ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ -
ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΔΙΟΙΚΗΣΗ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Έρευνα μεθόδων αυθεντικοποίησης των χρηστών κινητών τηλεφώνων

A survey of smartphone users' authentication methods

του

Κωνσταντίνου Κουτσιούκη

Επιβλέπων : Αναπληρωτής Καθηγητής Σπύρος Κοκολάκης

Μέλη εξεταστικής επιτροπής: Αναπληρωτής Καθηγητής Καμπουράκης Γεώργιος
Αναπληρωτής Καθηγητής Καρύδα Μαρία

Σάμος, Μάρτιος 2019

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος

Η διπλωματική αυτή εργασία πραγματοποιήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος σπουδών «Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων» του Τμήματος Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου, κατά το χειμερινό και εαρινό εξάμηνο του Ακαδημαϊκού έτους 2017-2018. Επιβλέπων καθηγητής και καθοδηγητής της εργασίας ήταν ο αναπληρωτής καθηγητής κ. Σπύρος Κοκολάκης. Το θέμα της εργασίας είναι: « A survey of smartphone users' authentication methods».

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κ. Σπύρο Κοκολάκη για τις πάντα εύστοχες και πολύτιμες συμβουλές και παρατηρήσεις του, καθώς και για την βοήθειά του σε όλη την διάρκεια της παρούσας εργασίας.
Ευχαριστώ πολύ τον κ. Ιωάννη Στύλιο, Υποψήφιο Διδάκτωρ του Τμήματος Μηχ/κων ΠΕΣ του Πανεπιστημίου Αιγαίου για τη βοήθειά του και τις πολύτιμες συμβουλές και παρατηρήσεις του.
Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου και την Κωνσταντίνα-Μαρία Κρίκα για την πλήρη στήριξή τους στην ολοκλήρωση της διαδικασίας συγγραφής της παρούσας εργασίας καθώς και σε όλη την πορεία του μεταπτυχιακού προγράμματος.

Πίνακας περιεχομένων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Περίληψη

Η παρούσα διπλωματική εργασία προσπαθεί να κάνει μια εκτενή έρευνα και μια διεξοδική ανάλυση των υφιστάμενων μεθόδων αυθεντικοποίησης στα κινητά τηλέφωνα. Τα κινητά τηλέφωνα αποτελούν στις μέρες μας μία από τις πιο συχνά και ευρέως χρησιμοποιούμενες συσκευές τόσο για πρόσβαση στο διαδίκτυο όσο και για την αποθήκευση και επεξεργασία σημαντικών προσωπικών δεδομένων, πολλές φορές ακόμα και ευαίσθητων δεδομένων, του εκάστοτε χρήστη. Οι χρήστες χρησιμοποιούν το κινητό τους τηλέφωνο για να έχουν πρόσβαση σε ποικίλες εφαρμογές, για παράδειγμα στους τραπεζικούς λογαριασμούς τους, σε social media λογαριασμούς, στα εταιρικά και προσωπικά τους email κλπ.

Συνεπώς, αυτό έχει ως επακόλουθο και κάποιους κινδύνους. Σε περίπτωση που κάποιος τρίτος κακόβουλος χρήστης αποκτήσει πρόσβαση στο κινητό αυτό, λόγου χάρη σε περίπτωση κλοπής ή απώλειας της συσκευής, καταφέρνοντας να παρακάμψει το μηχανισμό αυθεντικοποίησης θα αποκτήσει πλήρη πρόσβαση σε όλα τα δεδομένα που ο πραγματικός χρήστης έχει αποθηκεύσει στη συσκευή. Για το λόγο αυτό πέρα από τις κλασσικές μεθόδους αυθεντικοποίησης έχουν προταθεί και μέθοδοι συνεχούς αυθεντικοποίησης του χρήστη (continuous authentication) καθώς και πολυτροπικοί μέθοδοι αυθεντικοποίησης του (multimodal).

Στη ανάλυση που θα ακολουθήσει γίνεται μια πλήρη αναφορά τόσο των υπαρχόντων μεθόδων αυθεντικοποίησης όσο και των βιομετρικών μεθόδων αυθεντικοποίησης, της συνεχούς αυθεντικοποίησης και της πολυτροπικής αυθεντικοποίησης.

Abstract

In this dissertation, I will try to make an extensive research and analysis of the existent authentication methods concerning mobile phones. Nowadays, smartphones are the most common used devices. Many users prefer surfing on the Internet and accomplishing many tasks using only their mobile phones. Due to the ease of use and convenience, users tend to store their private data, such as personal identifiers and bank account details, on their smartphones.

However, this sensitive data can be vulnerable if the device is stolen or lost. In case of a malicious user gain access in a mobile device and if they manage to crack the authentication mechanism, they could have full access to the data stored on the smartphone. For the aforementioned reason, beyond the classic authentication methods, the continuous authentication (CA) and the multimodal authentication methods have been proposed.

In the following paper, I will describe both the existent authentication methods, as well as the authentication ones based on biometrics, the CA and multimodal authentication methods. This work has been validated with analyzing various surveys, which demonstrate the effectiveness of each proposed method.

1

Έξυπνα τηλέφωνα και ασφάλεια πληροφοριών

Οι συσκευές νέας τεχνολογίας και συγκεκριμένα τα smartphones και τα tablets είναι οι πιο ευρέως χρησιμοποιούμενες συσκευές στην καθημερινή ζωή. Σύμφωνα με έρευνα, 400,000 Apple και 1,3εκ. Android συσκευές ενεργοποιούνται σε αντίθεση με τις μόλις 300,000 γεννήσεις μωρών κάθε μέρα [1], [2]. Ο τρόπος χρήσης αυτών των συσκευών απέχει πολύ από τον τρόπο που χρησιμοποιούμε τα laptops και τους ηλεκτρονικούς υπολογιστές. Οι λόγοι που έκαναν τα smartphones τόσο δημοφιλή είναι οι επεξεργαστές τους, η γρήγορη πρόσβαση στο διαδίκτυο και το εξελιγμένο λογισμικό τους.

Η συνεχόμενη χρήση των smartphones σε ποικίλες εφαρμογές ενέχει σοβαρούς κινδύνους για την ασφάλεια και την ιδιωτικότητα του χρήστη. Για να αποκτήσουμε καλύτερη εικόνα για τις απειλές κατά των δεδομένων του χρήστη, μία αμερικάνικη εταιρία, η Symantec, διεξήγαγε ένα κοινωνικό πείραμα σε πέντε μεγάλες πόλεις. Πενήντα smartphones αφέθηκαν σε δημόσιο χώρο χωρίς φύλαξη. Τα αποτελέσματα της έρευνας έδειξαν πώς το 96% όσων τα βρήκαν απέκτησαν πρόσβαση σε αυτά, το 86% είχε πρόσβαση στις προσωπικές πληροφορίες, το 83% σε εταιρικές πληροφορίες, το 60% σε μέσα κοινωνικής δικτύωσης και προσωπικά email, 50% εγκαθίδρυσε απομακρυσμένη διαχείριση και το 43% είχε πρόσβαση στο internet banking [3].

Κάθε ένα smartphone που είναι διαθέσιμο στην αγορά σήμερα συλλέγει διαρκώς την ακριβή τοποθεσία του χρήστη και παρέχει συνεχή πρόσβαση σε διάφορες εφαρμογές όπως για παράδειγμα το mobile banking, το Facebook, το Whatsapp, το Instagram, το Viber, το Twitter κλπ. Όλες οι προαναφερόμενες εφαρμογές αποθηκεύουν ευαίσθητα προσωπικά δεδομένα τα οποία είναι εύκολα προσβάσιμα από οποιονδήποτε αποκτήσει πρόσβαση στο κινητό. Επομένως, κάθε μη εξουσιοδοτημένη πρόσβαση σε αυτές τις συσκευές θα μπορούσε να έχει σοβαρές επιπτώσεις στον χρήστη [4].

1.1 *Αντικείμενο της διπλωματικής εργασίας*

Ο σκοπός κάθε μηχανισμού αυθεντικοποίησης είναι να αποτρέψει κάθε μη εξουσιοδοτημένη πρόσβαση στις συσκευές. Τα πιο ευρέως διαδεδομένα σχήματα αυθεντικοποίησης για κινητά τηλέφωνα στηρίζονται σε «κάτι που ο χρήστης ξέρει» ("something the user knows") π.χ. PIN/ password, σε «κάτι που ο χρήστης κατέχει» ("something the user possesses") π.χ. κάποιο είδος token, σε «κάτι που ο χρήστης είναι» ("something the user is") π.χ. δακτυλικό αποτύπωμα, αναγνώριση προσώπου και σε «κάτι που ο χρήστης κάνει» ("something the user does") όπως το βάδισμα, η ομιλία κλπ.

Οι λύσεις αυθεντικοποίησης που βασίζονται στο τι ξέρει ο χρήστης π.χ. PIN, password δεν θεωρούνται πλέον αρκετά ασφαλείς και τα σχετιζόμενα ζητήματα ασφαλείας αποτελούν πολυγραφότατο θέμα στην σύγχρονη βιβλιογραφία [5]. Αυτές οι μέθοδοι δεν είναι ούτε ασφαλείς καθώς είναι ευάλωτες σε πολλών ειδών επιθέσεις όπως το guessing, το shoulder surfing και το smudge αλλά ούτε και εύχρηστες διότι δεν είναι εύκολο να τις θυμάται ο χρήστης [6]. Επιπλέον, η χρήση token δημιουργεί περαιτέρω προβλήματα χρήσης καθώς είναι εύκολο να χαθούν ή να αντιγραφούν. Επιπροσθέτως, η πολυπαραγοντική αυθεντικοποίηση (π.χ. PIN και token) θέτει ζητήματα χρηστικότητας: για ποιο λόγο ένας χρήστης να κουβαλάει μία επιπλέον συσκευή απλά και μόνο για την αυθεντικοποίηση του; Αποτέλεσμα των ανωτέρω, σύμφωνα με σχετική έρευνα [7] το 70% των χρηστών δεν χρησιμοποιούν καμία μέθοδο αυθεντικοποίησης και θεωρούν την χρήση κωδικού πιο ενοχλητική από οποιοδήποτε άλλο τεχνολογικό πρόβλημα στα κινητά τηλέφωνα, όπως η έλλειψη σήματος, η μικρή οθόνη ή η χαμηλή ποιότητα ήχου [8].

Αντικείμενο της συγκεκριμένης διπλωματικής είναι να γίνει μια ανάλυση των υπαρχόντων μεθόδων αυθεντικοποίησης με έμφαση στα συμπεριφορικά βιομετρικά χαρακτηριστικά, την συνεχή αυθεντικοποίηση και την Multimodal αυθεντικοποίηση ενώ γίνεται και μία σύντομη αναφορά στις συχνότερες επιθέσεις εναντίον κινητών τηλεφώνων.

1.2 *Σκοπός και στόχοι*

Τα τελευταίας τεχνολογίας κινητά τηλέφωνα αποτελούν μέρος της καθημερινότητας μας όσο και οι προσωπικοί υπολογιστές. Οι χρήστες χρησιμοποιούν τις συσκευές τους για ποικιλία εργασιών και διαχειρίζονται ευαίσθητες πληροφορίες όπως η αποθήκευση προσωπικών και εταιρικών δεδομένων και η πρόσβαση σε εταιρικά email και δίκτυα. Όσο αυξάνονται οι λειτουργίες και η αποθήκευση ευαίσθητων πληροφοριών στη συσκευή αυξάνεται και η ανάγκη για αποτελεσματική προστασία. Προκειμένου να εξασφαλίσουμε την ορθή πρόσβαση του χρήστη στα ευαίσθητα και «πολύτιμα» δεδομένα του, απαιτείται ένα βελτιωμένο σύστημα αυθεντικοποίησης.

Είναι λοιπόν προφανές ότι τα κινητά τηλέφωνα απαιτούν πιο ισχυρή αυθεντικοποίηση. Αυτή η αναπτυγμένη τεχνική αυθεντικοποίησης πρέπει να αυξήσει το επίπεδο ασφάλειας πέρα από την point-of-entry αυθεντικοποίηση με το να παρέχει μη παρεμβατικές, εύχρηστες στο χρήστη και διαρκείς μεθόδους αυθεντικοποίησης καθ' όλη την διάρκεια της περιόδου χρήσεως. Επιπλέον η πλειοψηφία των εταιρειών (69%) κινητών τηλεφώνων θεωρεί ότι η ενσωματωμένη (integrated)

ασφάλεια είναι ο πιο αποτελεσματικός τρόπος για να προστατεύσουμε τις συσκευές [9]. Αυτό σημαίνει ότι η προστασία πρέπει να αποτελεί μέρος της συσκευής, η οποία θα είναι ασφαλής χωρίς επιπλέον ενέργειες από τον χρήστη.

