also, some special gestures are collected such as single or multiple finger touches and swipe up or down in a specific area, because they could be used for continuous authentication. As for keystroke dynamics, in each game, the time limit decreases to collect typing data at different typing speeds. Finally, the typing games that are used are based on something that the user must recall

from his/her memory, like a password, and games that are based on something that the user sees and types, like a captcha.

As shown in the current behavioral biometrics collection technologies section there are no tools available that combine the keystroke and touch gesture modalities. In addition, BioGames App uses a methodology where users simply play games without participating in an experimental painstaking process. None of the tools presented in the literature suggests an enjoyable user-friendly biometric collection methodology except for the BrainRun application. However, BrainRun only collects tapping and swiping gestures and is not publicly available.

6.5.1 Limitations

One limitation of the research is that it does not include behavioral modalities such as behavioral profile, power consumption, and hand waving. Researchers and practitioners who may be interested could participate on GitHub as contributors to extend BioGames and cover more behavioral modalities.

6.6 Conclusion

In this section, a new paradigm and a new behavioral biometrics collection tool, named BioGames paradigm and BioGames App, respectively, are proposed. The BioGames paradigm suggests a user-friendly methodology for the collection of behavioral biometrics by simply playing mobile device games. BioGames App employs games and challenges that combine keystroke dynamics and touch gestures modalities. It also collects some special gestures such as single or multiple fingers touches and swipe up or down in a specific area, because they can be used for continuous authentication.

7

Continuous Authentication with Feature-Level Fusion of Touch Gestures and Keystroke Dynamics to Solve Security and Usability Issues

7.1 Introduction

Behavioral Biometrics (BB) Continuous Authentication (CA) systems monitor user behavior and continuously re-authenticate user identity alongside the initial login process. Most studies use single behavioral modality methods to authenticate users. However, the behaviors of genuine users may change, and systems fail when significant changes occur. This results in either usability or security issues. In the literature, the fusion of biometrics is used to solve this problem and achieves improved results. This chapter presents research on the design and evaluation of new approaches to CA using touch gestures and keystroke dynamics. Each modality is examined separately, and an investigation is made on improving the performance results with a feature-level fusion. For this reason, a new appropriate feature set is developed that combines touch gestures and keystroke dynamics. The Multi-Layer Perceptron (MLP) and Long Short-Term Memory (LSTM) are used, and a comparison of their performance is made. The results showed that feature-level fusion of touch gestures and keystroke dynamics improves the performance of systems and solves security and usability issues.

7.2 Current behavioral biometrics continuous authentication systems

Following the current behavioral biometrics continuous authentication systems on touch gestures, keystroke dynamics, and fusion are presented.

7.2.1 Touch gestures

Buriro et al. [39] employed the movements of users' fingers during signing or writing and the device's movements to profile them. With Multi-Layer Perceptron (MLP) achieved 95% TAR and 3.1% FAR. Filippov et al. [96] employed seven types of gestures. With the Isolation Forest method, their system achieved 6.4% FRR and 7.5% FAR. Shen et al. [104] used touch data collected during three different operation scenarios. The best performance was when users held the smartphone while sitting or standing still and performed touch actions. More specifically, with the HMM they achieved 3.98% FAR, 5.03% FRR, and 4.71% EER. Debard et al. [106] suggested CNN to recognize touch gestures. Their method achieved 89.96% Accuracy. Yang et al. [126] employed touch gestures with One-class SVM and Isolation Forest. They achieved 95.85% average Accuracy. Stylios et al. [251] present a research on the development and validation of a BBCA system (named BioPrivacy), that is based on the user's keystroke dynamics and touch gestures, using a Multi-Layer Perceptron (MLP). For touch gestures their system achieved Accuracy 91.32 and EER 1.2. The performance of the systems on touch gestures is presented in Table 20.

Table 20: Research works on touch gestures.

Method	Publications	Classification	Performance (%)				
			FAR	TAR	Accuracy	FRR	EER
Touch Gestures	[39] in 2016	MLP	3.1	95			
	[96] in 2018	Isolation Forest	7.5			6.4	
	[104] in 2018	HMM	3.9			5.03	4.71
	[106] in 2018	CNNs			89.96		
	[126] in 2019	Isolation Forest			95.85		
	[251] in 2022	MLP			91.36		1.2

7.2.2 Keystroke dynamics

Clark and Furnell [40] authenticated users based on their typing patterns while entering telephone numbers and text messages. The MLP achieved a 12.8% average EER. Draffin et al. [44] collected keystrokes not limited to passwords or prearranged text. By using FFNN they

achieved an Accuracy of 86% and an FRR of 2.2% and a FAR of 14%. Darren and Inguanez [111] used the typing data during four different activities. They used a Least Squares SVM with an RBF kernel, and all their results achieved an EER of approximately 1%, while the best results were an EER of 0.44%, an Accuracy of 100%, a FAR of 0%, and an FRR of 1%. Krishnamoorthy [43] classified users by applying machine learning concepts to keystroke dynamics. The typing characteristics of participants were recorded while typing a particular password. By using the Random Forest classifier, they achieved 98.44% identification Accuracy. Stylios et al. [249] collected keystrokes with the BioPrivacy collection tool. The best results were an Accuracy of 97.18%, an EER of 0.02%, a TAR of 97.2%, and a FAR of 0.02% with MLP. In Table 21, the keystroke dynamics systems are presented.

Table 21: Research works on keystroke dynamics.

Method	Works	Classification	Performance (%)				
			FAR	TAR	Accuracy	FRR	EER
Keystroke Dynamics	[40] in 2006	MLP					12.8
	[44] in 2013	FFNN	14		86.0	2.2	
	[111] in 2013	SVM	0		100	1	0.44
	[43] in 2018	Random Forest			98.44		2.2
	[249] in 2022	MLP	0.02	97.2	97.18		0.02

7.2.3 Fusion

Saevanee et al. [24] applied matching-level fusion on keystroke dynamics with behavior and linguistic profiling and increased the MLP reliability with an 8% overall EER. Zheng et al. [52] combined the features of acceleration, pressure, size, and time for typing a PIN on a smartphone touch screen. They evaluated the performance of fusing these modalities and achieved higher performance when compared to the results of single modalities. They achieved an EER of 3.65% with the k-NN. In [53] they collected slide swipe features, features of the arm movement while users carried the device towards their ear, and voice recognition features. Their multimodal system achieved a FAR of 11.01% and an FRR of 4.12% using the BayesNet. Li and Bours [122] collected data from the gyroscope, accelerometer, Bluetooth, and Wi-Fi and performed a score-level fusion. Their method achieved 9.67% EER with the Random Forest

for the score-level fusion. Volaka et al. [178] combined touchscreen scroll with accelerometer and gyroscope data from the Hand Movement, Orientation, and Grasp (HMOG) dataset, as provided by Sitova et al. [38]. By using the LSTM, they achieved 88% average Accuracy, 78% average TAR, and 15% EER. Lamiche et al. [179] employed gait patterns and keystroke dynamics and achieved an Accuracy of 99.11%, an average FAR of 0.684%, an FRR of 7%, and an EER of 1% with the MLP. Table 22 presents the fusion systems' performance.

Table 22: Research works on fusion.

Method	Publications	Classification	Performance (%)				
			FAR	TAR	Accuracy	FRR	EER
Fusion	[24] in 2011	MLP					8
	[52] in 2014	k-NN					3.65
	[53] in 2015	BayesNet	11.01			4.12	
	[122] in 2018	Random forest					9.67
	[178] in 2019	LSTM		78	88		15
	[179] in 2019	MLP	0.684		99.11	7	1

7.2.4 Discussion on related work

A plethora of combinations is used to authenticate individuals by fusing biometrics, which achieves improved results [24, 52, 53, 122, 178, 179]. In table 22, the best performance for each model separately is shown. The research aims to design and evaluate new approaches to CA using touch gestures and keystroke dynamics. The MLP and LSTM will be used since they have given good results, and it will be easier to compare them to the approaches of this research. Each modality will be evaluated separately under the zero-effort evaluation and a comparison of the results with those of the literature will be made (Table 20, Table 21). Then, an investigation will be made regarding if there can be an improvement of the performance with the feature-level fusion of biometrics and a comparison of the results with those of the literature will be made (Table 22).

7.3 Experimental setup

Following, the problem analysis, the data collection architecture, the features extraction process and the methodology are presented.

7.3.1 Problem Analysis

In BBCA systems there are some fundamental weaknesses such as achieving a balance between false positives / false negatives, that is, between security and usability [9, 193]. Most BBCA systems often operate with a high FRR at thresholds attempting to keep the FAR under 0.1% [9, 116, 193]. Of course, a false rejection (usability) is less costly than a false acceptance (security). A higher false acceptance rate will reduce the security level of the authentication system while a higher false rejection rate will block a legitimate user. However, this imbalance may make the whole system unusable. Thus, it is a critical topic to explore how to achieve a balance between security and usability.

7.3.2 Data collection architecture

We developed the BioGames paradigm [246] to collect behavioral biometrics from mobile device users and follows an innovative approach. This approach is about gamification of data collection. At the same time, a behavioral biometric collection tool (Biogames App) based on the BioGames example was developed. The Bio-Games App uses games and challenges that combine Keystroke Dynamics and Touch Gestures. Each category has 4 sessions and each session 4 games where the levels are becoming more difficult to complete. In the beginning, the user has access only to Game 1 of Session 1. Following, the user must complete all 4 games of session 1 to unlock the first game of the next session. If the user successfully completes game 1 and within the given timeframe, then the next game unlocks until the user success-fully completes all 4 games in each session. Also, in each game played the time limit decreases to collect typing data at different typing speeds. Finally, the typing games that are used are based on something that the user must recall from his/her memory, like a password, and games that are based on something that the user sees and types, like a captcha. BioGames App sends the data to an API that stores the data in the Aegean-DataBase. The Aegean-DataBase is designed

to allow multiple users to store their sensor data at any time. Thus, there is no concern about data separation and synchronization.

7.3.3 Features extraction

In this section, we describe the touch gestures, keystroke dynamics and fusion features extraction that we use in our experiments.

7.3.3.1 Touch gestures

Touch gestures are the strokes or swipes made on the screen of mobile devices. The BioGames app extracts the location points, timestamps, and touch pressure. Each of them can be encoded as a series of vectors [249]:

$$S_i = (x_i, y_i, t_i, p_i), i = \{1, 2, \dots, N\}, (6)$$

where x_i, y_i are location points, $t_i, p_i$are timestamps and screen touch pressure, respectively. Here, the total number of swipes is N.

Table 23 presents the touch gestures features of the BioGames app.

Table 23: Features of touch gestures.

Sensor	X_value	Y_value	Time	Pressure
Touch Screen (Gestrures)	646.8269	1248.5352	20	0.1
	652.2571	1227.4142	10	0.5
	790.6092	1199.5518	30	0.5

7.3.3.2 Keystroke dynamics

Users are identified based on their tapping habits by recording and analysing their typing inputs collected from the BioGames's App keyboard [16, 187]. Duration, latency, key pressure and location points of the fingers are extracted by BioGames App as described in [105, 110, 179, 187, 246]:

- Duration: the time between pressing and releasing a key.
- *Latency*: the time between releasing a pressed key until pressing the next key.
- *Pressure*: key pressure.
- *Location*: location points (xi, yi) on the screen.

Table 24 shows the database entries of keystroke dynamics that were sent by the BioGames app.

Table 24: Features of keystroke dynamics.