Στη συγκεκριμένη εργασία κάνω μια ανασκόπηση της υπάρχουσας τεχνολογίας και ένα literature survey με έμφαση στο Continuous authentication, τα multimodal και τα συμπεριφορικά βιομετρικά χαρακτηριστικά.

1.3 *Συνεισφορά της διπλωματικής*

Για να ξεπεραστεί το πρόβλημα των μεθόδων αυθεντικοποίησης που βασίζονται στη χρήση κωδικού, οι μελέτες επικεντρώθηκαν στη χρήση βιομετρικών χαρακτηριστικών, συνεχούς αυθεντικοποίησης και πολυτροπικών μεθόδων (Biometric-based solutions, Continuous Authentication (CA) και Multimodal). Αυτή η προσέγγιση είναι αποδεκτή τόσο από τη βιομηχανία όσο και από την ακαδημαϊκή κοινότητα. Για παράδειγμα σχετικά πρόσφατες εξελίξεις στον τρόπο αυθεντικοποίησης κινητών περιλαμβάνουν το ξεκλείδωμα συσκευής με αναγνώριση προσώπου, με αναγνώριση φωνής και με ξεκλείδωμα με το δακτυλικό αποτύπωμα του χρήστη [10], [11], [12]. Επίσης πρόσφατα η Google ανακοίνωσε την αντικατάσταση της χρήσης κωδικού με το Trust API . Το Trust API θα παρακολουθεί συνεχώς και θα «αναγνωρίζει» την εμπιστοσύνη στο χρήστη που βασίζεται στα διαθέσιμα βιομετρικά χαρακτηριστικά όπως είναι η τοποθεσία, τα keystrokes κλπ. Η βασική ιδέα είναι να αυξηθεί η ασφάλεια των δεδομένων και η ιδιωτικότητα του χρήστη με έναν καλύτερο αυτοματοποιημένο, αξιόπιστο και διακριτικό τρόπο.

Τα βιομετρικά χαρακτηριστικά χωρίζονται σε φυσιολογικά, συμπεριφορικά, χημικά και υποσυνειδησιακά (physical, behavioral, chemical and cognitive).

Τα φυσιολογικά χαρακτηριστικά βασίζονται στα μέλη του σώματος π.χ. το πρόσωπο, το δαχτυλικό αποτύπωμα, η παλάμη, η ίριδα κλπ.

Τα συμπεριφορικά χαρακτηριστικά βασίζονται στη συμπεριφορά του χρήστη όπως το keystroke, το βάδισμα και η φωνή κλπ. ενώ τα χημικά χαρακτηριστικά βασίζονται σε ενδείξεις του ανθρώπινου σώματος όπως η οσμή και θερμοκρασία.

Τα υποσυνειδησιακά βασίζονται στη αντίδραση του εγκεφάλου σε διάφορα ερεθίσματα όπως για παράδειγμα η οσμή, ο ήχος κλπ. Η βιομετρική αυθεντικοποίηση έχει πολλαπλά πλεονεκτήματα σε σύγκριση με άλλες παραδοσιακές μεθόδους. Σε γενικές γραμμές, τα βιομετρικά χαρακτηριστικά θεωρούνται περισσότερο ασφαλή διότι είναι δύσκολο να αντιγραφούν, πιο αξιόπιστα διότι δεν είναι δυνατή η μεταβίβαση τους και απαιτούν την συνεχή παρουσία του χρήστη κατά τη στιγμή της αυθεντικοποίησης.

Τα συστήματα που βασίζονται στα φυσιολογικά βιομετρικά χαρακτηριστικά, όπως το πρόσωπο, το αποτύπωμα και η ίριδα, από ότι φαίνεται είναι λιγότερο προτιμητέα για διάφορους λόγους. Πρώτον, απαιτούν συγκριτικά περισσότερη συνεργασία από τον χρήστη καθώς δεν μπορούν να συλλεχθούν χωρίς τη συγκατάθεση του. Πρόσφατες έρευνες δείχνουν ότι οι χρήστες δίνουν μεγαλύτερη βαρύτητα στην ευκολία τους παρά στην ασφάλεια των δεδομένων τους και η εύκολη χρήση παίζει κεντρικό ρόλο στις επιλογές τους [13]. Επίσης τέτοια συστήματα μπορούν εύκολα να

παραπλανηθούν (spoof attacks) και η εφαρμογή μεθόδων αντιπαραπλάνησης μπορεί να αυξήσει κατά πολύ το κόστος της συσκευής [14] .

Είναι γνωστό ότι για την διεκπεραίωση μίας εργασίας κάθε άνθρωπος χρησιμοποιεί διαφορετικούς τρόπους, μεθόδους και γνώσεις. Τα συμπεριφορικά βιομετρικά χαρακτηριστικά στηρίζονται στην αρχή « πως ο χρήστης κάνει κάτι» π.χ. το βάδισμα, το keystroke κλπ. [15]. Τα συμπεριφορικά βιομετρικά χαρακτηριστικά έχουν πολλά πλεονεκτήματα έναντι των φυσιολογικών χαρακτηριστικών. Μπορούν να συλλεχθούν με διαφάνεια ή μερικές φορές ακόμα και χωρίς τη γνώση του χρήστη. Ακόμα πιο σημαντικό, η συλλογή αυτών των δεδομένων δεν απαιτεί κάποιο εξειδικευμένο hardware. Παρόλο που τα συμπεριφορικά χαρακτηριστικά δεν είναι απολύτως μοναδικά σε κάθε χρήση, ωστόσο έχουν δείξει ενθαρρυντικά αποτελέσματα στην αυθεντικοποίηση χρηστών. Δεδομένου ότι τα συμπεριφορικά χαρακτηριστικά εξαρτώνται από τις ενέργειες και τις συνήθειες του χρήστη, αυτό τα κάνει πιο ελκυστικά σε σχέση με τις παραδοσιακές μεθόδους αυθεντικοποίησης.

Η συγκεκριμένη εργασία προσπαθεί να μαζέψει την πλειοψηφία των υπαρχουσών σύγχρονων μελετών πάνω σε αυτά τα θέματα και να παρέχει ένα οδηγό σε άλλους νέους ερευνητές που επιθυμούν να ασχοληθούν περαιτέρω με το συγκεκριμένο επίκαιρο κλάδο.

1.4 *Δομή της διπλωματικής εργασίας*

Στο Κεφάλαιο 2 κάνω μια ανάλυση του γνωστικού και τεχνολογικού υπόβαθρου. Στο Κεφάλαιο 3 κάνω μια βιβλιογραφική ανασκόπηση. Στο Κεφάλαιο 4 αναφέρομαι στις βασικότερες επιθέσεις εναντίον της αυθεντικοποίησης στα κινητά τηλέφωνα. Στο Κεφάλαιο 5 είναι ο επίλογος και γίνεται μια συζήτηση για περαιτέρω έρευνα. Και τέλος στο Κεφάλαιο 6 είναι η βιβλιογραφία.

2

Γνωστικό και τεχνολογικό υπόβαθρο

2.1 *Αισθητήρες των Smartphones*

Εδώ θα κάνω μια πολύ σύντομη αναφορά στους αισθητήρες που έχουν τα σύγχρονα κινητά τηλέφωνα και που βοηθάνε σε όλους τους τρόπους αυθεντικοποίησης. Τα σύγχρονα smartphones έχουν ενσωματωμένους αισθητήρες που μπορούν να μετρήσουν την κίνηση (motion), το περιβάλλον (environmental) και τη θέση (positional) [16]. Παρέχουν πολλές διευκολύνσεις στο χρήστη και παρέχουν ακριβή και σαφή πρωτογενή (raw data) δεδομένα, βοηθούν στη παρατήρηση της θέση του κινητού σε τρεις διαστάσεις και μετράνε τις αλλαγές στο περιβάλλον γύρω από τη συσκευή. Πολλές μελέτες σε διαφορετικά πεδία όσον αφορά τα φυσιολογικά και τα συμπεριφορικά βιομετρικά χαρακτηριστικά γίνονται με βάση της μετρήσεις διαφορετικών αισθητήρων και την καταγραφή της συμπεριφοράς του χρήστη όπως τον προσανατολισμό της συσκευής, η πίεση στην οθόνη αφής, τον τρόπο που κρατάει την συσκευή και την ταχύτητα της κίνησης της.

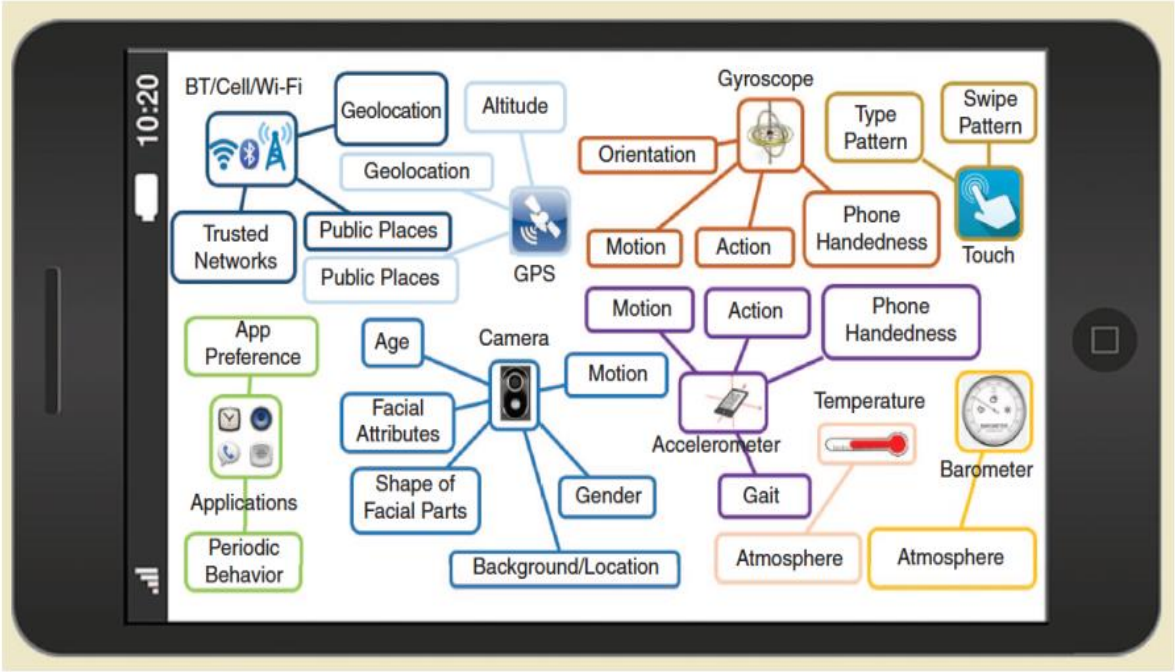
Σε γενικές γραμμές, τα smartphones αυτές τις μέρες έχουν ως λογισμικό κυρίως Apple – IOS, Android και Windows πλατφόρμες και έρχονται με τρείς τύπους αισθητήρων, οι οποίοι είναι οι αισθητήρες θέσης, οι αισθητήρες κίνησης και οι περιβαλλοντικοί αισθητήρες [27], [28], [29].

Οι αισθητήρες θέσης χρησιμοποιούνται για να βρουν τη φυσική θέση της συσκευής. Αυτή η ομάδα αισθητήρων περιλαμβάνει διάφορους αισθητήρες, συμπεριλαμβανομένων των αισθητήρων προσανατολισμού και τα μαγνητόμετρα. Το μαγνητόμετρο χρησιμοποιείται για να μετρήσει την δύναμη και την κατεύθυνση των μαγνητικών πεδίων της γης, η οποία εκφράζονται σε tesla. Μπορεί να χρησιμοποιηθεί ως μια πυξίδα, το οποίο μπορεί να χρησιμοποιηθεί για να βρει ο χρήστης οδηγίες στο χάρτη.

Οι αισθητήρες κίνησης μετρούν την επιτάχυνση και τις δυνάμεις περιστροφής κατά μήκος τριών αξόνων. Παραδείγματα τέτοιου είδους αισθητήρων είναι τα επιταχυνσιόμετρα, οι αισθητήρες βάρους, τα γυροσκόπια και οι αισθητήρες περιστροφής [13]. Ένα επιταχυνσιόμετρο μπορεί να μετρήσει οποιαδήποτε κίνηση του τηλεφώνου συμπεριλαμβανομένων την πτώση του ιδιοκτήτη του κινητού όταν κρατάει το κινητό τηλέφωνο στα χέρια του. Ένα γυροσκόπιο ανιχνεύει τον τρέχοντα προσανατολισμό της συσκευής και την πιθανή περιστροφή ή την αλλαγή περιστροφής. Επιταχυνσιόμετρα και γυροσκόπια επιστρέφουν πάντα τριών διαστάσεων τιμές (3D) [13]. Ο προσανατολισμός του smartphone μπορεί να υπολογιστεί από τη γωνιακή ταχύτητα που ανιχνεύεται από το γυροσκόπιο.

Οι περιβαλλοντικοί αισθητήρες μετρούν παραμέτρους του περιβάλλοντος. Τα εργαλεία σε αυτή την κατηγορία των αισθητήρων περιλαμβάνουν τα βαρόμετρα, τους θερμοστάτες και τα θερμόμετρα [27].

Εκτός από αυτούς τους αισθητήρες, τα smartphones περιλαμβάνουν επίσης άλλους αισθητήρες όπως μικρόφωνα, φωτογραφικές μηχανές, οθόνες αφής, συστήματα εντοπισμού θέσης (GPS) και πυξίδες.



Εικόνα 1: Αισθητήρες, υπηρεσίες και συσκευές στα κινητά τηλέφωνα που μπορούν να χρησιμοποιηθούν για αυθεντικοποίηση σε μορφολογικά ή συμπεριφορικά χαρακτηριστικά [17]

2.2 *Βιομετρικά χαρακτηριστικά*

Η χρήση βιομετρικών δεδομένων είναι μια μέθοδος μέσω της οποίας μπορούμε να ορίσουμε την ταυτότητα ενός ατόμου βάσει των φυσικών ή συμπεριφορικών χαρακτηριστικών του [18].

Βιομετρικά στοιχεία έχουν χρησιμοποιηθεί για σκοπούς αυθεντικοποίησης, δηλαδή για να βεβαιωθεί κάποιος ότι ένα πρόσωπο είναι αυτός που ισχυρίζεται (επίσης γνωστή ως «θετική αναγνώριση»). Στην περίπτωση αυτή, η αυθεντικοποίηση γίνεται συγκρίνοντας ένα βιομετρικό χαρακτηριστικό του ατόμου (π.χ. ένα δακτυλικό αποτύπωμα) με ένα προ-καταγραμμένο βιομετρικό πρότυπο του ίδιου τύπου και από το ίδιο πρόσωπο. Τα κινητά τηλέφωνα μπορούν να συλλάβουν και να αποθηκεύσουν τα βιομετρικά πρότυπα επιτρέποντας στους ιδιοκτήτες τους την αυθεντικοποίηση τους με χρήση βιομετρικών στοιχείων.

Για πολλά χρόνια, η μέθοδος «κάτι που ο χρήστης ξέρει» (π.χ. ένα PIN ή έναν κωδικό πρόσβασης) υπήρξε η πιο δημοφιλής μέθοδος για αυθεντικοποίηση. «Κάτι που ο χρήστης έχει» (π.χ. ένα token) χρησιμοποιούνταν συνήθως συμπληρωματικά, για 2-factor authentication σε κρίσιμες εφαρμογές

(π.χ. e-banking). Ωστόσο, οι δύο παραπάνω μέθοδοι έχουν ορισμένα σοβαρά μειονεκτήματα και υπάρχει ανάγκη για την υιοθέτηση μιας τρίτης κατηγορία αυθεντικοποίησης: «τι ο χρήστης είναι» Η χρήση βιομετρικών στοιχείων για την αυθεντικοποίηση σε συσκευή έχει πολλά πλεονεκτήματα. Πιο συγκεκριμένα:

- Η βιομετρική αυθεντικοποίηση βασίζεται σε χαρακτηριστικά που είναι μοναδικά για κάθε άτομο και σπάνια μεταβάλλονται διαχρονικά, παρέχοντας έτσι μια πιο αξιόπιστη μέθοδο αυθεντικοποίησης σε σχέση με τις παραδοσιακές μεθόδους αυθεντικοποίησης.
- Τα βιομετρικά γνωρίσματα είναι πολύ δύσκολο να πλαστογραφηθούν – αντιγραφούν (αν και όχι αδύνατο) και δεν μπορεί να τα μαντέψει κάποιος, όπως είναι η περίπτωση με τα PIN και τους κωδικούς πρόσβασης. Επιπλέον, οι χρήστες δεν μπορεί να μοιράσουν – δώσουν τα βιομετρικά χαρακτηριστικά τους σε άλλους χρήστες όπως μπορούν να κάνουν με τους κωδικούς πρόσβασης ή τις κάρτες, παρέχοντας έτσι αληθή και πλήρη λογοδοσία.
- Ο χρήστης δεν απαιτείται να θυμάται οτιδήποτε (π.χ. PIN ή κωδικούς πρόσβασης που πρέπει να αλλάζει συχνά) ή να μεταφέρει πράγματα μαζί του (π.χ. κάρτες, tokens). Επίσης δεν μπορείς να τα ξεχάσεις ή να τα χάσεις.
- Η χρήση βιομετρικών μεθόδων για αυθεντικοποίηση είναι μια πολύ γρήγορη και εύκολη διαδικασία, παρέχοντας έτσι μια μέθοδο ελέγχου ταυτότητας εύχρηστη και βολική.

Βεβαίως, τα βιομετρικά χαρακτηριστικά παρουσιάζουν και ορισμένες αδυναμίες, αλλά στη βιβλιογραφία έχουν προταθεί κάποια αντίμετρα. Οι αδυναμίες τους συνοψίζονται παρακάτω [19] :

- Ένας κωδικός πρόσβασης είναι ασφαλής όσο είναι κρυφός: θα μπορούσαν τα βιομετρικά στοιχεία να είναι κρυφά; (Μεγάλης σπουδαιότητας είναι η φυσική παρουσία και η ακεραιότητα του βιομετρικού χαρακτηριστικού).
- Η δημοσίευση γεωμετρικών αλγορίθμων: στην κρυπτογραφία οι αλγόριθμοι είναι γνωστοί και η ασφάλεια προέρχεται από την μυστικότητα του κλειδιού. Στην βιομετρία η γνώση των αλγορίθμων μειώνει την ασφάλεια. (π.χ. Hill climbing επίθεση).
- Η ανάκληση των βιομετρικών χαρακτηριστικών: Εάν ένας κωδικός διαρρεύσει, μπορεί να ανακληθεί και μπορεί να δημιουργηθεί ένας νέος και να χρησιμοποιηθεί. Αν ένα βιομετρικό χαρακτηριστικό διαρρεύσει, τι μπορεί να γίνει;
- Εξαπάτηση (spoofing): πώς μπορεί να αντιμετωπιστεί η δημιουργία των spoof βιομετρικών; (π.χ. φωτογραφίες υψηλής ανάλυσης, εκμαγεία προσώπου, συνθετικά δακτυλικά αποτυπώματα κ.λπ.).

2.2.1 Φυσιολογικά (μορφολογικά) βιομετρικά χαρακτηριστικά

Τα φυσιολογικά (ή μορφολογικά) βιομετρικά χαρακτηριστικά αυθεντικοποιούν ένα χρήστη βασιζόμενα σε μέρη του σώματος του χρήστη [20]. Τέτοια παραδείγματα αποτελούν η αναγνώριση δακτυλικού αποτυπώματος (fingerprint recognition), η αναγνώριση μέσω παλάμης - παλαμική (palm print recognition), η αναγνώριση με βάση την γεωμετρία του χεριού (HGR-hand geometry recognition), η αναγνώριση προσώπου (face detection & recognition), η σάρωση αμφιβληστροειδούς (retinal scan), η αναγνώριση ίριδας (iris recognition) κλπ.

2.2.2 Συμπεριφορικά βιομετρικά χαρακτηριστικά

Η ανθρώπινη συμπεριφορά είναι πιθανό να αλλάξει με την πάροδο του χρόνου επειδή οι χρήστες ενεργούν με διαφορετικό τρόπο ανάλογα με την διάθεση, κάποια ενδεχόμενη ασθένεια, το άγχος,

προηγούμενα συμβάντα κλπ. Ως αποτέλεσμα, τα χαρακτηριστικά που ξεχωρίζουν -διακρίνουν ένα χρήστη- τείνουν επίσης να αλλάζουν κάτι που επηρεάζει την απόδοση του συστήματος. Παρόλα αυτά, ο αντίκτυπος μπορεί να ελαχιστοποιηθεί αν το πρότυπο εξετάζεται και ενημερώνεται τακτικά. Σε σύγκριση με τα φυσιολογικά βιομετρικά χαρακτηριστικά, τα συμπεριφορικά βιομετρικά χαρακτηριστικά είναι λιγότερο μοναδικά είναι, όμως, πιο ευέλικτα και φιλικά προς το χρήστη. Αν και τα συμπεριφορικά βιομετρικά χαρακτηριστικά δεν είναι μοναδικά για να παρέχουν μια αξιόπιστη αυθεντικοποίηση, είναι επαρκή για να παρέχουν μια καλή επαλήθευση [21]. Επιπλέον, οι συμπεριφορικές προσεγγίσεις τείνουν να εφαρμόζονται πιο διαφανώς προς τον χρήστη. Επίσης ειδικοί σε θέματα ασφαλείας πιστεύουν ότι τα συμπεριφορικά βιομετρικά θα αλλάξουν εντελώς τον τρόπο με τον οποίο θα αυθεντικοποιούνται οι χρήστες κινητών τηλεφώνων τα επόμενα 5-8 χρόνια [22]. Κάποια παραδείγματα συμπεριφορικών βιομετρικών χαρακτηριστικών αποτελούν τα κάτωθι:

2.2.2.1 Αναγνώριση βάση της υπογραφής (Signature Recognition)

Όπως το όνομα υπονοεί, η αναγνώριση βάση της υπογραφής στηρίζεται στο τρόπο που υπογράφει ο χρήστης. Τα συστήματα αναγνώρισης βάση της υπογραφής μπορούν να εκτελεστούν τόσο σε στατική όσο και σε δυναμική λειτουργία. Ο στατικός έλεγχος υπογραφής περιλαμβάνει τη χρήση της γεωμετρίας της υπογραφής, ενώ ο δυναμικός έλεγχος υπογραφής χρησιμοποιεί επίσης συμπεριφορικά χαρακτηριστικά όπως η δύναμη, η πίεση που ασκείται από το στυλό, η επιτάχυνση κατά την διάρκεια της υπογραφής και το συνολικό μέγεθος της υπογραφής. Οι υπογραφές μπορεί να αλλάξουν με την πάροδο του χρόνου και επίσης επηρεάζονται από τις φυσικές και συναισθηματικές συνθήκες ενός ατόμου [23]. Δεδομένου ότι οι υπογραφές έχουν χρησιμοποιηθεί για δεκαετίες ως μέθοδος επαλήθευσης, η αναγνώριση βάση της υπογραφής θεωρείται ως μη παρεμβατική μέθοδος. Ως αποτέλεσμα, η τεχνολογία θα μπορούσε να είναι ευρέως αποδεκτή από τους χρήστες. Η απόδοση των συστημάτων αναγνώρισης με υπογραφή μπορεί να επηρεαστεί όταν τα συμπεριφορικά χαρακτηριστικά μιας υπογραφής είναι ασυνεπή. Επιπλέον, η τεχνολογία αυτή περιλαμβάνει τη χρήση ενός στυλό και μιας ειδικής οθόνης κάτι το οποίο μπορεί να αποτελέσει εμπόδιο για να το συνηθίσουν οι χρήστες. Παρόλα αυτά, αρκετές επιχειρήσεις έχουν υιοθετήσει την υπογραφή ως μέσο αυθεντικοποίησης όπως για παράδειγμα η Chase Manhattan Bank (η πρώτη τράπεζα που το έκανε), η υπηρεσία Internal Revenue Service, που χρησιμοποιεί την τεχνολογία αυτή για να επαληθεύσει τις δηλώσεις φόρου εισοδήματος που κατατίθενται online κλπ. [24].