Sensor	Duration	Latency	Pressure	X_value	Y_value
Touch Screen (Keyboard)	134	189	1.0	943.0	404.0
	96	176	1.0	637.0	417.0
	57	358	0.50	339.0	243.0

7.3.3.3 Fusion

In feature-level fusion, the feature sets from multiple behavioral biometrics are unified into a single feature set [14, 187]. A new feature set that combines touch gestures and keystroke dynamics was developed. Table 25 presents the fusion features set.

Table 25: Fusion feature set

Modality	X_value (touch)	Y_value (touch)	Time	Pressure (touch)	Pressure (keystroke)	Duration	latency	X_value (kestroke)	Y_value (keystroke)
Fusion of touch gestures and keystrokes	0.410958	0.514873	606	0.05	0.08	0.605809	21516	5433	302196
	0.410958	0.514873	804	0.80	0.70	0.456432	64547	220472	178188
	0.506854	0.513326	952	0.50	0.07	0.46473	62796	49291	349696

7.3.4 Methodology

In the data collection process, the BioGames App [246] was installed on the mobile devices of 39 participants. Users play the games developed in their everyday environment, and the various hardware components collect the biometrics, as mentioned above. The BioGames App sends to the database all the data for each modality.

The process of touch gestures data collection has 16 sessions, where each session lasts approximately 2 minutes. The gestures of swipe down/ swipe up and swipe right/ swipe left which are commonly employed are collected. One or many finger touches, swiping down or up in a particular area are also collected, since they can be employed for continuous authentication [246]. Of the 39 participants in the sample, 38 are considered impostors, and one person is considered genuine.

The process of keystroke dynamics collection has 16 sessions, where each session lasts approximately 2 minutes. In the course of the sessions, there was a display of specific text or numbers and users had to type them directly after the display or memorize them and then type them. This resulted in two groups of inputs, one that participants must read and write immediately and another that participants read, memorize, and then write. Of the 39 participants in the sample, 38 are considered impostors, and one person is considered genuine.

Regarding fusion, the feature-level fusion of keystroke dynamics and touch gestures is applied and their unification into a single feature set consisting of 39 individuals and 1488 Instances. Of the 39 participants in the sample, 38 are considered impostors, and one person is considered genuine.

Lastly, a comparison of the performance of Multi-Layer Perceptron (MLP) and Long Short-Term Memory (LSTM) is made. Each modality is examined separately and an investigation is made regarding if there can be an improvement of the performance by applying feature-level fusion of keystroke dynamics and touch gestures.

7.4 Results

In this section, the performance of the MLP and the LSTM is evaluated. The TAR, FAR, TRR, FRR, Accuracy, and Equal Error Rate are calculated. The results achieved by the systems are presented below.

7.4.1 Touch gestures results

By using the collected data from the BioGames App a feature set with 4749 instances is created and normalized with scale 1.0. The LSTM was applied with the following configurations (table 26):

Table 26: Network configuration (*W: Weights, RW: Recurrent weights, b: Biases*).

VertexName (VertexType)	nIn, nOut	Total Params	Params Shape	Vertex Inputs
LSTM layer	5,2	64	W: {5,8}, RW:{2,8}, b:{1,8}	[input]
Output layer	2,2	6	W: {2,2}, b:{1,2}	[LSTM layer]

Also, the following configurations were applied on MLP:

- Learning rate (L): 0.3.
- Momentum: 0.2.
- Training time (N): 500.
- Hidden layers (H): 3.

With test mode 10-fold cross-validation the systems achieved:

- LSTM achieved: 77.5%Accuracy, 22% Equal Error Rate, 47.3% TAR, 89.8% TRR, 10.2% FAR and 52,7% FRR.
- MLP achieved: 77.2% Accuracy and 24.7% Equal Error Rate, 53.4% TAR, 86.9% TRR, 13.1% FAR and 46.6% FRR.

Table 27 summarizes the performance achieved for touch gestures.

Table 27: The results for touch gestures.

System	Accuracy	EER	TAR	TRR	FAR	FRR
LSTM	77.5%	22%	47.3%	89.8%	10.2%	52,7%
MLP	77.2%	24.7%	53.4%	86.9%	13.1%	46.6%

Table 28 presents the results by class.

LSTM has given the following results.

- Class Impostor: 89.8% TAR, 52.7% FAR.
- Class Genuine: 47.3% TAR, 10.2% FAR.
- Weighted Average: 77.5% TAR, 40.5% FAR.

MLP has given the following results.

- Class Impostor: 86.9% TAR, 46.6% FAR.
- Class Genuine: 53.4% TAR, 13.1% FAR.
- Weighted Average: 77.2% TAR, 36.6% FAR.

Table 28: Touch gestures results by class.

System	Modality	TAR	FAR	Class
LSTM	Touch Gestures	89.8%	52,7%	Impostor
		47.3%	10.2%	Genuine
Weighted Avg.		77.5%	40.5%	
MLP	Touch Gestures	86.9%	46.6%	Impostor
		53.4%	13.1%	Genuine
Weighted Avg.		77.2%	36.6%	

7.4.2 Keystroke dynamics results

By using the collected data from the BioGames App a feature set from 1488 instances was created and normalized with scale 1.0. The LSTM was applied with the following configurations (table 29):

Table 29: Network configuration (*W: Weights, RW: Recurrent weights, b: Biases*).

VertexName (VertexType)	nIn, nOut	Total Params	Params Shape	Vertex Inputs
LSTM layer	5,2	64	W: {5,8}, RW:{2,8}, b:{1,8}	[input]
Output layer	2,2	6	W: {2,2}, b:{1,2}	[LSTM layer]

Also, the following configurations were applied on MLP:

- Learning rate (L): 0.3.
- Momentum: 0.2.

- Training time (N): 500.
- Hidden layers (H): 3.

With test mode 10-fold cross-validation the systems achieved:

- LSTM achieved: 96.1% Accuracy, 3% Equal Error Rate, 100% TAR, 92.4% TRR, 7.6% FAR and 0% FRR.
- MLP achieved: 97.17% Accuracy and 2% Equal Error Rate, 100% TAR, 94.5% TRR, 5.5% FAR and 0% FRR.

Table 30 summarizes the performance for keystroke dynamics.

Table 30: The results for keystroke dynamics.

System	Accuracy	EER	TAR	TRR	FAR	FRR
LSTM	96.1%	3%	100%	92.4%	7.6%	0%
MLP	97.17%	2%	100%	94.5%	5.5%	0%

Table 31 presents the results by class.

LSTM has given the following results.

- Class Impostor: 92.4% TAR, 0% FAR.
- Class Genuine: 100% TAR, 7.6% FAR.
- Weighted Average: 96.1% TAR, 3.7% FAR.

MLP has given the following results.

- Class Impostor: 94.5% TAR, 0% FAR.
- Class Genuine: 100% TAR, 5.5% FAR.
- Weighted Average: 97.2% TAR, 2.7% FAR.

Table 31: The keystroke dynamics results by class.

System	Modality	TAR	FAR	Class
LSTM	Keystroke	92.4%	0%	Impostor
		100%	7.6%	Genuine
Weighted Avg.		96.1%	3.7%	
MLP	Keystroke Dynamics	94.5%	0%	Impostor
		100%	5.5%	Genuine
Weighted Avg.		97.2%	2.7%	

7.4.3 Fusion of touch gestures and keystrokes results

From the data collected with the BioGames App, both from keystroke dynamics and touch gestures, a feature set was created in which feature-level fusion was applied and it was unified into a single feature set that consists of 1488 Instances. Also, it was normalized with scale 1.0.

The following configurations were applied on LSTM (table 32):

Table 32: Network configuration (*W: Weights, RW: Recurrent weights, b: Biases*).

VertexName (VertexType)	nIn, nOut	Total Params	Params Shape	Vertex Inputs
LSTM layer	9,2	96	W: {9,8}, RW:{2,8}, b:{1,8}	[input]
Output layer	2,2	6	W: {2,2}, b:{1,2}	[LSTM layer]

Also, the following configurations were applied on MLP:

- Learning rate (L): 0.3.
- Momentum: 0.2.
- Training time (N): 500.
- Hidden layers (H): 3.

With the test mode 10-fold cross-validation the systems achieved:

- LSTM achieved: 95.09% Accuracy, 4% Equal Error Rate, 99.6% TAR, 90.8% TRR, 9.2% FAR and 0.4% FRR.
- MLP achieved: 98.3% Accuracy and 1% Equal Error Rate, 99.4% TAR, 97.4% TRR, 2.6% FAR and 0.6% FRR.

Table 33 summarizes the performance for fusion.

Table 33: The results for fusion.

System	Accuracy	EER	TAR	TRR	FAR	FRR
LSTM	95.09%	4%	99.6%	90.8%	9.2%	0.4%
MLP	98.3%	1%	99.4%	97.4%	2.6%	0.6%

Table 34 presents the results by class.

LSTM has given the following results.

- Class Impostor: 90.8% TAR, 0.4% FAR.
- Class Genuine: 99.6% TAR, 9.2% FAR.
- Weighted Average: 95.1% TAR, 4.7% FAR.

MLP has given the following results.

- Class Impostor: 97.4% TAR, 0.6% FAR.
- Class Genuine: 99.4% TAR, 2.6% FAR.
- Weighted Average: 98.4% TAR, 1.6% FAR.

Table 34: Fusion results by class.

System	Modality	TAR	FAR	Class
LSTM	Fusion Touch Gestures & Keystroke	90.8%	0.4%	Impostor
		99.6%	9.2%	Genuine
Weighted Avg.		95.1%	4.7%	
MLP	Fusion Touch Gestures & Keystroke	97.4	0.6	Impostor
		99.4	2.6	Genuine
Weighted Avg.		98.4	1.6	

7.5 Discussion

In this chapter a comparative study between MLP and LSTM on the development of a keystroke dynamics and touch gestures CA system was presented. Each modality was examined separately and then an investigation was made regarding if there can be an improvement of the performance by using the feature-level fusion to solve security and usability issues that occurred. A discussion of the results follows.

7.5.1 Touch gestures

By applying the touch gestures feature set both systems achieved a not-so-high performance. The LSTM achieved: 77.5% Accuracy, 22% Equal Error Rate, 47.3% TAR, 89.8% TRR,

10.2% FAR and 52,7% FRR. The MLP achieved: 77.2% Accuracy and 24.7% Equal Error Rate, 53.4% TAR, 86.9% TRR, 13.1% FAR and 46.6% FRR.

In relation to the literature, both the MLP and the LSTM have had lower performance. The not-so-good performance in touch gestures is due to the user playing games with the BioGames App and for this reason, do not make the same movements and the systems fail to understand these changes in the users. This is an indication that the BioGames paradigm gives us data that are very close to the actual use of the devices, as opposed to a controlled behavioral biometrics collection methodology where users would make specific, researcher-led moves.

Comparing the performance of the two systems it is noticed that both have a not-so-high performance in all metrics. LSTM has a slightly better performance as it has higher Accuracy, TAR, and TRR, while it has a lower Equal Error Rate and FAR, compared to MLP. In conclusion, in this context, both systems did not perform so well in terms of security and usability.

7.5.2 Keystroke dynamics

By applying the keystroke dynamics feature set both systems achieved high performance. The LSTM achieved: 96.1% Accuracy, 3% Equal Error Rate, 100% TAR, 92.4% TRR, 7.6% FAR and 0% FRR. The MLP achieved: 97.17% Accuracy and 2% Equal Error Rate, 100% TAR, 94.5% TRR, 5.5% FAR and 0% FRR.

In relation to the literature, both LSTM and MLP achieved better performance. In [44] the FFNN performed relatively low achieving a FAR of 14%, an Accuracy of 86%, and an FRR of 2.2%. In [40] average EERs of 12.8% were achieved with the MLP. Finally, almost the same results with MLP as in [249] were achieved.