2.2.2.2 Τρόπος πληκτρολόγησης (η δυναμική του τρόπου πληκτρολόγησης) (Keystroke Dynamics)

Η δυναμική πληκτρολόγησης είναι ένα συμπεριφορικό βιομετρικό χαρακτηριστικό που βασίζεται στο τρόπο πληκτρολόγησης ενός χρήστη σε ένα πληκτρολόγιο. Αυτό το συμπεριφορικό βιομετρικό χαρακτηριστικό δεν αναμένεται να είναι μοναδικό για κάθε χρήστη, αλλά διαθέτει επαρκείς πληροφορίες που διακρίνουν τους διαφορετικούς χρήστες. Τα χαρακτηριστικά που χρησιμοποιούνται για να ξεχωρίσουν τους χρήστες περιλαμβάνουν την ταχύτητα πληκτρολόγησης, τη διάρκεια του διαστήματος μεταξύ δύο διαδοχικών πατημάτων γραμμάτων, τη διάρκεια του διαστήματος μεταξύ του πατήματος και της απελευθέρωσης ενός πλήκτρου, τη συχνότητα των γραμμάτων που χρησιμοποιούνται και την ακολουθία που χρησιμοποιούνται για να πληκτρολογήσουν ένα κεφαλαίο γράμμα. Η δυναμική πληκτρολόγηση δεν απαιτεί οποιοδήποτε πρόσθετο ή ειδικό υλικό στη συσκευή. Η δυναμική πληκτρολόγηση μπορεί να πραγματοποιηθεί είτε στατική (εξαρτώμενη από το κείμενο) είτε δυναμική (ανεξάρτητη του κειμένου). Στη στατική προσέγγιση, ο τρόπος πληκτρολόγησης του χρήστη εξετάζεται όταν συγκεκριμένα κουμπιά πατιούνται (π.χ. όταν εισάγετε ο κωδικός πρόσβασης). Στη δυναμική προσέγγιση, ένας χρήστης επαληθεύεται βασιζόμενος στο συνολικό τρόπο που πληκτρολογεί (π.χ. ταχύτητα

πληκτρολόγησης). Η δυναμική προσέγγιση έχει ορισμένα μειονεκτήματα, όπως για παράδειγμα αν ο χρήστης έχει καταναλώσει αλκοόλ, κάνει χρήση ναρκωτικών, η κούραση και τα σπασμένα ή φθαρμένα χέρια μπορεί να αλλάξουν την ταχύτητα της πληκτρολόγησης. Η δυναμική πληκτρολόγηση (στατική λειτουργία) έχει χρησιμοποιηθεί ως ένα πρόσθετο επίπεδο προστασίας για τους υπάρχοντες μηχανισμούς ελέγχου αυθεντικοποίησης. Για παράδειγμα, το BioPassword, ένα υπάρχον εμπορικό προϊόν, απαιτεί από τους χρήστες να πληκτρολογούν το user name και τους κωδικούς πρόσβασης με ένα συγκεκριμένο τρόπο για να συνδεθούν στο σύστημα .

2.2.2.3 Αυθεντικοποίηση μέσω της φωνής (Voice Verification)

Η αυθεντικοποίηση μέσω της φωνής είναι επίσης γνωστή ως αναγνώριση του ομιλητή. Η τεχνική χρησιμοποιεί ένα συνδυασμό φυσιολογικών και συμπεριφορικών χαρακτηριστικών που βασίζονται στη φωνή ενός ατόμου για να κάνει διακρίσεις μεταξύ των ομιλητών. Τα χαρακτηριστικά αυτά περιλαμβάνουν το σχήμα της φωνητικής οδού, την κίνηση, τον τρόπο και προφορά του λόγου [25]. Παρόμοια με το keystroke dynamics, η αυθεντικοποίηση μέσω της φωνής μπορεί να πραγματοποιηθεί είτε στατική (εξαρτώμενη από το κείμενο) είτε δυναμική (ανεξάρτητη από το κείμενο). Στη στατική προσέγγιση, ο χρήστη απαιτείται να μιλήσει και να πει μια προκαθορισμένη φράση, η οποία είναι επίσης γνωστή ως η «φράση πρόσβασης» ("pass phrase"). Στη δυναμική προσέγγιση δεν απαιτείται κάποια συγκεκριμένη έκφραση για να αυθεντικοποιηθεί ο χρήστης. Αντίθετα, το σύστημα παρακολουθεί συνεχώς τα χαρακτηριστικά ομιλίας του χρήστη (π.χ. ρυθμό). Σε σύγκριση με μια στατική προσέγγιση, η δυναμική προσέγγιση είναι πιο βολική, επειδή ο χρήστης μπορεί να μιλήσει ελεύθερα στο σύστημα [26].

Τα πλεονεκτήματα αυτής της βιομετρικής τεχνολογίας είναι ότι είναι εύκολη στη χρήση, χωρίς να απαιτείται ειδικό υλικό καθότι οι κινητές συσκευές είναι ήδη εξοπλισμένες με ένα μικρόφωνο και επίσης καμία ειδική εκπαίδευση δεν απαιτείται για το χρήστη. Ωστόσο, παράγοντες όπως ο θόρυβος του περιβάλλοντος, η διάθεση, η τυχόν φαρμακευτική αγωγή και η φυσική αλλαγή των φωνητικών οδών μπορεί να επηρεάσει την απόδοση του συστήματος. Το 2013, η αναγνώριση ομιλητή χρησιμοποιήθηκε από την Barclays Wealth για να αυθεντικοποιεί τους πελάτες της μέσω τηλέφωνου [27].

2.2.2.4 Γλωσσικό προφίλ (Linguistic Profiling)

Το γλωσσικό προφίλ είναι μια συμπεριφορική μέθοδος βιομετρικών χαρακτηριστικών που επιχειρεί να προσδιορίσει και να κάνει διακρίσεις σε χρήστες με βάση την γλωσσολογική μορφολογία [28]. Στην τεχνική του γλωσσικού προφίλ χρησιμοποιείται ένας μεγάλος αριθμός μετρήσεων των γλωσσικών γνωρισμάτων. Στο γλωσσικό προφίλ διάφορα χαρακτηριστικά λαμβάνονται υπόψιν όπως τα λεξικογραφικά μοτίβα, η σύνταξη, το περιεχόμενο, η διασπορά των λέξεων μέσα στην πρόταση κλπ. [29] .Τα πλεονεκτήματα του γλωσσικού προφίλ είναι ότι δεν απαιτεί οποιοδήποτε πρόσθετο ή ειδικό υλικό και μπορεί να εφαρμοστεί σε μη παρεμβατική και συνεχή αυθεντικοποίηση.

2.2.2.5 Αναγνώριση βάδισης (Gait Recognition)

Η αναγνώριση βάδισης επιχειρεί να προσδιορίσει ένα χρήστη βασιζόμενο στον τρόπο που περπατάει. Επί του παρόντος, τρεις προσεγγίσεις έχουν αναπτυχθεί για την αναγνώριση βάδισης: Machine Vision (MV) αναγνώριση βάδισης από μηχάνημα: σε αυτήν την περίπτωση η συμπεριφορά βαδίσματος συλλαμβάνεται σε βίντεο και τεχνικές επεξεργασίας βίντεο που χρησιμοποιούνται για την ανάλυση του.

Floor Sensor (FS) αναγνώριση βάδισης με αισθητήρες στο πάτωμα: μετράνε την δύναμη κατά την διάρκεια βάδισης και χρησιμοποιούν αυτές τις πληροφορίες για την ανάλυση.

Wearable Sensor (WS) αναγνώριση βάδισης με βάση κάτι που φοράει ο χρήστης: σε αυτή την περίπτωση ο χρήστης φοράει μία συσκευή που μετρά το τρόπο περπατήματος και αναγνωρίζει την αναγνώριση μοτίβων [30]. Αναγνώριση βάδισης είναι μια μη παρεμβατική προσέγγιση καθότι ο τρόπος βάδισης θα μπορούσε να συλληφθεί από απόσταση χωρίς τη γνώση του χρήστη και χωρίς να απαιτείται οποιαδήποτε συνεργασία από το χρήστη σε αντίθεση, για παράδειγμα, με την αναγνώριση δακτυλικού αποτυπώματος. Ωστόσο, ο τρόπος βάδισης ενός χρήση θα μπορούσε να αλλάξει με την πάροδο του χρόνου, την αυξομείωση του βάρους ή από κάποιο τραυματισμό. Επιπλέον, παράγοντες όπως τα υποδήματα, οι συνθήκες του εδάφους και η προσωπική συγκίνηση μπορεί επίσης να επηρεάσουν τον τρόπο που ένα πρόσωπο περπατά. Ως αποτέλεσμα, οι επιδόσεις της βάδισης ως μέσο αυθεντικοποίησης μπορεί να ποικίλουν. Εφαρμογές αναγνώρισης βηματισμού δυνητικά θα μπορούσε να χρησιμοποιηθούν σε ένα κινητό τηλέφωνο, όπως ένα iPhone, για να επαληθεύσουν το χρήστη [31].

2.2.2.6 Σκιαγράφηση συμπεριφοράς (Behavioural Profiling)

Η σκιαγράφηση συμπεριφοράς βασίζεται στον τρόπο που ένα άτομο αλληλοεπιδρά με εφαρμογές ή / και υπηρεσίες [32]. Για παράδειγμα, σε περιβάλλον PC, η σκιαγράφηση συμπεριφοράς θα περιλάμβανε την παρακολούθηση της χρήσης των εφαρμογών, όπως ποια εφαρμογή χρησιμοποιεί κάποιος χρήστης, πότε και για πόσο καιρό σε συνδυασμό και με άλλους παράγοντες. Σε κινητά τηλέφωνα, αυτό θα περιλαμβάνει την παρακολούθηση του χρήστη για το ποιους καλεί στο τηλέφωνο (π.χ. την ημέρα έναρξης, ώρα έναρξης μιας κλήσης, διάρκεια κλήσης, κληθέντες τηλεφωνικοί αριθμοί και τη θέση), τον τρόπο χρήσης της συσκευής, την χρήση Bluetooth, wifi κλπ. Η τεχνική αυτή δεν αναμένεται να δίνει μοναδικά χαρακτηριστικά, ωστόσο, είναι μια μη παρεμβατική προσέγγιση και μπορεί να χρησιμοποιηθεί για να παρακολουθείται συνεχώς η ταυτότητα των χρηστών ενώ χρησιμοποιούν μια κινητή συσκευή. Πολλές εταιρείες χρησιμοποιούν συμπεριφορική ανάλυση χαρακτηριστικών για προστασία από την απάτη πιστωτικών καρτών και τα συστήματα κινητής τηλεφωνίας.

Σε γενικές γραμμές, τα φυσιολογικά βιομετρικά χαρακτηριστικά τείνουν να αποδίδουν καλύτερα την μοναδικότητα, την μονιμότητα και την απόδοση. Ωστόσο, αυτές οι μέθοδοι θεωρούνται να είναι ενοχλητικοί (intrusive), δεδομένου ότι απαιτούν κάποιο επίπεδο της σωματικής επαφής με τους χρήστες. Σε αντίθεση, συμπεριφορικά βιομετρικά χαρακτηριστικά τείνουν να αλλάζουν με την πάροδο του χρόνου, αλλά είναι σε θέση βοηθούν σε μια συνεχής αυθεντικοποίηση. Επιπλέον, συμπεριφορικά βιομετρικά χαρακτηριστικά τείνουν να έχουν καλύτερα επίπεδα αποδοχής, φιλικότητα προς τον χρήστη και είναι λιγότερο παρεμβατικά.

2.2.3 Επεξήγηση όρων μέτρησης της απόδοσης των βιομετρικών συστημάτων

Οι μετρήσεις που χρησιμοποιούνται για την αξιολόγηση των μεθόδων βιομετρικής αυθεντικοποίησης είναι False rejection rate (FRR), False acceptance rate (FAR), True Accept Rate (TAR) και Equal error rate (EER). Οι ορισμοί τους δίνονται παρακάτω [33] :

False rejection rate (FRR): Το FRR είναι ο αριθμός των πραγματικών χρηστών που λανθασμένα το σύστημα απέρριψε προς τον συνολικό αριθμό των προσπαθειών του νόμιμου χρήστη. Ένα χαμηλό FRR υπονοεί ότι ο πραγματικός χρήστης είναι λίγες φορές που δεν μπορεί να αυθεντικοποιηθεί και

επομένως έχει μεγαλύτερο βαθμό χρηστικότητας. Το FRR είναι επίσης γνωστό και ως false alarm rate, false negative rate, false non-match rate. Ο μαθηματικός τύπος υπολογισμού του είναι :

FRR= $\frac{FR}{TA+FR}$ όπου FR είναι το false reject, δηλαδή ο πραγματικός χρήστης εσφαλμένα απορρίπτεται από το σύστημα, TA είναι το true accept, δηλαδή ο πραγματικός χρήστης ορθά αυθεντικοποιείται από το σύστημα.

False acceptance rate (FAR): Το FAR είναι ο αριθμός των ψεύτικών χρηστών που τους δέχτηκε το σύστημα προς τον συνολικό αριθμό των προσπαθειών των ψεύτικων χρηστών. Ένα μικρό FAR δείχνει ένα υψηλό επίπεδο ασφάλειας καθώς οι ψεύτικοι χρήστες συνήθως απορρίπτονται. Το FAR είναι επίσης γνωστό και ως miss alarm rate, false positive rate, false match rate. Ένα 0,001% FAR υπονοεί ότι 1 από 100.000 επιθέσεις Brute force, κατά μέσο όρο, θα είναι επιτυχής [34] .

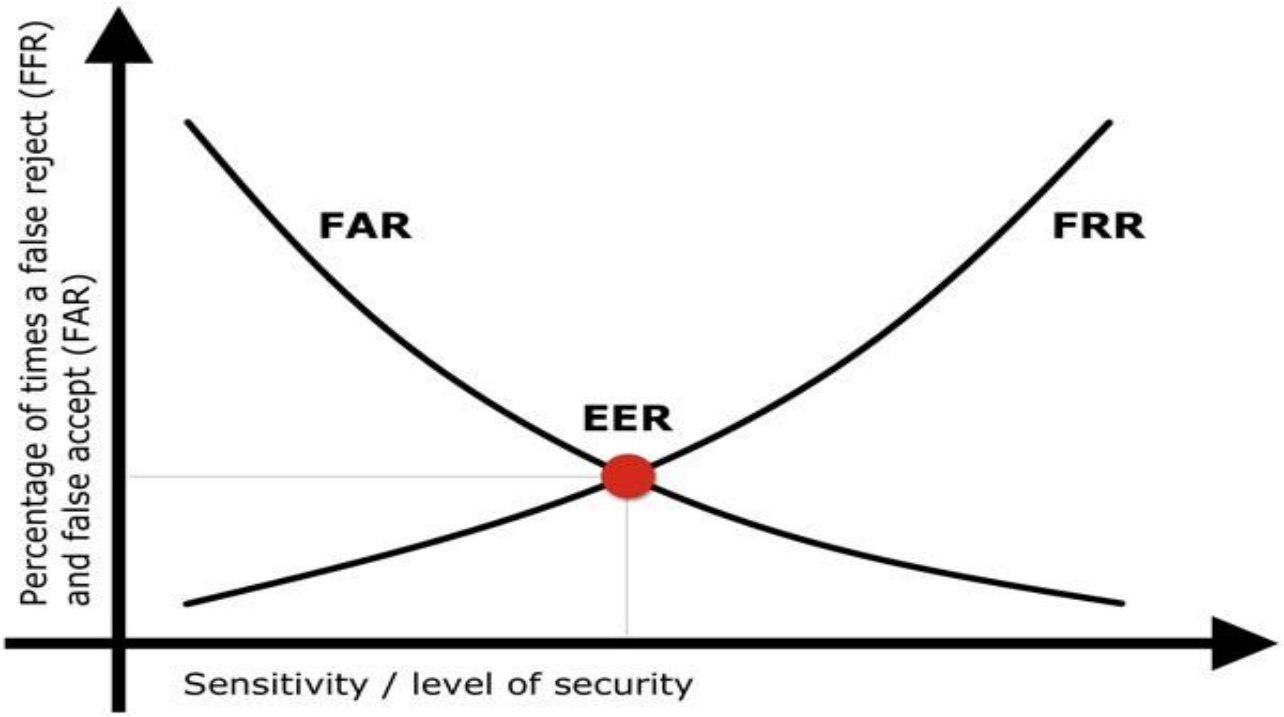
Ο μαθηματικός τύπος υπολογισμού του είναι :

FAR= $\frac{FA}{FA+TR}$ όπου FA είναι το false accept, δηλαδή ο εισβολέας λανθασμένα αυθεντικοποιείται ως ο πραγματικός και TR είναι το true reject, δηλαδή το σύστημα ορθά απορρίπτει τον εισβολέα.

True Accept Rate (TAR): Το TAR περιγράφει την πιθανότητα το σύστημα σωστά να ταιριάξει τον αυθεντικό χρήστη με βάση τα αποθηκευμένα templates. Ο μαθηματικός τύπος υπολογισμού του είναι :

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

Equal error rate (EER): Το EER είναι ο αριθμός που εκφράζει την συνολική ακρίβεια της βιομετρικής μεθόδου αυθεντικοποίησης. Πρέπει να σημειωθεί ότι το FAR και το FRR είναι αρνητικά συσχετισμένα, δηλαδή δεν είναι δυνατόν να μειωθούν την ίδια στιγμή οι τιμές και του FAR και του FRR. Το EER βρίσκεται στη τομή των FRR και FAR. Μία χαμηλή τιμή των FRR και FAR παράγει μια χαμηλή τιμή του EER. Γι' αυτό το λόγο το EER χρησιμοποιείται για να εκφράσει την συνολική ακρίβεια του βιομετρικού συστήματος. Στην Εικόνα 2 φαίνεται γραφικά η ανωτέρω σχέση.



Εικόνα 2: Γραφική αναπαράσταση των FAR, FRR και EER [33]

Σύμφωνα με την Jain et al [35], ένα βιομετρικό σύστημα μπορεί να αξιολογηθεί, αξιολογώντας τις παρακάτω ιδιότητες των μορφολογικών ή συμπεριφορικών χαρακτηριστικών στα οποία βασίζεται.

- Καθολικότητα (Universality), που μετρά το βαθμό στον οποίο το χαρακτηριστικό μπορεί να βρεθεί στην πλειοψηφία των ανθρώπων.
- Μοναδικότητα (Uniqueness), που μετρά το βαθμό στον οποίο το χαρακτηριστικό είναι μοναδικό ανάμεσα σε διαφορετικούς ανθρώπους.
- Μονιμότητα (Permanence), που μετρά την μη αλλαγή του, λόγω ηλικίας, ασθένειας ή / και ατυχημάτων.
- Εισπραξιμότητα (Collectability), που μέτρα πόσο εύκολο και βολικό είναι να συλληφθεί και να μετρηθεί το χαρακτηριστικό.
- Επιδόσεις (Performance), που μετρά παράγοντες, όπως την ταχύτητα και την ακρίβεια της σύλληψη του χαρακτηριστικού.
- Αποδοχή (Acceptability), που μετρά την προθυμία των λαών να δεχθεί ένα βιομετρικό σύστημα που βασίζεται σε αυτό το χαρακτηριστικό.
- Καταστρατήγηση (Circumvention), που μετρά πόσο εύκολο είναι να χρησιμοποιηθούν δόλιες τεχνικές προκειμένου να ξεγελάσουν ένα βιομετρικό σύστημα που βασίζεται σε αυτό το χαρακτηριστικό.

Είναι σημαντικό να τονίσουμε εδώ ότι δεν υπάρχει μία ενιαία απάντηση ως προς το πόσο κατάλληλο είναι ένα χαρακτηριστικό για ένα βιομετρικό σύστημα. Κάθε χαρακτηριστικό έχει διαφορετικά χαρακτηριστικά που πρέπει να εξεταστούν και αφορούν το πλαίσιο και την εφαρμογή του βιομετρικού συστήματος για να κατασκευαστεί. Ένα χαρακτηριστικό που φαίνεται να είναι κακό για ένα συγκεκριμένο βιομετρικό σύστημα θα μπορούσε να είναι άριστος υποψήφιος για

κάποιο άλλο σύστημα. Εν συνεχεία θα αναφερθούν και θα αναλυθούν σύντομα κάποια συγκεκριμένα βιομετρικά χαρακτηριστικά.

2.2.4 Σύνοψη βιομετρικών χαρακτηριστικών

Βάσει των απαιτήσεων του βιομετρικού συστήματος [20] γίνεται μια σύγκριση όλων προαναφερθεισών βιομετρικών προσεγγίσεων όπως παρουσιάζονται στον Πίνακας 1 (H, M και L αντιπροσωπεύουν υψηλή, μέση και χαμηλή αντίστοιχα). Για παράδειγμα, η αναγνώριση ίριδας είναι ένα από τα πιο μοναδικά βιομετρικά χαρακτηριστικά, μένει μόνιμα και είναι εξαιρετικά δύσκολο να αναπαραχθεί, αλλά τα άτομα μπορεί να δυσκολεύονται να αποδεχθούν αυτήν την τεχνολογία λόγω της δυσκολίας στη σύλληψη βιομετρικού προτύπου καλής ποιότητας. Σε σύγκριση, η επαλήθευση μέσω φωνής τείνει να έχει μια πολύ υψηλή αποδοχή, επειδή είναι εύκολο να αποκτηθεί, ωστόσο, η μονιμότητα είναι πολύ μικρότερη καθώς είναι πιθανό να αλλάξει με την πάροδο του χρόνου.

Biometric Features	**Univ**	**Dist**	**Perm**	**Coll**	**Perf**	**Acce**	**Circ**
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	H
Face	H	L	M	H	L	H	H
Facial Thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand Geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palm print	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Πίνακας 1: Σύγκριση των βιομετρικών χαρακτηριστικών

2.3 *Κύριοι μέθοδοι αυθεντικοποίησης σε κινητά τηλέφωνα σήμερα*

2.3.1 Αυθεντικοποίηση

Αυθεντικοποίηση (Authentication) είναι η διαδικασία του προσδιορισμού αν κάποιος ή κάτι είναι αυτός ή αυτό που δηλώνει ότι είναι [36]. Η αυθεντικοποίηση είναι ένας τομέας ο οποίος έχει διευρύνει την απήχηση του τις τελευταίες δεκαετίες και χρησιμοποιείται σε όλο και περισσότερους διαφορετικούς τομείς. Η αυθεντικοποίηση είναι μια καθ' όλα σημαντική παράμετρος της ασφάλειας των πληροφοριών (Information Security) που αποσκοπεί στο να αποτρέψει την μη εξουσιοδοτημένη πρόσβαση και να μειώσει το ρίσκο ενάντια σε κλοπή ή αποκάλυψη ευαίσθητων προσωπικών πληροφοριών. Παραδείγματα αυθεντικοποίησης είναι οι κωδικοί και τα μοτίβα που χρησιμοποιούμε στα κινητά τηλέφωνα, οι κωδικοί ασφαλείας που χρησιμοποιούμε στο Mobile banking κλπ. Ταυτοποιούμε τους φίλους και γνωστούς μας από την φωνή τους, τα πρόσωπα τους, τον τρόπο που περπατάνε κλπ. Οι λέξεις αυθεντικοποίηση (authentication) και ταυτοποίηση (identification) είναι όροι που πολύ συχνά μπερδεύονται αλλά έχουν εξ ορισμού διαφορετική σημασία. Η αυθεντικοποίηση είναι μία 1:1 (ένα προς ένα) ταυτοποίηση της ταυτότητας κάποιου ενώ ταυτοποίηση σημαίνει να βρεις την ταυτότητα ενός προσώπου [34].

Ειδικότερα μπορούμε να πούμε ότι η διαφορά μεταξύ Authentication και identification είναι η εξής:

- Ταυτοποίηση: Απαντά στο ερώτημα: «Ποιος είναι;».
- Αυθεντικοποίηση: Απαντά στο ερώτημα: «Είναι πράγματι αυτός που ισχυρίζεται

ότι είναι;».

Αυθεντικοποίηση

- Παροχή βιομετρικού και ισχυρισμός μιας ταυτότητας.
- Σύγκριση 1:1
- Απάντηση «αποδοχή» ή «άρνηση»

Ταυτοποίηση

- Παροχή μόνο του βιομετρικού
- Σύγκριση 1: N
- Απάντηση «ταυτότητα» ή /και «άγνωστο»

Για να προστατεύσουν τα κινητά τηλέφωνα από μη εξουσιοδοτημένη πρόσβαση, ένας μηχανισμός αυθεντικοποίησης απαιτείται. Η μέθοδος που χρησιμοποιείται κατά κόρον σήμερα στα κινητά τηλέφωνα αποκαλείται επίσης one-shot αυθεντικοποίηση [37], [38]. Αυτό σημαίνει ότι ο χρήστης αποδεικνύει ότι είναι ο πραγματικός και όχι κακόβουλος εισάγοντας στην αρχή της συνόδου τον σωστό κωδικό, δαχτυλικό αποτύπωμα, πρόσωπο κλπ. Η συγκεκριμένη σύνοδος παραμένει ενεργή μέχρι να την τερματίσει ο χρήστης οπότε και πρέπει να ξανά αυθεντικοποιηθεί την επόμενη φορά που θα χρησιμοποιήσει το κινητό τηλέφωνο του. Σήμερα, οι περισσότερες συσκευές κινητών τηλεφώνων χρησιμοποιούν της παρακάτω μεθόδους αυθεντικοποίησης :

2.3.2 Personal Identification Number (PIN) αυθεντικοποίηση

Η PIN αυθεντικοποίηση χρησιμοποιείται για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση τόσο στο κινητό τηλέφωνο όσο και για την SIM κάρτα. Συνήθως τα PIN των κινητών τηλεφώνων αποτελούνται από 4 έως 8 αριθμητικά ψηφία. Ο χρήστης απαιτείται να βάλει το σωστό PIN πριν από την πρώτη πρόσβαση στο κινητό τηλέφωνο κάθε φορά που το κλειδώνει χειροκίνητα είτε μέχρι την επόμενη επανεκκίνηση. Επίσης υπάρχει η δυνατότητα για μεγαλύτερη ασφάλεια, να ζητείται από το χρήστη να πληκτρολογεί το PIN μετά από κάποια συγκεκριμένη χρονική περίοδο π.χ. 5 δευτερόλεπτα μη χρήσης του κινητού τηλεφώνου.