Comparing the performance of the two systems it is firstly noticed that both have a high performance in all metrics. The MLP, however, clearly has better performance as it has higher Accuracy, TAR, and TRR while respectively lower Equal Error Rate and FAR. In the Genuine class, both systems performance is 100%. In conclusion, in this context, both systems performed perfect, but MLP is superior to LSTM.

7.5.3 Fusion

Taking all this into account, an investigation was made regarding if there could be an improvement in the performance for touch gesture modality by applying fusion with keystroke dynamics to solve these security and usability issues of touch gestures. By applying the feature-level fusion feature set both systems achieved high performance. The LSTM achieved: 95.09% Accuracy, 4% Equal Error Rate, 99.6% TAR, 90.8% TRR, 9.2% FAR and 0.4% FRR. The MLP achieved: 98.3% Accuracy and 1% Equal Error Rate, 99.4% TAR, 97.4% TRR, 2.6% FAR and 0.6% FRR.

In relation to the literature both LSTM and MLP achieved a better performance except for Accuracy and FAR in [179]. In [179] the MLP achieved 7% FRR, and 1% EER. The MLP of the present thesis also achieved EER of 1% but a better usability with an FRR of 0.6%. Also, the LSTM achieved better FRR 0.4%. In [24] the MLP achieved EER 8%. In [52] the k-NN achieved 3.65% EER. In [53], the BayesNet achieved 11.01% FAR and 4.12% FRR. In [122] the Random Forest achieved 9.67% EER. Finally, in [178] the LSTM achieved an average accuracy of 88%, an EER of 15% and an average TAR of 78%.

By comparing the performance of both systems, it is observed that they both achieve a high performance in all metrics. The performance of LSTM in improved to a great extent. The model achieved Accuracy 95.09% (increased 17.59%), EER 4% (The error was reduced by 19%), the TAR 99.6% (increased 17,6%), the TRR 90.8% (increased 1%), the FAR 9.2% (reduced by 1%) and the FRR 0.4% (reduced by 52.3%). The performance of MLP is also greatly improved. The model achieved Accuracy 98.3% (increased 21.1%), EER 1% (The error was reduced by 23.7%), the TAR 99.4% (increased 46%), the TRR 97.4% (increased 10%), the FAR 2.6% (reduced by 10.5%) and the FRR 0.6% (reduced by 46%).

In conclusion, the MLP is superior to LSTM in this context. It is shown that the feature-level fusion of touch gestures and keystroke dynamics improves the performance of the systems and solves both security and usability issues.

7.5.4 Limitations

High effort approaches should be used to evaluate the systems [83, 131, 146, 150, 151]. A sample of 39 individuals was used to test the systems and there are plans to evaluate them in a larger sample of users. Large amounts of training data are normally required for deep learning models.

7.6 Conclusions

In this chapter, a comparative study between MLP and LSTM on the development of a CA system that is based on the user's touch gestures and keystroke dynamics was presented. Each modality was examined separately and an investigation was made regarding if there could be an improvement of the performance results of touch gestures, by applying feature-level fusion with keystroke dynamics. It is shown that the feature-level fusion of touch gestures and keystroke dynamics improves the performance of the systems and solves security and usability issues. The MLP achieved greater improvement and better performance compared to the LSTM. The MLP achieved Accuracy 98.3% (increased 21.1%), EER 1% (the error was reduced by 23.7%), the TAR 99.4% (increased 46%), the TRR 97.4% (increased 10%), the FAR 2.6% (reduced by 10.5%) and the FRR 0.6% (reduced by 46%).

8

Summary and Conclusions

8.1 Introduction

This doctoral thesis includes four research stages that each address one of the research questions. These are the research stages of a designed single project. First, an extensive systematic literature review is presented that maps the research area and identifies challenges and open problems. Then, a new theoretical framework is presented, to investigate the key factors that show us the user requirements that influence the adoption of BBCA technology. In the third stage, a new paradigm (BioGames paradigm) and a new tool (BioGames App) for collecting behavioral biometric data that follows an innovative approach, are presented. This approach is about the gamification of data collection. In the fourth stage, an experimental data collection process of keystroke dynamics and touch gestures is applied by using smartphones, and a comparison is made between Multi-Layer Perceptron (MLP) and Long Short-Term Memory (LSTM). Each modality is examined separately and an investigation is made regarding the improvement of performance by applying feature-level fusion of keystroke dynamics and touch gestures to solve either security or usability issues.

8.2 Research stage 1

In the first stage, an extensive survey is presented that maps the research area. The main objective of the research was to answer the research question: What are the challenges, the open issues, and the future trends of BBCA technology? To answer the question an extensive literature review on BBCA technology and the performance of machine learning systems was conducted. Additionally, another literature review on potential attack vectors on BBCA systems was conducted and promising countermeasures were highlighted. Also, a classification of behavioral biometrics (Behavioral Biometrics - BB) into seven categories and the analysis

of their collection and feature extraction methodologies were carried out. Finally, challenges, open issues, and future trends are identified.

The research showed that CA technology is a promising method with many advantages. It can operate without user intervention, requires no additional hardware, and exhibits high accuracy. A large corpus of research has shown evidence regarding the superiority of the fusion of multimodal biometric approaches. A variety of combinations is used with the fusion of biometrics that achieves improved results compared to the single modality methods. Thus, the fusion of multimodal biometrics authentication emerges as a definite future trend. There is also evidence that the fusion of multimodal biometrics in combination with the Zero Interaction Authentication (ZIA) paradigm may also be a trend.

Of course, several challenges and open issues were identified, which were resolved in this doctoral thesis, such as the investigation of the factors of technology acceptance by users. Also, in the bibliography was found the need for a user-friendly BB collection methodology. A major challenge is the design of a methodology for collecting behavioral biometrics, in a way that makes it user-friendly. The selection and optimization of a proper set of behavioral biometrics constitutes a challenge and an open issue. Also, behavioral biometrics continuous authentication is subject to limitations, such as risk of false positives/false negatives, i.e., balance between security and usability resulting in its limited applicability. To overcome these limitations, it is crucial to maximize accuracy and examine how to find a balance between security and usability.

Research contribution of this stage:

- A classification of behavioral traits on seven categories and an analysis of behavioral biometrics collection methodologies and feature extraction.
- A wide range, state-of-the-art literature review on BBCA technology and the performance of machine learning systems.
- A literature review on possible attack vectors on BBCA technology and a highlight on promising countermeasures.
- Identification of challenges, open issues, and future trends.

8.3 Research stage 2

The main goal of the second research stage of this thesis was to answer the research question: Which are the key factors of user acceptance (or rejection) of BBCA technology? The challenges and limitations in the application of biometric technology are not understood sufficiently. As a result, many organizations are investing less or not at all in such technologies [188, 192]. This research constitutes an exploration of the key factors of behavioral intent to adopt BBCA technology. It provides detailed information and several useful insights and new knowledge for researchers, practitioners, governments, and the providers of BBCA technology. To answer the research question, the effect of various factors on Behavioral Intention to adopt technology (Behavioral Intention - BI) was investigated through a new integration of the Technology Acceptance Model (TAM) and the Diffusion of Innovation Theory (DOI). Also, a new theoretical framework was developed with constructs such as Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC) and Perceived Risk of Technology Use (PROU). In addition, the constructs Trust in Technology (TT) and Innovativeness (Innov) were used. It was found that the main Facilitators of Behavioral Intention are Trust in Technology (TT), followed by Compatibility (COM), Perceived Usefulness (PU) and Innovativeness (INNOV). Trust in technology is a factor that must be considered for the success of future investments. A factor that may decrease trust in technology is biometrics privacy concerns. Users are concerned about their biometrics and believe that they may be sent to third parties. Therefore, a suggestion is made that research should concentrate towards the preservation of their biometrics privacy. To achieve this, behavioral measurements should be processed on the mobile device of users, and biometrics are not sent to the online service. A device-centric approach is likely to increase the trust in technology and consequently lead to BI. Also, Shila et al. [242] reported that the cloud-based authentication was outperformed by the device-centric implementation in terms of detection latency and classification accuracy. Moreover, there are specific and appropriate security measures that should be established in BBCA systems, as, the encryption of biometric data both in the database and the device. Finally, it is necessary providers of BBCA technology adopt different approaches in building users' initial trust in technology. There are two types of users e.g., young people who trust such technologies and

people unfamiliar with biometric technologies. In the first case, the providers must introduce added-value services to them and in the latter case, service providers must emphasize usefulness.

Similarly, the compatibility is one of the factors that can lead to the adoption of technology. In this research, it is shown that individuals who believe that the usage of the BBCA technology would fit well with the way they want to secure their personal data and accounts (e.g., bank accounts, e-mail, etc.), have a higher intent to adopt this technology. Moreover, individuals who believe that BBCA would fit into their lifestyle have a higher appraisal of ease-to-use and perceived usefulness. So, providers can run a more cost-effective advertising campaign by comparing the BBCA to entry-point authentication technology as well as traditional methods (e.g., eliminating the necessity to remember PINs or passwords).

Another factor that must be considered is usefulness. Individuals are concerned about their security and privacy from a possible breach of the security mechanism. This leads them to recognize the usefulness of BBCA technology as it will protect their assets and personal data. Thus, it is essential that accuracy is maximized and to investigate how to find a balance between usability and security. Innovation is also one of the factors that can help BBCA Technology Suppliers to promote technology to a relevant audience first. For instance, they can reach their target group through magazines focusing on new technologies, discussion groups or seminars. In this way, their promotional advertising campaign can be more effective with a greater chance of gaining the targeted market share.

For the new constructs added, the results support the hypothesis that Security & Privacy Risks (SPR) is a facilitator of Perceived Usefulness (PU). Also, PU acts as a facilitator of Behavioral Intention to adopt technology (BI). Consequently, individuals who do not feel sufficiently protected by classic authentication methods will consider the usefulness of BBCA technology for their additional protection against risks. Also, with the constructs Biometrics Privacy Concerns (BPC) and Perceived Risk of Using the technology (PROU) it was examined whether individuals' concerns about their biometric privacy act as inhibitors to BI. It was concluded that individuals consider the benefits related to the security of their assets (e.g., money in a bank account) from using BBCA technology to be far more important than the perceived risks

to the privacy of their biometrics. This results from the fact that the hypothesis that the main inhibitor of BI is the construct Perceived Risk of Using the technology (PROU) is not supported by the model. The new constructs were used to extend the TAM model and address its limitations in addressing security and privacy issues. Therefore, it is proposed that this new theoretical framework is combined with TAM for research on the adoption of biometric and continuous authentication technologies. Finally, this model may also be used to design policies for increasing the adoption of the BBCA technology.

Research contribution of this stage:

- It proposes a new integration of a modified TAM model and DOI theory, which examines the influence of various factors on BBCA's behavioral intent of adoption.
- A new theoretical framework is created with constructs such as Security & Privacy Risks (SPR), Biometrics Privacy Concerns (BPC) and Perceived Risk of Using the Technology (PROU).
- A research model focused on BBCA technology is developed that can be used by researchers, practitioners, governments, decision-makers, and providers of BBCA technology.

8.4 Research stage 3

The main objective in the third research stage of the present thesis was to answer the research questions: Is there a need for the development of a new paradigm for the collection of behavior biometrics data for research purposes? Could this new paradigm be supported by an effective behavioral biometrics collection tool? It has been observed in the literature that a major challenge and open problem, for research related to the development of BBCA systems, is the collection and refinement of an appropriate set of behavioral biometric data. The issue is compounded by the fact that most users avoid engaging in the time-consuming, laborious processes involved in collecting research biometric data. For this reason, developing and testing a user-friendly biometric collection methodology and tool is another major challenge. Also, as shown in the current behavioral biometrics collection technologies, there are no tools available that combine the keystroke and touch gesture modalities.