2.3.3 Αυθεντικοποίηση με χρήση password

Είναι παρεμφερής μέθοδος σαν αυτή του PIN απλά απαιτεί όχι μόνο αριθμούς αλλά και γράμματα και ειδικούς χαρακτήρες. Με αυτό τον τρόπο αυξάνονται εκθετικά οι πιθανοί συνδυασμοί κωδικών. Είναι πολύ συχνή μέθοδος αυθεντικοποίησης με σχετικά καλή αντοχή σε επιθέσεις brute-force ειδικά με μεγάλου μήκους κωδικούς [39] .

2.3.4 Αυθεντικοποίηση μέσω αναγνώρισης

Αυτός ο τρόπος αυθεντικοποίησης δεν στηρίζεται σε αριθμητικούς ή αλφαριθμητικούς κωδικούς αλλά στο τρόπο που ένας χρήστης σχεδιάζει ένα συνδυασμό κινήσεων π.χ. ενώνει κουκίδες με την σωστή σειρά προκειμένου να ξεκλειδώσει το κινητό τηλέφωνο. Για παράδειγμα στις Android συσκευές υπάρχει το μοτίβο (pattern) όπου ο χρήστης απαιτείται να δημιουργήσει ένα συγκεκριμένο μοτίβο ενώνοντας 3*3 κουκίδες με το σωστό τρόπο. Το μήκος του μοτίβου είναι από 4 έως 9 κουκίδες. Ωστόσο επειδή υπάρχει ο περιορισμός ότι μία κουκίδα δεν μπορεί να χρησιμοποιηθεί πάνω από μία φορά αυτή η συγκεκριμένη τεχνική δίνει πολύ λιγότερους πιθανούς συνδυασμούς από την χρήση PIN ή κωδικού. Επίσης στη περίπτωση με τις 4 κουκίδες, χωρίς να χρησιμοποιήσει ο χρήστης 2 φορές την ίδια κουκίδα, υπάρχουν μόνο 389.112 πιθανοί συνδυασμοί οι οποίοι εύκολα μπορούν να σπάσουν με brute force [40]. Ο Ye at al [41] κατάφερε να «σπάσει» το 95% από 120 μοναδικά μοτίβα που συλλέχθηκαν από 215 συμμετέχοντες με μόνο 5 προσπάθειες απλά βιντεοσκοπώντας την οθόνη του κινητού των χρηστών από μακριά όταν αυτοί ξεκλείδωναν τον κινητό τους τηλέφωνο.

Αν και αυτές οι τεχνικές είναι διαθέσιμες σε όλες τις κινητές συσκευές, πολλοί χρήστες δεν χρησιμοποιούν καμία μέθοδο αυθεντικοποίησης [42]. Για την έλλειψη χρήσης οποιαδήποτε μεθόδου αυθεντικοποίησης έχει επισημανθεί ότι οι κύριοι λόγοι είναι ότι δεν την θεωρούν αξιόπιστη λύση και ότι δεν είναι βολική στη χρήση [43]. Επίσης πολλοί χρήστες που χρησιμοποιούν κωδικό δεν τον χρησιμοποιούν με σωστό τρόπο. Σύμφωνα με έρευνα [42] η πλειοψηφία όσων συμμετείχαν απάντησαν ότι χρησιμοποιούν τον εργοστασιακό κωδικό της συσκευής. Επίσης ποσοστό περίπου 12% απάντησε ότι χρησιμοποιεί τον ίδιο κωδικό μεταξύ πολλών διαφορετικών λογαριασμών και συσκευών, πάνω από τους μισούς μοιράζονται τον κωδικό τους με κάποιον άλλον και περίπου 15% σώζει τον κωδικό στο κινητό του τηλέφωνο. Όλα αυτά καθιστούν το PIN ως μέθοδο αυθεντικοποίησης ακατάλληλο ως μέσο αυθεντικοποίησης στα κινητά τηλέφωνα [44].

Μία παρατήρηση σχετικά με τα PIN/κωδικούς πρόσβασης είναι ότι αυτές οι προσεγγίσεις βασίζονται σε μηχανισμούς point-of-entry που απαιτούν από το χρήστη να κάνει κάτι ενεργά όπως να εισάγει έναν αριθμό PIN ή τον κωδικό πρόσβασης προκειμένου να κάνει αυθεντικοποίηση πριν

την έναρξη μιας περιόδου λειτουργίας. Αφού αυθεντικοποιηθεί, η κινητή συσκευή είναι σε θέση να παραμείνει ξεκλείδωτη χωρίς περαιτέρω αυθεντικοποίηση του χρήστη παρά μόνο αν απενεργοποιηθεί ή λήξει η συγκεκριμένη σύνοδος (session). Κατά την συγκεκριμένη σύνοδο (session), όλες οι υπηρεσίες, εφαρμογές και πληροφορίες σχετικά με την κινητή συσκευή είναι προσιτές στο συγκεκριμένο χρήστη. Οι χρήστες είναι σε θέση να κάνουν οτιδήποτε, όπως για παράδειγμα να παίζουν ένα παιχνίδι, να στείλουν ένα μήνυμα κειμένου, να κάνουν ένα διεθνές τηλεφώνημα, να έχουν πρόσβαση στο προσωπικό / εταιρικό ηλεκτρονικό ταχυδρομείο και εξ αποστάσεως πρόσβαση σε εταιρικά δίκτυα για να αντιγράψουν τη βάση δεδομένων των πελατών της εταιρείας. Ένας άλλος περιορισμός της point-of-entry μεθόδου είναι ότι απαιτεί από το χρήστη να κάνει μια ενέργεια (actively) προκειμένου να αυθεντικοποιηθεί. Αυτό μπορεί να θεωρηθεί ενοχλητικό καθώς διακόπτει τις δραστηριότητες του χρήστη [45].

Πέρα από την αυθεντικοποίηση με χρήση κωδικού, υπάρχουν δύο άλλες τεχνικές ελέγχου ταυτότητας, η χρήση token και βιομετρικών χαρακτηριστικών. Η χρήση token θεωρείται ανέφικτη υπό την έννοια ότι ο χρήστης θα πρέπει συνεχώς να μεταφέρει μαζί με την κινητή συσκευή το token, αυξάνοντας έτσι τον κίνδυνο, όπως αναφέραμε και προηγουμένως, να το χάσει ή να το ξεχάσει. Ένα άλλο ζήτημα είναι ότι, αν η διαδικασία αυθεντικοποίησης απαιτεί το token να τοποθετηθεί στη συσκευή, τότε οι περισσότεροι χρήστες θα το αφήνουν μόνιμα πάνω στο κινητό, ακυρώνοντας έτσι την χρησιμότητα του.

Αυτό μπορούμε εύκολα να το δείξουμε για παράδειγμα με τη χρήση μιας κάρτας SIM στις κινητές συσκευές. Όταν οι χρήστες δεν θέλουν να χρησιμοποιούν το κινητό, θα μπορούσαν να αφαιρούν την κάρτα SIM όταν η συσκευή δεν είναι σε χρήση. Ωστόσο, η αφαίρεση της κάρτας SIM θα ήταν άβολη. Με την αξιοποίηση ανέπαφων τεχνολογιών (π.χ. Bluetooth ή RFID) είναι δυνατό να αναπτυχθούν tokens που να ενσωματωθούν μέσα σε πράγματα που οι χρήστες έχουν πάντα μαζί τους, όπως δαχτυλίδια ή ρολόγια χειρός. Η τεχνική αυτή είναι εφικτή και μπορεί να αυξήσει την ευκολία του χρήστη πάνω στην προσέγγιση secret-knowledge καθώς καμία αλληλεπίδραση δεν είναι απαραίτητη. Ωστόσο, αυτή η προσέγγιση εξακολουθεί να απαιτεί από το χρήστη να θυμάται να φέρει μαζί του το token.

Η τελευταία προσέγγιση για τον έλεγχο ταυτότητας είναι τα βιομετρικά χαρακτηριστικά. Η τεχνική αυτή αυθεντικοποιεί έναν χρήστη βασιζόμενη στα μοναδικά χαρακτηριστικά του όπως το δακτυλικό αποτύπωμα, το χέρι και το πρόσωπο. Η βιομετρική μέθοδος δεν απαιτεί από τον χρήστη να ενεργεί αλλά απλά να είναι ο εαυτός τους. Οι περισσότερες κινητές συσκευές σήμερα είναι εξοπλισμένες με αναγνώστη δακτυλικών αποτυπωμάτων ή προσώπου, μία τεχνολογία αναγνώρισης που μπορεί να παρέχει πιο ασφαλή μηχανισμό ελέγχου αυθεντικοποίησης. Σήμερα πάρα πολύ μεγάλη γκάμα κινητών συσκευών έχει ενσωματώσει τέτοιου είδους αυθεντικοποίηση. Ωστόσο, αν και οι τεχνολογίες αναγνώρισης δακτυλικών αποτυπωμάτων και προσώπου αύξησαν το επίπεδο ασφάλειας και την ευχρηστία για τον χρήστη, οι τεχνικές αυτές παραμένουν point-of-entry αυθεντικοποίηση και απαιτούν την παρέμβαση – «ενόχληση» του χρήστη.

Όπως περιγράφεται παραπάνω, είναι σαφές ότι η προσέγγιση point-of-entry αυθεντικοποίηση έχει αναπτυχθεί για να παρέχει άδεια πρόσβασης στη συσκευή και δεν παρέχει καμία περαιτέρω προστασία κατά τη διάρκεια της χρήσης. Ωστόσο, στην πραγματικότητα, οι ανάγκες για ασφάλεια θα διαφέρουν ανάλογα με το τι κάνει ο χρήστης και σε τι υπηρεσίες και δεδομένα έχει πρόσβαση καθώς η κάθε εργασία απαιτεί διαφορετικά επίπεδα ασφάλειας. Δεδομένου ότι κάθε υπηρεσία

φέρνει ένα ορισμένο κίνδυνο μη ορθής χρήσης, αυτό πρέπει να είναι ένας παράγοντας για την επιλογή του κατάλληλου επιπέδου ασφάλειας. Εάν το επίπεδο ασφαλείας είναι κατάλληλα κατανεμημένο σε κάθε υπηρεσία, έτσι ώστε κάθε υπηρεσία ή λειτουργία να μπορεί να απαιτούν ένα συγκεκριμένο επίπεδο ελέγχου ταυτότητας προκειμένου να αποκτήσει πρόσβαση στη συγκεκριμένη υπηρεσία. Με αυτόν τον τρόπο, πιο κρίσιμες λειτουργίες θα μπορούσαν να τυγχάνουν μεγαλύτερη προστασία αφήνοντας έτσι τις λιγότερο σημαντικές εφαρμογές σε χαμηλότερο επίπεδο αυθεντικοποίησης. Ως αποτέλεσμα, μια διαρκής αυθεντικοποίηση (CA) που είναι ικανή για την συνεχή παρακολούθηση και τον έλεγχο ταυτότητας ενός χρήστη είναι αδήριτη ανάγκη. Αυτό μπορεί να επιτευχθεί αποτελεσματικά με τη χρήση μη-παρεμβατικών ή με διαφάνεια μεθόδων, έτσι ώστε οι χρήστες δεν θα γνωρίζουν ότι ο έλεγχος ταυτότητας πραγματοποιείται, αποφεύγοντας να διακόψουν την λειτουργία για να εισαγάγουν ξανά έναν κωδικό PIN.

2.4 *Συνεχής Αυθεντικοποίηση*

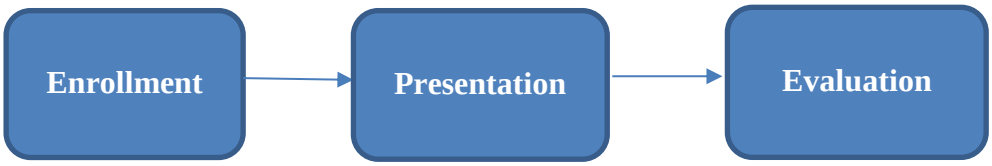
Προκειμένου να αντιμετωπιστούν οι ελλείψεις του σημείο εισόδου κατά τον έλεγχο ταυτότητας, μία από τις προσεγγίσεις που προτείνονται στη βιβλιογραφία καλείται συνεχής αυθεντικοποίηση continuous authentication (CA) [46]. Στο εξής, θα δούμε μια CA προσέγγιση όπως παρουσιάζεται στο βιβλίο: "Continuous Authentication Using Biometrics: Data, Models and Metrics" [47] καθώς επίσης βρήκα πολύτιμη βοήθεια στη εργασία που έχουν κάνει πάνω στο θέμα ο υποψήφιος διδάκτορας κ. Στύλιος Ιωάννης καθώς και ο επιβλέπων καθηγητής της εργασίας κ. Κοκολάκης Σπύρος και ειδικότερα από την διπλωματική εργασία με τίτλο : «Privacy Enhancing on Mobile Devices: Continuous Authentication with Biometrics and Behavioral Modalities» [48]. Τα συστήματα συνεχούς ελέγχου ταυτότητας (CA) αντιπροσωπεύουν μια νέα γενιά μηχανισμών ασφαλείας που παρακολουθούν συνεχώς τη συμπεριφορά του χρήστη και την χρησιμοποιούν για να γίνει επανέλεγχος της ταυτότητας περιοδικά κατά τη διάρκεια μιας περιόδου λειτουργίας σύνδεσης. Η ιδέα της συνεχούς αυθεντικοποίησης προέκυψε στις αρχές του 2000, εν μέρει λόγω ανησυχιών για την ασφάλεια που επέφερε η 11 Σεπτεμβρίου. Το ενδιαφέρον για την τεχνολογία αυτή έχει αυξηθεί από τότε, τόσο στον ακαδημαϊκό χώρο όσο και στη βιομηχανία.

2.4.1 Στατική σε σύγκριση με τη συνεχή αυθεντικοποίηση

Η στατική αυθεντικοποίηση είναι μια διαδικασία που αποτελείται από τρεις επιμέρους υποδιαδικασίες: εγγραφή, παρουσίαση και αξιολόγηση (enrollment, presentation και evaluation) (βλέπε Εικόνα 3). Η static (ή one-shot αυθεντικοποίηση) γίνεται στη αρχή της συνόδου και γίνεται με την χρήση συνήθως κάποιου κωδικού, κάποιου token, smart card ή κάποιου μορφολογικού βιομετρικού όπως το δαχτυλικό αποτύπωμα.

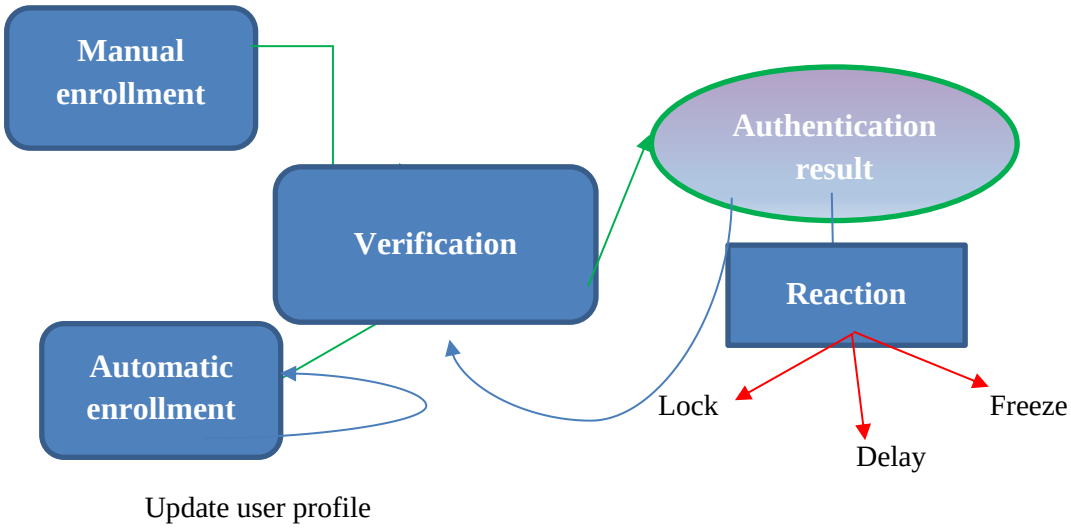
CA είναι ο μηχανισμός που επαναλαμβανόμενα αυθεντικοποιεί την ταυτότητα ενός χρήστη για όλη την διάρκεια της συνόδου όπως φαίνεται στην Εικόνα 4. Ειδικότερα CA είναι η προσέγγιση που συνεχώς αυθεντικοποιεί ένα χρήστη και κλειδώνει το κινητό τηλέφωνο όταν παρατηρηθεί αλλαγή στο χρήστη του κινητού τηλεφώνου [47]. Η CA γίνεται δυναμικά και επαναλαμβάνει τα 3 στάδια της στατικής αυθεντικοποίησης (Εικόνα 3) κατά την διάρκεια της συνόδου. Αυτές οι επαναλήψεις μπορεί να γίνονται στηριζόμενες σε κάποιο γεγονός, ανά κάποιο συγκεκριμένο χρονικό διάστημα (π.χ. κάθε Χ δευτερόλεπτα) ή τυχαία. Με αυτό τον τρόπο ξεπερνιούνται οι δυσκολίες της one-shot αυθεντικοποίησης όπου η αυθεντικοποίηση γίνεται μόνο κατά την διάρκεια της αρχικής εισόδου. Τα συμπεριφορικά βιομετρικά χαρακτηριστικά κατά κύριο λόγο προσελκύουν το ενδιαφέρον των

ερευνητών καθώς μπορούν να συλλεχθούν και να χρησιμοποιηθούν διαφανώς ως προς τον χρήστη. Επίσης ο CA είναι γνωστός και ως active authentication, implicit authentication και transparent authentication.



Εικόνα 3: Διαδικασία στατικής αυθεντικοποίησης [47]

Η δημιουργία ενός ακριβούς προφίλ χρήστη είναι βασική προϋπόθεση για μια επιτυχημένη συνεχή αυθεντικοποίηση (CA). Μια σημαντική πρόκληση είναι ότι τα προφίλ του χρήστη μπορεί να υπόκειται σε συνεχείς αλλαγές κατά περιόδους σε περιβάλλοντα δικτύων. Αυτό χαρακτηρίζεται ως παρασυρόμενη συμπεριφορά (behavior drift) και μπορεί να αντιμετωπιστεί με κατάλληλες τεχνικές τεχνητής νοημοσύνης.

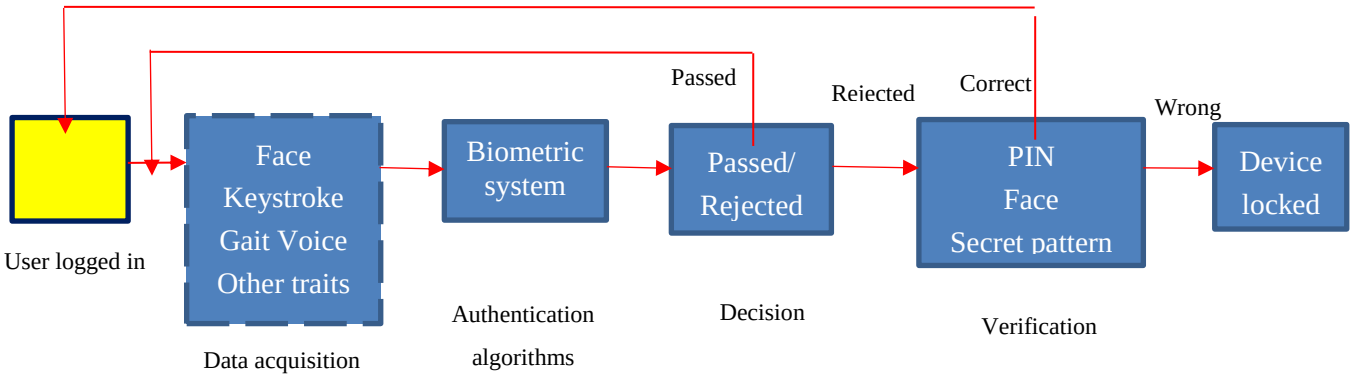


Εικόνα 4: Διαδικασία συνεχούς αυθεντικοποίησης [47]

2.4.2 Συνεχής αυθεντικοποίηση απαραίτητα στάδια

Η Εικόνα 5 δείχνει τη βασική ιδέα ενός συστήματος συνεχούς ελέγχου αυθεντικοποίησης (CA) σε κινητά τηλέφωνα που βασίζεται σε βιομετρικά στοιχεία [49]. Βιομετρικά χαρακτηριστικά όπως το βάδισμα, το σχήμα του προσώπου, το πάτημα ενός πλήκτρου ή η φωνή μετριούνται από τους αισθητήρες που υπάρχουν στην κινητή συσκευή. Στη συνέχεια το βιομετρικό σύστημα θα καθορίσει κατά πόσον αυτά τα βιομετρικά χαρακτηριστικά αντιστοιχούν σε ένα νόμιμο χρήστη ή όχι. Εάν τα

χαρακτηριστικά αντιστοιχούν στον νόμιμο χρήστη τότε το βιομετρικό σύστημα θα συνεχίσει να επεξεργάζεται τα νέα εισερχόμενα δεδομένα. Ωστόσο, αν το βιομετρικό σύστημα παράγει μια αρνητική απάντηση, στη συνέχεια, το σύστημα θα ζητήσει από το χρήστη να επιβεβαιώσει την ταυτότητά του, χρησιμοποιώντας τις παραδοσιακές μεθόδους όπως PIN ή κωδικός πρόσβασης. Εάν ο χρήστης είναι σε θέση να επαληθεύσει την ταυτότητά του, τότε θα είναι σε θέση να χρησιμοποιήσει την κινητή συσκευή του, διαφορετικά η συσκευή θα κλειδωθεί. Σε ένα πρακτικό σύστημα συνεχούς αυθεντικοποίησης το σύνολο της επεξεργασίας συμβαίνει σε πραγματικό χρόνο.



Εικόνα 5: Ένα πλαίσιο CA βασισμένο σε βιομετρικά χαρακτηριστικά

2.4.3 Στάδια σε continuous authentication συστήματα

Σε γενικές γραμμές σε κάθε σύστημα CA υπάρχουν τρία απαραίτητα στάδια. Το data collection, το feature extraction και το evaluation.

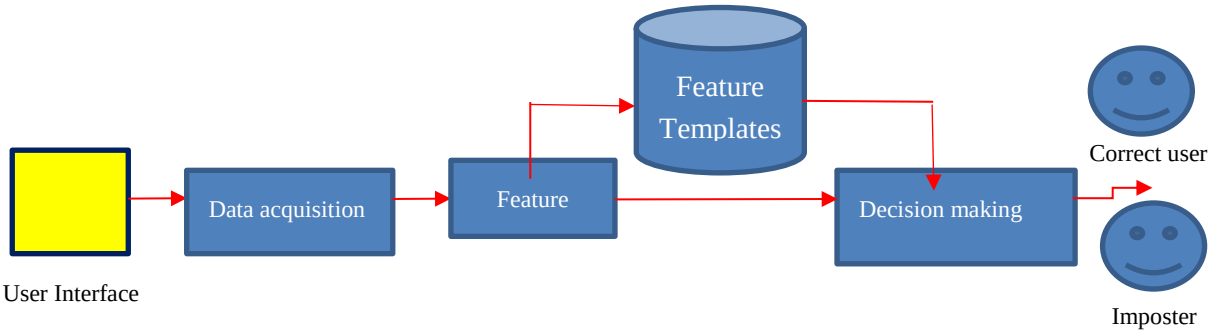
Data collection (acquisition): Είναι το πρώτο βήμα στο σύστημα όπου τα raw βιομετρικά χαρακτηριστικά συλλέγονται από ένα ή περισσότερους αισθητήρες του κινητού τηλέφωνου όπως για παράδειγμα η κάμερα ή η οθόνη αφής (Εικόνα 1). Η ποιότητα των συλλεχθέντων δεδομένων είναι πολύ σημαντική επειδή θα επηρεάσει την επιτυχία της φάσης αναγνώρισης (recognition process). Η ποιότητα των δεδομένων επηρεάζεται από τους χρησιμοποιούμενους αισθητήρες και από το περιβάλλον στο οποίο συλλέγονται τα δεδομένα.

Feature extraction: Πριν από την εξαγωγή των συγκεκριμένων χαρακτηριστικών, τα raw δεδομένα πρέπει να προ-επεξεργαστούν, να εντοπιστούν και να απομακρυνθούν λάθη, να βελτιωθεί η ποιότητα των δεδομένων, ειδικά αν τα δεδομένα συλλέχθηκαν σε ένα μη ελεγχόμενο περιβάλλον και με μη συνεργατικούς χρήστες. Ύστερα, όταν τα δεδομένα καθαριστούν και επεξεργαστούν, ένα σετ από διακριτά χαρακτηριστικά εξάγεται. Τα εξαγόμενα χαρακτηριστικά εξαρτώνται από τον τύπο των raw δεδομένων, για παράδειγμα αν τα συλλεχθέντα δεδομένα περιέχουν χρονοσήμανση τότε χρονικά χαρακτηριστικά μπορούν να εξαχθούν.