In response to these challenges, in the third stage of the research, a new behavioral biometric data collection paradigm, called the BioGames paradigm, is presented and follows an innovative approach. This approach is about the gamification of data collection. At the same time, a behavioral biometric collection tool (Biogames App) based on the BioGames example was developed. The BioGames App uses games and challenges that combine Keystroke Dynamics and Touch Gestures. In touch gestures, the types of games that are used collect gestures that are widely used. Also, some special gestures are collected such as single or multiple finger touches and swipe up or down in a specific area, because they could be used for continuous authentication. As for keystroke dynamics, in each game, the time limit decreases to collect typing data at different typing speeds. Finally, the typing games that are used are based on something that the user must recall from his/her memory, like a password, and games that are based on something that the user sees and types, like a captcha.

Research contribution of this stage:

- Presentation of a new paradigm, named BioGames, that suggests a user-friendly and entertaining way for the collection of behavioral biometrics for users of mobile devices.
- Development of a novel behavioral biometrics collection tool, named BioGames App, which is freely available for researchers and practitioners.
- Development of new appropriate feature sets for continuous authentication of touch gestures and keystroke dynamics.
- Introduction of a convenient data collection methodology by which the behavioral biometrics of the users can be collected via BioGames.

8.5 Research stage 4

The fourth stage of the research was related to the design and evaluation of new approaches to continuous authentication using Keystroke Dynamics and Touch Gestures. The main objective of the fourth research stage was to answer the research question: Does feature-level fusion of touch gestures and keystroke dynamics improve the performance of deep learning systems and address both security and usability issues? According to the literature [1, 9, 187, 193], most

studies use single behavioral modality methods to authenticate users. However, the behaviors of genuine users may change, and systems fail when significant changes occur [187, 193]. The above, result in either security or usability issues. For example, a false rejection that diminishes usability is less costly than a false acceptance that diminishes security. A higher false acceptance rate will reduce the security level of the authentication system, while a higher false rejection rate will block a genuine user [9, 193]. In the literature, the fusion of biometrics is used to solve this problem and achieves improved results. In this research, each behavioral biometric case was examined separately and the case of improving performance results with a feature-level fusion of touch gestures and dynamic typing was investigated. In the present approach a comparison is made between deep neural networks designed for data that entail important temporal dynamics, such as Multi-Layer Perceptron (MLP), and deep networks designed for independently distributed data, such as Long Short-Term Memory (LSTM).

By applying the touch gestures feature set both systems achieved a not-so-high performance. The not-so-good performance in touch gestures is due to the user playing games with the BioGames App and for this reason, do not make the same movements and the systems fail to understand these changes. This is an indication that the BioGames paradigm gives us data that are very close to the actual use of the devices, as opposed to a controlled behavioral biometrics collection methodology where users would make specific, researcher-led moves. In conclusion, in this context, both systems did not perform so well in terms of security and usability. By applying the keystroke dynamics feature set both systems achieved high performance. In relation to the literature, both LSTM and MLP achieved better performance. In the Genuine class, both systems performance is 100%. In conclusion, in this context, both systems performed perfect, but MLP is superior to LSTM.

Taking all this into account, an investigation was made regarding if there could be an improvement in the performance for touch gesture modality by applying fusion with keystroke dynamics to solve these security and usability issues of touch gestures. By applying the feature-level fusion dataset both systems achieved high performance. In relation to the literature both LSTM and MLP achieved a better performance. By comparing the performance of both

systems, the MLP is superior to LSTM in this context. The MLP achieved greater improvement and better performance compared to the LSTM. The MLP achieved Accuracy 98.3% (increased 21.1%), EER 1% (the error was reduced by 23.7%), the TAR 99.4% (increased 46%), the TRR 97.4% (increased 10%), the FAR 2.6% (reduced by 10.5%) and the FRR 0.6% (reduced by 46%). In relation to the literature, both LSTM and MLP achieved a better performance. From the results of the research it is shown that the feature-level fusion of touch gestures and keystroke dynamics improves the performance of the systems and solves both security and usability issues.

Research contribution of this stage:

- Development of a new appropriate feature set for continuous authentication that combines touch gestures and keystroke dynamics.
- A comparative study between MLP and LSTM on the development of a BBCA system is provided.
- Is shown that the feature-level fusion of touch gestures and keystroke dynamics improves the performance of the systems.
- Is shown that the feature-level fusion of touch gestures and keystroke dynamics solves both security and usability issues.
- Is shown that MLP is superior to LSTM in this context.

8.6 Future research

Future research could be conducted by extending the BBCA technology behavioral intention adoption model to desktop computers or even Internet of Things (IoT) devices. In addition, many external factors need to be explored such as consumer traits [228], situational factors [229], product characteristics [230], and previous experiences [231].

Future research could also focus on the extension of the BioGames App to include more behavioral modalities. Also, the creation of database with data collected from a larger population that will be publicly available.

Finally, future research could be focused on the evaluation of the deep learning systems under the high effort approaches to see the performance under the spectrum of today's possible threats and highlight relevant countermeasures.

Acknowledgments

This research has been financially supported by the General Secretariat for Research and Technology (GSRT) and the Hellenic Foundation for Research and Innovation (HFRI) (Scholarship Code: 13).

References

[1] I. Stylios, O. Thanou, I. Androulidakis., E. Zaitseva, A review of continuous authentication using behavioral biometrics, in: Conference: ACM SEEDA-CECNSM, At Kastoria, Greece, 2016, https://doi.org/10.1145/ 2984393.2984403.

[2] I. Stylios, S. Chatzis, O. Thanou, S. Kokolakis, S, (2015). Mobile Phones & Behavioral Modalities: Surveying Users' Practices. TELFOR 2015 International IEEE Conference, At SAVA Center, Belgrade, Serbia. DOI: 10.1109/TELFOR.2015.7377614.

[3] P. Corcoran, C. Costache, "Biometric Technology and Smartphones: a consideration of the practicalities of a broad adoption of biometrics and the likely impacts, IEEE Consumer Electronics Magazine 5 (2) (2016) 70–78, https://doi. org/10.1109/MCE.2016.2521937.

[4] R. Dash & P. Dash, (2017). MDHS–LPNN: A hybrid FOREX predictor model using a legendre polynomial neural network with a modified differential harmony search technique. Chapter 25. 10.1016/b978-0-12-811318-9.00025-9.

[5] N.L. Clarke, S.M. Furnell, Authentication of users on mobile telephones – a survey of attitudes and practices, Comput. Secur. 24 (2005) 519–e527.

[6] P. Pons, P. Polak, Understanding user perspectives on biometric technology, Commun. ACM 51 (9) (2008) 115–118.

[7] N.L. Clarke, S.M. Furnell, P.M. Rodwell, P.L. Reynolds, Acceptance of subscriber authentication methods for mobile telephony devices, Comput. Secur. 21 (3) (2002) 220–228.

[8] S. Karatzouni, S.M. Furnell, N.L. Clarke, R.A. Botha, Perceptions of user authentication on mobile devices, in: Proceedings of the 6th Annual ISOnEworld Conference, April 11-13, 2007, Las Vegas, NV, 2007.

[9] W. Meng, D.S. Wong, S. Furnell, J. Zhou, Surveying the development of biometric user authentication on mobile phones, IEEE Commun. Surv. Amp Tutor. 17 (2015) 1268–1293, https://doi.org/10.1109/COMST.2014.2386915.

[10] R.E. Crossler, A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, R. Baskerville, Future directions for behavioral information security research, Comput. Secur. 32 (2013) 90–101.

[11] A. Mahfouz, T.M. Mahmoud, A.S. Eldin, A survey on behavioral biometric authentication on smartphones, J. Inf. Secur. Appl. 37 (2017) 28–37.

[12] F. Cherifi, B. Hemery, R. Giot, M. Pasquet, C. Rosenberger, Performance evaluation of behavioral biometric systems. Behavioral Biometrics for Human Identification: Intelligent Applications, IGI Global, 2010, pp. 57–74.

[13] S. Furnell, N. Clarke, S. Karatzouni, Beyond the PIN: Enhancing user authentication for mobile devices, Comput. Fraud Secur. 2008 (8) (2008). Elsevier.

[14] C. Sanderson and K. K. Paliwal, (2002). Information fusion and person

verification using speech and face information. Research Paper IDIAP-RR 02-33, IDIAP.
[15] L. Zhang, B. Tiwana, X. Qian, Z. Wang, R.P. Dick, Z.M. Mao, L. Yang, Accurate online power estimation and automatic battery behavior-based power model generation for smartphones, in: Proceedings of the eighth IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis, ACM, 2010, p. 105{114.
[16] T-Y. Chang, C.J. Tsai, W.J. Tsai, C.C. Peng, H.S. Wu, A changeable personal identification number-based keystroke dynamics authentication system on smartphones, Secur. Commun. Netw. 2016 9 (2016) 2674–2685. Wiley Online Library (wileyonlinelibrary.com).
[17] F. Bergadano, D. Gunetti, C. Picardi, User authentication through keystroke dynamics, ACM Trans. Inf. Syst. Secur. (TISSEC) 5 (4) (2002) 367–397. November 2002.
[18] A.Jain Ross, Information fusion in biometrics, Pattern Recogn. Lett. 24 (13) (2003) 2115–2125, https://doi.org/10.1016/S0167-8655(03)00079-5.
[19] A.K.Jain Ross, Multimodal biometrics: an overview, in: Signal Processing Conference, 2004 12thEuropean, 2004, pp. 1221–1224.
[20] A.K Ross, K. Nandakumar, Jain A.K, Introduction to multi biometrics, in: A. K. Jain, P. Flynn, A.A. Ross (Eds.), Handbook of Biometrics, Springer, Boston, MA, 2008.
[21] M. Faundez-Zanuy, Data fusion in biometrics, IEEE Aerosp. Electron. Syst. Mag. 20 (1) (2005) 34–38, 2005.
[22] H. Chen, C.Y. Chen, Optimal fusion of multi-modal biometric authentication using wavelet probabilistic neural network, in: IEEE International Symposium on Consumer Electronics, 2013, pp. 55–56.
[23] S. Ben-Yacoub, Y. Abdeljaoued, E. Mayoraz, (1999). Fusion of face and speech data for person identity verification. Research Paper IDIAP-RR 99-03, IDIAP, CP 592, 1920 Martigny, Switzerland.
[24] H. Saevanee, N.L. Clarke, S.M. Furnell, Multi-modal behavioural biometric authentication for mobile devices, IFIP Int. Inf. Secur. Conf. (2012) 465–474. SEC 2012: Information Security and Privacy Research.
[25] H. Saevanee, N. Clarke, S. Furnell, V. Biscione, Continuous user authentication using multi-modal biometrics, Comput. Secur. 53 (2015) 234–246.
[26] F.T. Liu, K. Ting, Z.H. Zhou, Isolation Forest. eighth IEEE international conference on data mining, ICDM 08 (2009) 413–422, https://doi.org/10.1109/ICDM.2008.17.
[27] L. Rabiner, B. Juang, An introduction to hidden Markov models, IEEE ASSP Mag. 3 (1) (1986) 4–16.
[28] Y. Oner, T. Tunc, E. Egrioglu, Y. Atasoy, Comparisons of logistic regression and artificial neural networks in lung cancer data, Am. J. Intell. Syst. (2013) 71–74, https://doi.org/10.5923/j.ajis.20130302.03

[29] T. Feng, X. Zhao, W. Shi, Investigating Mobile Device Picking-up motion as a novel biometric modality, in: IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1–6.
[30] N. Al-Naffakh, N. Clarke, P. Haskell-Dowland, F. Li, (2016). Activity recognition using wearable computing. 10.1109/ICITST.2016.7856695.
[31] N. Al-Naffakh, N. Clarke, F. Li, P. Haskell-Dowland, Unobtrusive Gait Recognit. Using Smartwatches (2017), https://doi.org/10.23919/BIOSIG.2017.8053523.
[32] H. Saevanee, P. Bhatarakosol, User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device, in: Int. Conf. Comput. Electr. Eng., 2008, pp. 82–86. Page(s).
[33] M. Frank, R. Biedert, E. Ma, I. Martinovic, D. Song, Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication, IEEE Trans. Inf. Forensics Secur. 8 (1) (2013) 136–148, https:// doi.org/10.1109/TIFS.2012.2225048.
[34] L. Li, X. Zhao, G. Xue, Unobservable re-authentication for smartphones, in: Proceedings of the 20th Annual Network & Distributed System Security Symposium, NDSS2013. Internet Society, 2013.
[35] X. Zhao, T. Feng, W. Shi, Continuous mobile authentication using a novel Graphic Touch Gesture Feature, in: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1–6.
[36] C. Bo, L. Zhang, T. Jung, J. Han, X.-Y. Li, Y. Wang, Continuous user identification via touch and movement behavioral biometrics, in: Performance Computing and Communications Conference (IPCCC), 2014 IEEE International, 2014, p. 1{8.
[37] H. Xu, Y. Zhou, M.R. Lyu, (2014). Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones. Symposium On Usable Privacy and Security (SOUPS 2014). USENIX Association. ISBN Number 978-1-931971-13-3.
[38] Z. Sitova´, J. Sˇedˇenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, K.S. Balagani, HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users, IEEE Trans. Inf. Forensics Secur. 11 (5) (2015) 877–892. Page(s).
[39] Buriro, B. Crispo, F. Delfrari, K. Wrona, (2016). Hold & sign: a novel behavioral biometrics for smartphone user authentication conference: Mobile Security Technologies (MoST) 2016 in conjunction with IEEE Security and Privacy (S&P 16).
[40] N.L. Clarke, S.M. Furnell, Authenticating mobile phone users using keystroke analysis, Int. J. Inf. Secur. 6 (1) (2007) 1–14.
[41] T. Feng, X. Zhao, B. Carbunar, W. Shi, Continuous mobile authentication using virtual key typing biometrics, in: Published in: TRUSTCOM ’13 Proceedings of the 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, DC, USA., IEEE

Computer Society Washington, 2013, pp. 1547–1552. ISBN: 978-0-7695-5022-0.
[42] D. Buschek, A. De Luca, F. Alt, Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices, in: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015, pp. 1393–1402. ISBN: 978-1-4503-3145-6.
[43] S. Krishnamoorthy, Identification of user behavioural biometrics for authentication using keystroke dynamics and machine learning, Electron. Theses Dissertations (2018) 7440.
[44] J. Zhu Draffin, J.Y. Zhang, KeySens: passive user authentication through micro- behavior modeling of soft keyboard interaction, MobiCASE. (2013), https://doi. org/10.1007/978-3-319-05452-0_14.
[45] O. Klein, Generalization of Einstein's principle of equivalence so as to embrace the field equations of gravitation, Phys. Scr. 9 (2) (1974) 69.
[46] M.J.L. Orr, Introduction to radial basis function networks, Centre for Cognitive Science University of Edinburgh, 1996 [online]. Available, https://www.cc.gate ch.edu/~isbell/tutorials/rbf-intro.pdf. Accessed 20/3/2019.
[47] K. S. Killourhy, & R. A. Maxion, (2010). Why did my detector do that?! - predicting keystroke-dynamics error rates. RAID.
[48] D.W. Aha, D. Kibler, Instance-based learning algorithms, Mach. Learn. 6 (1991) 37–66.
[49] M.D. Corner, B.D. Noble, Zero-interaction authentication, in: Proc. 8th annual international conference on Mobile computing and networking, 2002, p. 1{11. MobiCom '02.
[50] T. Neal, D. Woodard, A. Striegel, Mobile device application, bluetooth and wi-fi usage data as behavioral biometric traits, in: IEEE International Conference on Biometrics Theory, Applications and Systems, 2015, pp. 1–6.
[51] Protect devices and data by letting users be themselves [online]. Available: https://www.kryptowire.com/continuous-authentication/, accessed on June., 6, 2020.
[52] N. Zheng, K. Bai., H. Huang, H. Wang, You are how you touch: user verification on smartphones via tapping behaviors, in: IEEE 22nd International Conference on Network Protocols, 2014, pp. 221–232. Page(s).
[53] A. Buriro & B. Crispo, & F. Del Frari, & J. Klardie, & K. Wrona, (2015). ITSME: multi-modal and unobtrusive behavioural user authentication for smartphones. 9551. 10.1007/978-3-319-29938-9_4.
[54] W. Shi, J. Yang, Y. Jiang, F. Yang, T. Feng, Y. Xiong, SenGuard: Passive user identification on smartphones using multiple sensors, in: International Conference on Wireless and Mobile Computing, Networking and Communications, 2011, pp. 141–148, https://doi.org/10.1109/ WiMOB.2011.6085412
[55] N.D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, A.T. Campbell, A

survey of mobile phone sensing, IEEE Commun. Mag. Arch. 48 (9) (2010) 140–150. IEEE Press Piscataway, NJ, USA.
[56] A. Ross, A. Rattani, M. Tistarelli, Exploiting the “doddington zoo” effect in biometric fusion, in: Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems, BTAS’09, Piscataway, NJ, USA, IEEE Press, 2009, pp. 264–270.
[57] L. Ballard, D. Lopresti, F. Monrose, Forgery quality and its implications for behavioral biometric security, Trans. Syst. Man Cybern. Part B 37 (5) (2007) 1107–1118.
[58] I.C. Stylios, S. Kokolakis, O. Thanou, S. Chatzis, User’s attitudes on mobile devices: can users’ practices protect their sensitive data?, in: 10th Mediterranean Conference on Information Systems, Cyprus, 2016.
[59] A. Serwadda, V.V. Phoha, When kids’ toys breach mobile phone security, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS ’13). ACM, New York, NY, USA, 2013, pp. 599–610, https://doi.org/10.1145/2508859.2516659.
[60] R. Kumar, V.V. Phoha, A. Jain, "Treadmill attack on gait-based authentication systems, in: IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), Arlington, VA, 2015, pp. 1–7, 2015.
[61] L. Breiman, Random forests, Mach. Learn. 45 (1) (2001) 5–32.
[62] C. Cortes, V. Vapnik, Support-vector networks, Mach. Learn. 20 (3) (1995) 273–297.
[63] R. Duda, P. Hart, D. Stork, Pattern Classification, 2nd edition, John Wiley and Sons, 2002.
[64] B. Shrestha, M. Mohamed, and N. Saxena, (2016). “Walk-unlock: Zero-interaction authentication protected with multi-modal gait biometrics,” CoRR, vol. abs/1 605.00766.
[65] J. Aviv, K. Gibson, E. Mossop, M. Blaze, J.M. Smith, Smudge attacks on smartphone touch screens, in: Published in: WOOT’10 4th USENIX conference on Offensive technologies, 2010. Article No. 1-7.
[66] T. Feng, J. Yang, Z. Yan, E.M. Tapia, W. Shi, Tips: Context-aware implicit user identification using touch screen in uncontrolled environments, in: Proc. ACM 15th Workshop Mobile Comput. Syst. Appl. (HotMobile’14), 2014, pp. 1–6.
[67] C.J. Tasia, T.Y. Chang, P.C. Cheng, J.H. Lin, Two novel biometric features in keystroke dynamics authentication systems for touch screen devices, Secur. Comput. Netw. 7 (4) (2014) 685–811, i-iv.
[68] J. Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, Combining biometric evidence for person authentication, in: Josef Bigun, Enrico Grosso (Eds.), Proceedings of the 1st international conference on Advanced Studies in Biometrics (ASB’03), Massimo Tistarelli, Berlin, Heidelberg, Springer-Verlag, 2003, pp. 1–18, https://doi.org/10.1007/11493648_1.

[69] C. Morris, S. Jassim, H. Sellahewa, L. Allano, J. Ehlers, D. Wu, J. Koreman, S. Garcia-Salicetti, L. Van, B. Dorizzi, Multimodal person authentication on a smartphone under realistic conditions, in: Proceedings Volume 6250, Mobile Multimedia/Image Processing for Military and Security Applications; 62500D (2006) Event: Defense and Security Symposium, Orlando (Kissimmee), Florida, United States, 2006.

[70] S. Kim, K.S. Hong, Multimodal biometric authentication using teeth image and voice in mobile environment, Published in, J. IEEE Trans. Consumer Electron. Arch. 54 (4) (2008) 1790–1797. November 2008Page.

[71] D.J. Kim, & K. W. Chung, & K. S. Hong, (2010). Person authentication using face, teeth and voice modalities for mobile device security. Consumer Electronics, IEEE Transactions on. 56. 2678-2685. 10.1109/TCE.2010.5681156.

[72] A. De Luca, A. Hang, F. Brudy, C. Lindner, H. Hussmann, Touch me once and I know it's you!: implicit authentication based on touch screen patterns, SIGCHI Conf. Human Factors Comput. Syst. (2012) 987–996. ACM. ISBN: 978-1-4503- 1015-4.

[73] N. Sae-Bae, K. Ahmed, K. Isbister, N. Memon, Biometric-rich gestures: a novel approach to authentication on multi-touch devices, in: SIGCHI Conf. Human Factors Comput. Syst., 2012, pp. 977–986. ACM. ISBN: 978-1-4503-1015-4.

[74] M. Shahzad, A.X. Liu, A. Samuel, Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it, Published in, in: Proceeding MobiCom '13 Proceedings of the 19th annual international conference on Mobile computing & networking, Miami, Florida, USA. ACM, 2013, pp. 39–50. ISBN: 978-1-4503-1999-7.

[75] J. Ohana, L. Phillips, L. Chen, Preventing Cell Phone Intrusion and Theft using Biometrics, IEEE Security and Privacy Workshops, San Francisco, CA, 2013, pp. 173–180, 2013.

[76] J. Sun, R. Zhang, J. Zhang, Y. Zhang, TouchIn: sightless two-factor authentication on multi-touch mobile devices, in: IEEE Conference on Communications and Network Security, 2014, https://doi.org/10.1109/CNS.2014.6997513. CNS 2014.

[77] E. Shi, Y. Niu, M. Jakobsson, R. Chow, Implicit authentication through learning user behavior ISBN:9783642181771, Springer-Verlag, in: Proceedings of the 13th International Conference on Information Security, 2010.

[78] M.N. Eshwarappa, M.V. Latte, Multimodal biometric person authentication using speech, signature and handwriting features, Article Published in International Journal of Advanced Computer Science and Applications (IJACSA), Special Issue on Artificial Intelligence (2011).

[79] R. Neha, P. Monica, A review of advancement in Multimodal Biometrics System, Int. J. Scientif. Eng. Res. 7 (12) (2016) 241. ISSN 2229-5518.

[80] K. Delac, M. Grgic, A survey of biometric recognition methods, in: 46th International Symposium Electronics in Marine, ELMAR-2004, Zadar, Croatia, 2004.
[81] M. Ghayoumi, A review of multimodal biometric systems: Fusion methods and their applications, in: IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS), Las Vegas, NV, 2015, pp. 131–136.
[82] L. Ballard, D. Lopresti, F. Monrose, Evaluating the security of handwriting biometrics, in: The 10th International Workshop on the Foundations of Handwriting Recognition, 2006, pp. 461–466.
[83] T.C. Meng, P. Gupta, D. Gao, "I can be you: Questioning the use of keystroke dynamics as biometrics, in: Proc. NDSS, 2013, pp. 1–16.
[84] V.M. Patel, R. Chellappa, D. Chandra, B. Barbello, Continuous user authentication on mobile devices: recent progress and remaining challenges, IEEE Signal Process Mag. 33 (4) (2016) 49–61.
[85] D. Crouse, H. Han, D. Chandra, B. Barbello, A.K. Jain, "Continuous authentication of mobile user: fusion of face image and inertial measurement unit data, in: Int. Conf. Biometrics, 2015, pp. 135–142.
[86] R. Murmuria, A. Stavrou, D. Barbara´, D. Fleck, Continuous authentication on mobile devices using power consumption, touch gestures and physical movement of users, in: Proc. Int. Workshop Recent Adv. Intrusion Detection, 2015, pp. 405–424.
[87] H. Crawford, "Keystroke dynamics: Characteristics and opportunities, in: Proc. 8th Int. Conf. Privacy Secur. Trust (PST'10), 2010, pp. 205–212.
[88] I.J. Goodfellow, Y. Bengio, A. Courville, Deep Learning, MIT Press, 2016. Chapter 10, url, http://www.deeplearningbook.org.
[89] R.V. Yampolskiy, V. Govindaraju, "Behavioural biometrics: a survey and classification, Int. J. Biom. 1 (1) (2008) 81–113.
[90] L. Lam, S.Y. Suen, "Application of majority voting to pattern recognition: an analysis of its behavior and performance, IEEE Trans. Syst. Man Cybern. - Part A: Syst. Humans 27 (5) (1997) 553–568, https://doi.org/10.1109/3468.618255.
[91] J. Ashbourn, Biometrics in the New World: The Cloud, Mobile Technology and Pervasive Identity, Springer, New York, NY, USA, 2014.
[92] K. Jain, "Biometric recognition: Overview and recent advances. Progress in Pattern Recognition, Image Analysis and Applications, Springer, New York, NY, USA, 2007, pp. 13–19.
[93] M. Rogowski, K. Saeed, M. Rybnik, M. Tabedzki, M. Adamski, User authentication for mobile devices. Computer Information Systems and Industrial Management, Springer, New York, NY, USA, 2013, pp. 47–58.
[94] A. Abdulaziz, J.K. Kalita, "Authentication of smartphone users using behavioral biometrics, IEEE Commun. Surv. Tutor. 18 (2016) 1998–2026.
[95] M. Muaaz, R. Mayrhofer, "Smartphone-based gait recognition: from

authentication to imitation, IEEE Trans. Mob. Comput. 16 (11) (2017) 3209–3221.
[96] I. Filippov, A.V. Iuzbashev, A.S. Kurnev, User authentication via touch pattern recognition based on isolation forest, in: IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, pp. 1485–1489, https://doi.org/10.1109/EIConRus.2018.8317378.
[97] Biometric authentication: the how and why [online]. Available: https://about-fra ud.com/biometric-authentication, accessed on 21/2/2019.
[98] A. Buriro, B. Crispo, Y. Zhauniarovich, Please hold on: unobtrusive user authentication using smartphone's built-in sensors, in: IEEE International Conference on Identity Security and Behavior Analysis (ISBA-2017), 2017.
[99] S. Bengio, & J. Mari´ethoz, (2004). A statistical significance test for person authentication. The Speaker and Language Recognition Workshop (Odyssey).
[100] L. Yang, Y. Guo, X. Ding, J. Han, Y. Liu, C. Wang, C. Hu, Unlocking smart phone through handwaving biometrics, IEEE Trans. Mobile Comput. 14 (5) (2015) 1044–1055.
[101] S.K.A. Kork, I. Gowthami, X. Savatier, T. Beyrouthy, J.A. Korbane, S. Roshdi, "Biometric database for human gait recognition using wearable sensors and a smartphone, in: 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART), Paris, 2017, pp. 1–4.
[102] D.M. Shila, E. Eyisi, Adversarial gait detection on mobile devices using recurrent neural networks, in: 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 316–321, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00055.
[103] M. Liu, "A study of mobile sensing using smartphones, Int. J. Distrib. Sensor Netw. 2013 (2013) 1–30.
[104] C. Shen, Y. Li, Y. Chen, X. Guan, R.A. Maxion, Performance analysis of multi- motion sensor behavior for active smartphone authentication, IEEE Trans. Inf. Forensics Secur. 13 (1) (2018) 48–62.
[105] D.D. Alves, G. Cruz, C. Vinhal, "Authentication system using behavioral biometrics through keystroke dynamics, in: Proceedings of the IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM '14), 2014, pp. 181–184. IEEE.
[106] Q. Debard, C. Wolf, S. Canu, J. Arne, "Learning to recognize touch gestures: recurrent vs. convolutional features and dynamic sampling, in: 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, 2018, pp. 114–121.
[107] Distances in Classification [online]. Available: http://www.ieee.ma/uaesb/pdf/di stances-in-classification.pdf. [Accessed

10/4/2019].
[108] L.I. Kuncheva, Combining pattern classifiers: methods and algorithms, John Wiley & Sons, 2004.
[109] K. Jain, Y. Chen, M. Demirkus, “Pores and ridges: Fingerprint matching using level 3 features, Proc. Int. Conf. Pattern Recog. 4 (2006) 477–480.
[110] H. Zhang, C. Yan, P. Zhao, M. Wang, Model construction and authentication algorithm of virtual keystroke dynamics for smart phone users, in: IEEE International Conference on Systems, Man, and Cybernetics (SMC), Budapest, 2016, pp. 000171–000175.
[111] C. Darren, F. Inguanez, Multi-Model authentication using keystroke dynamics for Smartphones, in: IEEE 8th International Conference on Consumer Electronics, Berlin (ICCE-Berlin), 2018.
[112] C. Braz, J.-M. Robert, “Security and usability: The case of the user authentication methods, in: Proc. IHM, 2006, pp. 199–203.
[113] V. Matyas Jr, Z. Riha, “Toward reliable user authentication through biometrics, IEEE Secur. Privacy 1 (3) (2003) 45–49.
[114] Introduction to android: sensors overview, android developers [online]. Available: https://goo.gl/MGWQy8, accessed on Feb., 21, 2019.
[115] F. Anjomshoa, M. Catalfamo, D. Hecker, N. Helgeland, A. Rasch, B. Kantarci, M. Erol-Kantarci, S. Schuckers, Mobile behaviometric framework for sociability assessment and identification of smartphone users, in: IEEE Symposium on Computers and Communication (ISCC), 2016.
[116] E.A. Ahmed, I. Traor´e, Continuous authentication using biometrics: data, models, and metrics, Hershey, IGI Global, PA, USA, 2011.
[117] Z. Wu, Z. Chen, An implicit identity authentication system considering changes of gesture based on keystroke behaviors, Int. J. Distrib. Sens. Netw. 2015 (2015) 110–130.
[118] L. Fridman, S. Weber, R. Greenstadt, M. Kam, Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location, IEEE Syst. J. 11 (2) (2017) 513–521.
[119] U. Mahbub, J. Komulaineny, D. Ferreiray, R. Chellappaz, (2018). Continuous authentication of smartphones based on application usage. arXiv:1808.03319v1 [cs.CR].
[120] M. Shoaib, H. Scholten, P.J.M. Havinga, Towards physical activity recognition using smartphone sensors, in: Proceedings of the 2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 2013 IEEE 10th International Conference on Autonomic & Trusted, Vietrisul Mere, Italy, 2013, pp. 80–87.
[121] E. Haq, M.A. Azam, J. Loo, K. Shuang, S. Islam, U. Naeem, Y. Amin, Authentication of smartphone users based on activity recognition and mobile sensing, Sensors 17 (2017) 2043.
[122] G. Li, P. Bours, A mobile app authentication approach by fusing the scores from multi-modal data, in: 21st International Conference on Information

Fusion (FUSION), 2018.
[123] M. Shoaib, S. Bosch, O. Incel, H. Scholten, P.J.M. Havinga, Fusion of Smartphone Motion Sensors for Physical Activity Recognition, Sensors (Basel, Switzerland) 14 (2014) 10146–10176, https://doi.org/10.3390/s140610146.
[124] Z. Yang, L. Shangguan, W. Gu, Z. Zhou, C. Wu and Y. Liu, (2014). Sherlock: micro- environment sensing for smartphones, in ieee transactions on parallel and distributed systems, vol. 25, no. 12, pp. 3295-3305. 10.1109/TPDS.2013.229730 9.
[125] A. Buriro, B. Crispo, M. Conti, AnswerAuth: a bimodal behavioral biometric-based user authentication scheme for smartphones, J. Inf. Secur. Appl. 44 (2019) 89–103, https://doi.org/10.1016/j.jisa.2018.11.008. ISSN 2214-2126.
[126] Y. Yang, B. Guo, Z. Wang, M. Li, Z. Yu, X. Zhou, BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics, Ad Hoc Netw. 84 (2019) (2019) 9–18, 1570-8705 Elsevier.
[127] Lykas, Computational Intelligence, University printing press, University of Ioannina, Greece, 1999.
[128] M. Wolff, (2013). Behavioral Biometric Identification on Mobile Devices. HCI.
[129] A. Shye, B. Scholbrock, G. Memik, Into the wild: studying real user activity patterns to guide power optimizations for mobile architectures, in: Proceedings of the 42nd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO 42). Association for Computing Machinery, New York, NY, USA, 2009, pp. 168–178, https://doi.org/10.1145/1669112.1669135.
[130] R. Murmuria, J. Medsger, A. Stavrou, J.M. Voas, Mobile application and device power usage measurements, in: IEEE Sixth International Conference on Software Security and Reliability (SERE), 2012, p. 147{156.
[131] K.A. Rahman, K.S. Balagani, V.V. Phoha, "Snoop-forge-replay attacks on continuous verification with keystrokes, IEEE Trans. Inf. Forensics Secur. 8 (3) (2013) 528–541.
[132] M. Muaaz, R Mayrhofer, Orientation independent cell phone based gait authentication, in: Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia (MoMM ’14), New York, NY, USA, ACM, 2014, pp. 161–164, https://doi.org/10.1145/2684103.2684152.
[133] B.B. Mjaaland, P. Bours, D. Gligoroski, Walk the Walk: Attacking Gait Biometrics by Imitation, Springer, Berlin, Germany, 2011, pp. 361–380.
[134] R. Kumar, V. V. Phoha, and R. Raina, (2016). Authenticating users through their arm movement patterns. arXiv preprintarXiv:1603.02211.
[135] T. Cover, P. Hart, Nearest neighbor pattern classification, IEEE Trans. Inf. Theor. 13 (1) (2006) 21–27.

[136] H. Witten, E. Frank, Data Mining: Practical Machine Learning Tools and Techniques, 2nd edition, Morgan Kaufmann, San Francisco, 2005.
[137] Y. Li, M. Xie, J. Bian, "SegAuth: a segment-based approach to behavioral biometric authentication, in: IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, 2016, pp. 1–9, https://doi.org/10.1109/ CNS.2016.7860464.
[138] T.C. Clancy, N. Kiyavash, D.J. Lin, "Secure smartcard-based fingerprint authentication, in: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, 2003, pp. 45–52. ACM.
[139] A. Buriro, Behavioral Biometrics for Smartphone User Authentication, in: PHD dissertation. International Doctoral School in Information Engineering and Communication Technologies (ICT), Italy, University of Trento, 2017.
[140] L. Clarke, S.M. Furnell, Authentication of users on mobile telephones –a survey of attitudes and practices, Comput. Secur. 24 (2005) 519e527. Elsevier.
[141] I.C. Stylios, S. Kokolakis, Privacy enhancing on mobile devices: continuous authentication with biometrics and behavioral modalities, Master thesis, University of the Aegean, 2016.
[142] D. Gafurov, E. Snekkenes, P. Bours, "Spoof Attacks on Gait Authentication System, IEEE Trans. Inf. Forensics Secur. 2 (3) (2007) 491–502.
[143] D. Gafurov, "Security analysis of impostor attempts with respect to gender in gait biometrics, in: First IEEE International Conference on Biometrics: Theory, Applications, and Systems, Crystal City, VA, 2007, pp. 1–6.
[144] A. Serwadda, V.V. Phoha, Z. Wang, R. Kumar, D. Shukla, "Towards robotic robbery on the touch screen, ACM TISSEC 18 (2016) 14, 1-14:25.
[145] R. Kumar, V.V. Phoha, A. Serwadda, "Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns, in: IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, 2016, pp. 1–8.
[146] P. Negi, P. Sharma, V.S. Jain, B. Bahmani, K-means vs. behavioral biometrics: one loop to rule them all, in: Network and Distributed Systems Security (NDSS) Symposium 2018, San Diego, CA, USA, 2018. ISBN 1-1891562-49-5.
[147] C.L. Miltgen, A. Popovi˘c, T. Oliveira, Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context, Decis. Support Syst. 56 (2013) 103–114, https://doi.org/10.1016/j. dss.2013.05.010. ISSN 0167-9236.
[148] A. Serwadda, V.V. Phoha, Z. Wang, "Which verifiers work?: a benchmark evaluation of touch-based authentication algorithms, in: IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, 2013, pp. 1–8.
[149] T. Feng, Z. Liu, K. Kwon, W. Shi, B. Carbunar, Y. Jiang, N. Nguyen, Continuous mobile authentication using touchscreen gestures, in: IEEE International Conference on Technologies for Homeland Security, HST, 2012,

pp. 451–456, https://doi.org/10.1109/THS.2012.6459891.
[150] A. Serwadda, V.V. Phoha, Examining a large keystroke biometrics dataset for statistical-attack openings, ACM Transactions on Information and System Security (2013) 16.
[151] Z. Wang, A. Serwadda, K.S. Balagani, V.V. Phoha, "Transforming animals in a cyber-behavioral biometric menagerie with Frog-Boiling attacks, in: IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, 2012, pp. 289–296.
[152] B. Dorizzi, (2005). Biometrics at the frontiers, assessing the impact on society technical impact of biometrics, background paper for the institute of prospective technological studies, DG JRC - Sevilla, European Commission.
[153] N. Yager, T. Dunstone, The biometric menagerie, IEEE Trans. Pattern Anal. Mach. Intell. 32 (2) (2010) 220–230.
[154] M.A. Ferrag, L. Maglaras, A. Derhab, et al., Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues, Telecommun. Syst. 73 (2020) 317–348, https://doi.org/10.1007/s11235-019- 00612-5, 2020.
[155] Z. Rui, Z. Yan, A survey on biometric authentication: toward secure and privacy- preserving identification, IEEE Access 7 (2019) 5994–6009, 2019.
[156] Y. Ashibani, Q.H. Mahmoud, A behavior profiling model for user authentication in iot networks based on app usage patterns, in: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, 2018, pp. 2841–2846.
[157] W. H. Lee, R. Lee, (2017). Implicit smartphone user authentication with sensors and contextual machine learning. 297-308. 10.1109/DSN.2017.24.
[158] Acien, MultiLock: mobile active authentication based on multiple biometric and behavioral patterns, in: 1st International Workshop on Multimodal Understanding and Learning for Embodied Applications, 2019.
[159] D. Baek, P. Musale, You walk, we authenticate: lightweight seamless authentication based on gait in wearable IoT systems, IEEE Access 7 (2019) 37883–37895, https://doi.org/10.1109/ACCESS.2019.2906663.
[160] G. Cola, M. Avvenuti, F. Musso, A. Vecchio, Gait-based authentication using a wrist-worn device, in: Proc. 13th Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services (MOBIQUITOUS), New York, NY, USA, 2016, pp. 208–217.
[161] H. Johnston, G.M. Weiss, Smartwatch-based biometric gait recognition, in: Proc. IEEE 7th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS), 2015, pp. 1–6.
[162] S. Alotaibi, A. Alruban, S. Furnell, N. Clarke, A novel behaviour profiling approach to continuous authentication for mobile applications, in: Proceedings of the 5th International Conference on Information Systems Security and Privacy, 2019, pp. 246–251, https://doi.org/10.5220/0007313302460251. Volume 1: ICISSP, ISBN 978-989-758-359-9.

[163] C.V. Nguyen, Y. Li, T.D. Bui, R.E. Turner, Variational Continual Learning, ICLR, 2018.
[164] L. Reyes-Ortiz, L. Oneto, A. SamA˜, X. Parra, D. Anguita, Transition-aware human activity recognition using smartphones, Neurocomputing (2015).
[165] F.E. Casado, G. Rodríguez, R. Iglesias, C.V. Regueiro, S. Barro, A. Canedo-Rodríguez, Walking recognition in mobile devices, 20, Sensors, 2020, p. 1189, 2020.
[166] U. Mahbub, S. Sarkar, V.M. Patel, R. Chellappa, Active user authentication for smartphones: a challenge data set and benchmark results, in: 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, 2016, pp. 1–8, https://doi.org/10.1109/BTAS.2016.7791155.
[167] H. Shin, J.K. Lee, J. Kim, J. Kim, Continual learning with deep generative replay, in: 31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA, 2017.
[168] S. Farquhar, Y. Gal, A unifying bayesian view of continual learning, in: Neural Information Processing Systems (NeurIPS) Bayesian Deep Learning Workshop, 2018.
[169] Y. Ashibani, M.H. Qusay, A machine learning-based user authentication model using mobile app data, in: International Conference on Intelligent and Fuzzy Systems, Cham, Springer, 2019.
[170] S. Eberz, K.B. Rasmussen, V. Lenders, I. Martinovic, Evaluating behavioral biometrics for continuous authentication: challenges and metrics, in: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS ’17). Association for Computing Machinery, New York, NY, USA, 2017, pp. 386–399, https://doi.org/10.1145/3052973.3053032.
[171] Zhao, Z. Xi, L. Itti. (2016). metricDTW: local distance metric learning in Dynamic Time Warping.
[172] S. Hochreiter, J. Schmidhuber, Long short-term memory, Neural Comput. 9 (8) (1997) 1735–1780.
[173] J. Liu, A. Shahroudy, D. Xu, and G. Wang. Spatio-temporal LSTM with trust gates for 3D human action recognition. 2016.
[174] BlueProximity: sourceforge project, [online]. Available: http://sourceforge.net/ projects/blueproximity, accessed on June, 6, 2020.
[175] Mercedes-Benz: Mercedes-Benz TechCenter: KEYLESS GO (2016), [Online]. Available: http://techcenter.mercedes-benz.com/_en/keylessgo/detail.html, accessed on June, 6, 2020.
[176] A. Czeskis, M. Dietz, T. Kohno, D. Wallach, D. Balfanz, Strengthening user authentication through opportunistic cryptographic identity assertions, in: Proc. 2012 ACM conference on computer and communications security, 2012, p. 404 {414, 2012.
[177] N.A. Tognazzini, (2013). The apple iwatch. Blog posting in AskTOG:

interaction design solutions for the real world [online]. Available: http://asktog.com/atc/ apple-iwatch/, accessed on June, 6, 2020.
[178] H.C. Volaka, G. Alptekin, O.E. Basar, M. Isbilen, O.D. Incel, Towards continuous authentication on mobile phones using deep learning models, Procedia Comput. Sci. 155 (2019) 177–184, 2019ISSN 1877-0509.
[179] I. Lamiche, G. Bin, Y. Jing, Z. Yu, A. Hadid, A continuous smartphone authentication method based on gait patterns and keystroke dynamics, J. Ambient Intell. Humanized Comput. 10 (11) (2019) 4417–4430, 2019.
[180] X. Pang, L. Yang, M. Liu, J. Ma, Mineauth: mining behavioural habits for continuous authentication on a smartphone, in: Australasian Conference on Information Security and Privacy. Springer, 2019, 2019, pp. 533–551.
[181] M.A. Alqarni, S. Chauhdary, M. Malik, M. Ehatisham-ul-Haq, A.M. Awais, Identifying smartphone users based on how they interact with their phones, Human-centric Comput. Inf. Sci. 10 (2020), https://doi.org/10.1186/s13673-020-0212-7.
[182] M. Abuhamad, T. Abuhmed, D. Mohaisen, D. Nyang, AUToSen: Deep Learning- based Implicit Continuous Authentication Using Smartphone Sensors, IEEE Internet of Things J. (2020), https://doi.org/10.1109/JIOT.2020.2975779, 1-1.
[183] Skalkos A, Stylios I., Karyda M., Kokolakis S. Users' Privacy Attitudes towards the Use of Behavioral Biometrics Continuous Authentication (BBCA) Technologies: A Protection Motivation Theory Approach. Journal of Cybersecurity and Privacy. 2021; 1(4):743-766. https://doi.org/10.3390/jcp1040036
[184] Ayeswarya S, Norman J. A survey on different continuous authentication systems. International Journal of Biometrics (IJBM), Vol. 11, No. 1, 2019
[185] Papamichail MD, Chatzidimitriou KC, Karanikiotis T, Oikonomou N-CI, Symeonidis AL, Saripalle SK. BrainRun: A Behavioral Biometrics Dataset towards Continuous Implicit Authentication. Data. 2019; 4(2):60. https://doi.org/10.3390/data4020060
[186] O'Neil R. Mobile Biometrics Market Analysis. Biometrics Research Group, Inc, 2015.
[187] Stylios I, Kokolakis S, Thanou O, Chatzis S. Behavioral biometrics & continuous user authentication on mobile devices: A survey, Information Fusion, Volume 66, 2021, Pages 76-99, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2020.08.021.
[188] C. L. Miltgen, et al., Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context, Decision Support Systems (2013).
[189] M.Y. Yi, J.D. Jackson, J.S. Park, J.C. Probst, Understanding information technology acceptance by individual professionals: toward an integrative view, Information Management 43 (3) (2006) 350–363.
[190] C. López-Nicolás, F.J. Molina-Castillo, H. Bouwman, An assessment of advanced

mobile services acceptance: contributions from TAM and diffusion theory models, Information Management 45 (6) (2008) 359–364.
[191] V. Venkatesh, M.G. Morris, G.B. Davis, F.D. Davis, User acceptance of information technology: toward a unified view, MIS Quarterly (2003) 425–478.
[192] A. Bhattacherjee, J. Perlos, C. Sanford, Information technology continuance: a theoretical extension and empirical test, The Journal of Computer Information Systems 49 (1) (2008) 17–26.
[193] B.A. Beemer, D.G. Gregg, Dynamic interaction in knowledge-based systems: an exploratory investigation and empirical evaluation, Decision Support Systems 49 (4) (2010) 386–395.
[194] T.C.E. Cheng, D.Y.C. Lam, A.C.L. Yeung, Adoption of internet banking: an empirical study in Hong Kong, Decision Support Systems 42 (3) (2006) 1558–1572.
[195] I.L. Wu, J.Y. Li, C.Y. Fu, The adoption of mobile healthcare by hospital's professionals: an integrative perspective, Decision Support Systems 51 (3) (2011) 587–596.
[196] F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Quarterly (1989) 319–340.
[197] H.W. Kim, H.C. Chan, S. Gupta, Value-based adoption of mobile internet: an empirical investigation, Decision Support Systems 43 (1) (2007) 111–126.
[198] M.T. Dishaw, D.M. Strong, Extending the technology acceptance model with task–technology fit constructs, Information Management 36 (1) (1999) 9–21.
[199] D. Gefen, D.W. Straub. The relative importance of perceived ease of use in IS adoption: a study of e-commerce adoption, Journal of the Association for Information Systems 1 (1) (2000) 1–28.
[200] V. Venkatesh, F.D. Davis. A theoretical extension of the technology acceptance model: four longitudinal field studies, Management Science (2000) 186–204
[201] J. Benamati, M.A. Fuller, M.A. Serva, J. Baroudi. Clarifying the integration of trust and TAM in E-commerce environments: implications for systems design and management, IEEE Transactions on Engineering Management 57 (3) (2010) 380–393.
[202] P.A. Pavlou. Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model, International Journal of Electronic Commerce 7 (3) (2003) 101–134
[203] L. Carter, F. Bélanger. The utilization of e-government services: citizen trust, innovation and acceptance factors, Information Systems Journal 15 (1) (2005) 5–25
[204] C. Kim, M. Mirusmonov, I. Lee. An empirical examination of factors influencing the intention to use mobile payment, Computers in Human Behavior 26 (3) (2010) 310–322.
[205] D.J. Kim, D.L. Ferrin, H.R. Rao. A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents, Decision Support Systems 44 (2) (2008) 544–564.
[206] W.W. Chin. Issues and opinion on structural equation modeling, MIS Quarterly 22 (1) (1998) VII–XVI.
[207] I.-L. Wu, J.-L. Chen. An extension of Trust and TAM model with TPB in the initial

adoption of on-line tax: an empirical study, International Journal of Human Computer Studies 62 (6) (2005) 784–808.
[208] R. Agarwal, J. Prasad. A conceptual and operational definition of personal innovativeness in the domain of information technology, Information Systems Research 9 (2) (1998) 204–215
[209] J.-H. Wu, S.-C. Wang. What drives mobile commerce?: an empirical evaluation of the revised technology acceptance model, Information Management 42 (5) (2005) 719–729.
[210] E. Chin, A. Porter Felt, V. Sekar, D. Wagner. Measuring user confidence in smartphone security and privacy. Proceedings of the Eighth Symposium on Usable Privacy and Security. Article No. 1. ISBN: 978-1-4503-1532-6NY, (2012). Publisher ACM New York, USA.
[211] S. Kurkovskyand E. Syta. Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. IEEE International Symposium on Technology and Society (ISTAS), (2010). Conference Location: Wollongong, NSW. Page(s): 441 -449. Print ISBN: 978-1-4244-7777-7.
[212] N. L. Clarke, S. M. Furnell. Advanced user authentication for mobile devices. Computers & Security. 26, 109{119 (2007).
[213] A. A. E. Awad, I. Traore. Continuous Authentication Using Biometrics: Data, Models and Metrics. Publisher: IGI Global. ISBN: 9781613501290. Release Date: September 2011.
[214] G. Ng-Kruelle, P.A. Swatman, J.F. Hampe, D.S. Rebne. Biometrics and e-identity (e-passport) in the European Union: end-user perspectives on the adoption of a controversial innovation, Journal of Theoretical and Applied Electronic Commerce Research 1 (2) (2006) 12–35.
[215] E. M. Rogers. Diffusion of innovations (1st ed.). New York: Free Press of Glencoe. OCLC 254636. (1962).
[216] V. Venkatesh. Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. Information Systems Research, 11 (4), pp. 342–365. (2000).
[217] V. Venkatesh, H. Bala. Technology Acceptance Model 3 and a Research Agenda on Interventions. Decision Sciences, 39 (2): 273–315, doi:10.1111/j.1540-5915.2008.00192.x. (2008).
[218] G. C. Moore, I. Benbasat. Integrating Diffusion of Innovations and Theory of Reasoned Action Models to Predict Utilization of Information Technology by End-Users. In Diffusion and Adoption of Information Technology, K. Kautz and J. Pries-Heje (eds.), Chapman & Hall, London, 1996, pp. 132-146.
[219] S. Ha, L. Stoel. Consumer e-shopping acceptance: antecedents in a technology acceptance model. Journal of Business Research 62 (5) (2009) 565–571.
[220] S. Y. Yousafzai, G. R. Foxall, J. G. Pallister. Explaining internet banking behavior: theory of reasoned action, theory of planned behavior, or technology acceptancemodel? Journal of Applied Social Psychology 40 (5) (2010) 1172–1202.
[221] M. G. Aboelmaged. Predicting e-procurement adoption in a developing country: an

empirical integration of technology acceptance model and theory of plannedbehaviour. Industrial Management & Data Systems 110 (3) (2010) 392–414.
[222] C. D. Chen, Y.-W. Fan, C.-K. Farn. Predicting electronic toll collection service adoption: an integration of the technology acceptance model and the theory of planned behavior. Transportation Research Part C: Emerging Technologies15 (5) (2007) 300–311.
[223] D. Manjunath, A. S. Nagesh, M. P. Sathyajeeth, J. R. Naveen Kumar, S. Akram. A Survey on Knowledge-Based Authentication, International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.2, Issue 4, page no.1194-1201, April-2015.
[224] J. Fogel, E. Nehmad. Internet social network communities: risk taking, trust, and privacy concerns. Computers in Human Behavior 25 (1) (2009) 153–160
[225] L.R. Vijayasarathy, Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model, Information Management 41 (6) (2004) 747–762.
[226] P. M. Bentler, & D. G. Bonett. Significance Tests and Goodness-of-Fit in the Analysis of Covariance Structures, Psychological Bulletin, 88: 588-600, 1980.
[227] N. Koenig-Lewis, A. Palmer, A. Moll. Predicting young consumers' take up of mobile banking services. International Journal of Bank Marketing 28 (5) (2010) 410–432.
[228] P.A. Dabholkar, R.P. Bagozzi. An attitudinal model of technology-based self-service: moderating effects of consumer traits and situational factors. Journal of the Academy of Marketing Science 30 (3) (2002) 184–201.
[229] M. Wolfinbarger, M.C. Gilly, Shopping online for freedom, control, and fun. California Management Review 43 (2) (2001), (34–+).
[230] S. Elliot, S. Fowell. Expectations versus reality: a snapshot of consumer experiences with internet retailing. International Journal of Information Management20 (2000) 323–336.
[231] M.A. Eastlick, S. Lotz. Profiling potential adopters and non-adopters of an interactive electronic shopping medium. International Journal of Retail & Distribution Management 27 (6) (1999) 209–223.
[232] D. Laux, A. Luse, B. Mennecke, A.M. Townsend, Adoption of biometric authentication systems: implications for research and practice in the deployment of end-user security systems, Journal of Organizational Computing and Electronic Commerce 21 (3) (2011) 221–245.
[233] J.F. Hair, C.M. Ringle, M. Sarstedt, D. Smith, R. Reams. Partial least squares structural equation modelling (PLS-SEM): a useful tool for family business researchers. J. Family Bus. Strategy 5 (1), 105–115, 2014.
[234] C. Fornell, D. F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research 18 (1) (1981) 39–50.
[235] J. C. Nunnally, Psychometric Theory, McGraw-Hill, New York, 1978.
[236] M. C. Ringle, S. Wende and M. J. Becker. 2015. "SmartPLS 3." Boenningstedt: SmartPLS GmbH, http://www.smartpls.com
[237] S. Nikou. Factors driving the adoption of smart home technology: An empirical

assessment. Telematics and Informatics 45 (2019) 101283
[238] D. Hooper, J. Coughlan, M. Mullen. Structural equation modelling: guidelines for determining model fit. Electron. J. Bus. Res. Methods 6 (1), 53–60. (2008).
[239] L. T Hu, P. M. Bentler. Fit indices in covariance str ucture modelling: sensitivity to under parameterized model misspecification. Psychol. Methods 3 (4), 424, 1998.
[240] F. Bélanger, L. Carter. Trust and risk in e-government adoption. The Journal of Strategic Information Systems 17 (2) (2008) 165–176.
[241] W. W. Chin, B.L. Marcolin, P.R. Newsted. A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. Information Systems Research 14 (2) (2003) 189–217.
[242] P. Ajibade, (2018). Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches. Library Philosophy and Practice (e-journal).1522-0222.
[243] Jr, Hair, & Ringle, Christian & Sarstedt, Marko. (2011). PLS-sem: Indeed a silver bullet. The Journal of Marketing Theory and Practice. 19. 139-151. 10.2753/MTP1069-6679190202.
[244] V. Venkatesh, F. D. Davis, (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. Management Science 46(2):186-204.
[245] N. Samarin, (2018). A Key to Your Heart: Biometric Authentication Based on ECG Signals. 4th Year Project Report Computer Science, School of Informatics, University of Edinburgh
[246] I. Stylios, S. Kokolakis, A. Skalkos, S. Chatzis, (2021). BioGames: a new paradigm and a behavioral biometrics collection tool for research purposes, Information and Computer Security, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-12-2020-0196
[247] I. Androulidakis, V. Christou, N. G. Bardis, and I. Stilios, (2009). Surveying users' practices regarding mobile phones' security features. In Proceedings of the 3rd international conference on European computing conference (ECC'09). Tbilisi, Georgia, Pages: 25-30.
[248] D. Shaveta, K. Munish, (2020), A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities, Expert Systems with Applications, Volume 143, 2020, 113114, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2019.113114.
[249] Ioannis Stylios, Andreas Skalkos, Spyros Kokolakis, Maria Karyda, (2021). BioPrivacy: Development of a Keystroke Dynamics Continuous Authentication System. 5th International Workshop on SECurity and Privacy Requirements Engineering SECPRE 2021, 6 – 8 October 2021.
[250] Stylios, I., Kokolakis, S., Thanou, O. and Chatzis, S. (2022), "Key factors driving the adoption of behavioral biometrics and continuous authentication technology: an empirical research", Information and Computer Security, Vol. 30 No. 4, pp. 562-582.

https://doi.org/10.1108/ICS-08-2021-0124
[251] Stylios, I., Skalkos, A., Kokolakis, S. and Karyda, M. (2022), "BioPrivacy: a behavioral biometrics continuous authentication system based on keystroke dynamics and touch gestures", Information and Computer Security, Vol. 30 No. 5, pp. 687-704. https://doi.org/10.1108/ICS-12-2021-0212
[252] Agadakos, Ioannis & Hallgren, Per & Damopoulos, Dimitrios & Sabelfeld, Andrei & Portokalidis, Georgios. (2016). Location-enhanced authentication using the IoT: because you cannot be in two places at once. 251-264. 10.1145/2991079.2991090.
[253] Damopoulos, Dimitrios & Kambourakis, Georgios. (2019). Hands-Free one-Time and continuous authentication using glass wearable devices. Journal of Information Security and Applications. 46. 138-150. 10.1016/j.jisa.2019.02.002.
[254] Krašovec, Andraž & Pellarini, Daniel & Geneiatakis, Dimitrios & Baldini, Gianmarco & Pejović, Veljko. (2020). Not Quite Yourself Today: Behaviour-Based Continuous Authentication in IoT Environments. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies. 4. 1-29. 10.1145/3432206.
[255] Damopoulos, Dimitrios & Kambourakis, Georgios & Gritzalis, S. (2013). From Keyloggers to Touchloggers: Take the Rough with the Smooth. Computers & Security. 32. 10.1016/j.cose.2012.10.002.
[256] Georgios Kambourakis, Dimitrios Damopoulos, Dimitrios Papamartzivanos, and Emmanouil Pavlidakis. 2016. Introducing touchstroke: keystroke-based authentication system for smartphones. Sec. and Commun. Netw. 9, 6 (April 2016), 542–554. https://doi.org/10.1002/sec.1061