Evaluation: Το evaluation περιλαμβάνει το feature templates και το matching και decision-making. Το feature templates είναι μια βάση που περιέχει μια αλληλουχία εξαγόμενων χαρακτηριστικών για ένα συγκεκριμένο χρήστη (π.χ. τον ιδιοκτήτη της συσκευής). Κατασκευάζεται κατά την διάρκεια

της φάσης εγγραφής (enrollment) και χρησιμοποιείται κατά την διάρκεια της φάσης αναγνώρισης (recognition) για να συγκριθεί με τα συλλεχθέντα χαρακτηριστικά για να αυθεντικοποιήσει το χρήστη.

Το matching και decision-making χρησιμοποιείται μόνο κατά την διάρκεια της φάσης αναγνώρισης όπου συγκρίνονται τα εξαχθέντα χαρακτηριστικά με τα ήδη αποθηκευμένα χαρακτηριστικά στη βάση για να παράγουν ένα σκορ ταύτισης και να πάρει το σύστημα μια απόφαση. Η απόφαση δείχνει αν ο χρήστης είναι ο νόμιμος ή κάποιος εισβολέας (Εικόνα 6).



Εικόνα 6: Η διαδικασία της βιομετρικής αυθεντικοποίησης

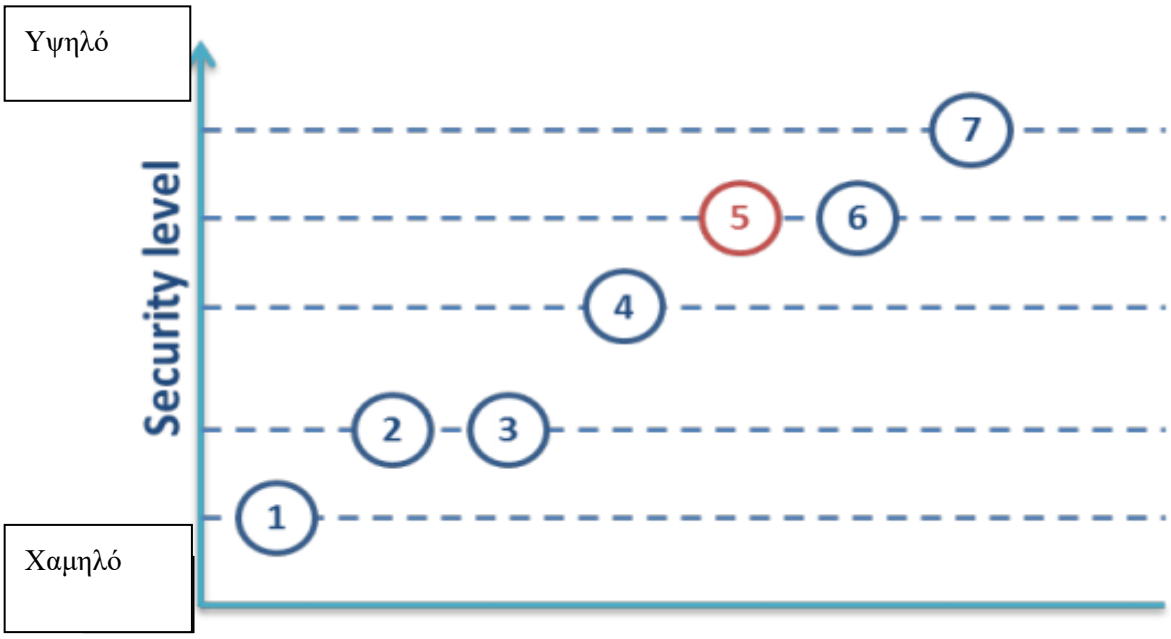
2.5 *Πολυτροπικά βιομετρικά συστήματα (multimodal)*

Τα συστήματα αυθεντικοποίησης που χρησιμοποιούν πολυτροπικά βιομετρικά χαρακτηριστικά προσφέρουν μια ευκαιρία να αυξήσουν την πληθυσμιακή κάλυψη καθώς τα πολλαπλά βιομετρικά στοιχεία μπορούν να λύσουν το ζήτημα με τους χρήστες που δεν έχουν ή δεν είναι δυνατό να επιδείξουν συγκεκριμένα βιομετρικά χαρακτηριστικά. Η χρήση της περισσότερων του ενός βιομετρικών τεχνικών επιτρέπει το σύστημα να μειώσει τον αριθμό των περιπτώσεων όπου το σύστημα δεν είναι σε θέση να λάβει μια απόφαση. Για παράδειγμα, εάν ο χρήστης δεν είναι δυνατό να επαληθευτεί από τη χρήση γλωσσικών χαρακτηριστικών (linguistic profiling) εξαιτίας των ανεπαρκών στοιχείων μέσα στο μήνυμα, ο χρήστης μπορεί να αυθεντικοποιηθεί χρησιμοποιώντας keystroke dynamics ή behaviour profiling. Οι επιδόσεις αυτής της προσέγγιση μπορεί επίσης να βοηθήσει τους χρήστες να παρέχουν όλα τα χαρακτηριστικά (Jain et al [50]). Επιπλέον, η ανάγκη να παρέχονται περισσότερα από ένα δείγματα θα βοηθήσει στην πρόληψη επιθέσεων spoof, επειδή ένας εισβολέας θα πρέπει να παρακάμψει περισσότερο από μια τεχνικές. Ως εκ τούτου, τα πολυτροπικά βιομετρικά χαρακτηριστικά μπορούν να βελτιώσουν την ακρίβεια και την αξιοπιστία των μονοτροπικών συστημάτων. Τα πολυτροπικά βιομετρικά συστήματα απαιτούν ένα συνδυασμό δύο ή περισσότερων βιομετρικών μεθόδων και δεδομένων. Υπάρχουν διάφορα σενάρια που είναι πιθανά στις πολυτροπικές βιομετρικές μεθόδους συμπεριλαμβανομένων των παρακάτω (Ross et al [51]):

- Πολλαπλοί αισθητήρες: η χρήση από περισσότερους από έναν αισθητήρα για να συλλάβει ένα βιομετρικό χαρακτηριστικό (π.χ. αισθητήρες δακτυλικών αποτυπωμάτων οπτικοί και χωρητικοί).

- Πολλαπλοί υποτύποι: η χρήση περισσοτέρων από μίας υποκατηγορίας του ίδιου βιομετρικού χαρακτηριστικού (π.χ. ο αριστερός δείκτης και ο δεξιός δείκτης).
- Πολλαπλά δείγματα: η χρήση περισσότερων του ενός δείγματος του ίδιου βιομετρικού χαρακτηριστικού (π.χ. πολλαπλές εικόνες του προσώπου ενός ατόμου υπό συνθήκες διαφορετικής πόζας / φωτισμού)
- Πολλαπλοί αλγόριθμοι: η χρήση περισσότερων matcher αλγόριθμων στη διαδικασία ταξινόμησης (π.χ. πολλαπλές ταυτίσεις δακτυλικών αποτυπωμάτων που βασίζονται σε μικρολεπτομέρειες του αποτυπώματος)
- Πολλαπλά βιομετρικά χαρακτηριστικά: η χρήση περισσότερων από ένα χαρακτηριστικών (π.χ. πρόσωπο, δακτυλικό αποτύπωμα και η ίριδα).

Όταν χρησιμοποιείται ο συνδυασμός παραγόντων αυθεντικοποίησης, είναι σημαντικό να βεβαιωθούμε ότι όλοι οι παράγοντες χρησιμοποιούνται και απαιτούνται για την αυθεντικοποίηση. Για παράδειγμα, για να έχει ο χρήστης πρόσβαση σε τραπεζικό λογαριασμό και να κάνει μεταφορά χρημάτων θα πρέπει να γνωρίζει και τον μυστικό κωδικό πρόσβασης και να έχει μαζί του ένα token, σε περίπτωση που λείπει ένα από αυτά δεν θα μπορεί να κάνει τη μεταφορά . Στην Εικόνα 7 το (1) είναι κάτι που ο χρήστης ξέρει, το (2) κάτι που ο χρήστης έχει, το (3) κάτι που ο χρήστης ξέρει και κάτι που έχει, το (4) κάτι που ο χρήστης είναι ή κάνει, το (5) κάτι που ο χρήστης έχει και κάτι που κάνει ή είναι, το (6) κάτι που ο χρήστης ξέρει και κάτι που είναι ή κάνει και το (7) κάτι που ο χρήστης ξέρει και κάτι που έχει και κάτι που είναι ή κάνει.

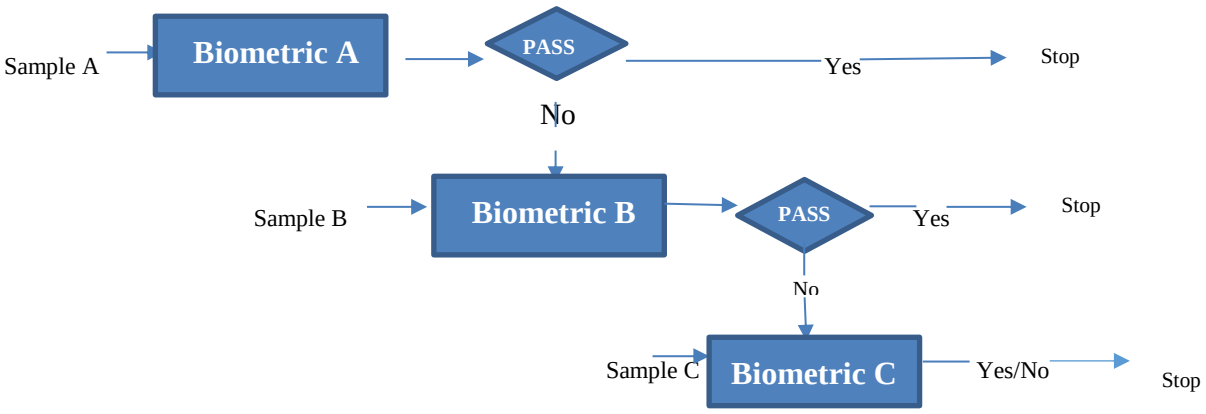


Εικόνα 7: Επίπεδα ασφάλειας σε ένα σύστημα αυθεντικοποίησης

Κατά τη διάρκεια κάθε μιας αλληλεπίδρασης με τους χρήστες, τα βιομετρικά δεδομένα που συλλέγονται θα αυξάνονται και θα ενσωματώνονται στο ήδη υπάρχον δείγμα δεδομένων από έναν αριθμό αισθητήρων που είναι διαθέσιμοι στην κινητή συσκευή. Επομένως, είναι πιθανόν ότι τα πολλαπλά δείγματα, οι πολλαπλοί υποτύποι, οι πολλαπλοί αλγόριθμοι και τα πολλαπλά βιομετρικά χαρακτηριστικά θα είναι διαθέσιμα σε οποιαδήποτε κινητή συσκευή.

Η σειρά ή η ακολουθία με την οποία αποκτώνται τα βιομετρικά δείγματα μπορεί να εκτελεστεί σε μια σύγχρονη και ασύγχρονη προσέγγιση. Η σύγχρονη αναφέρεται στη σύλληψη βιομετρικών δειγμάτων ταυτόχρονα ή παράλληλα. Η ασύγχρονη προσέγγιση αναφέρεται στην καταγραφή των βιομετρικών δειγμάτων διαδοχικά. Και οι δύο αυτές προσεγγίσεις θα μπορούσαν αποτελεσματικά να συμβαίνουν σε οποιοδήποτε χρονικό σημείο καθώς τα δείγματα καταγράφονται συνεχώς στο παρασκήνιο. Η επεξεργασία των δειγμάτων μπορεί να πραγματοποιηθεί επίσης με τις σύγχρονες και ασύγχρονες μεθοδολογίες.

Σε σειριακή λειτουργία, η επεξεργασία των δειγμάτων πραγματοποιείται διαδοχικά, όπως φαίνεται στην Εικόνα 8. Εάν το δείγμα A του χρήστη δεν μπορούσε να επαληθευθεί, το σύστημα μπορεί να χρησιμοποιήσει το δείγμα B ή C. Όταν το σύστημα έχει βεβαιότητα για την ταυτότητα του χρήστη μετά την επεξεργασία του πρώτου βιομετρικού δείγματος, ο χρήστης δεν υποχρεούται να παρέχει τα άλλα δείγματα. Έτσι ένα τέτοιο πολυτροπικό βιομετρικό συστήματος είναι πιο βολικό για τον χρήστη και απαιτεί λιγότερο χρόνο αναγνώρισης σε σύγκριση με μια παράλληλη προσέγγιση. Παρόλα αυτά, για μια πιο διαφανή προσέγγιση η οποία παραμερίζει την ευκολία για τον χρήστη, είναι η τελευταία αναφερόμενη παράλληλη προσέγγιση, η οποία προσφέρει την ευκαιρία να βελτιώσουμε τις επιδόσεις επαλήθευσης των ασθενέστερων συμπεριφορικών βιομετρικών χαρακτηριστικών.



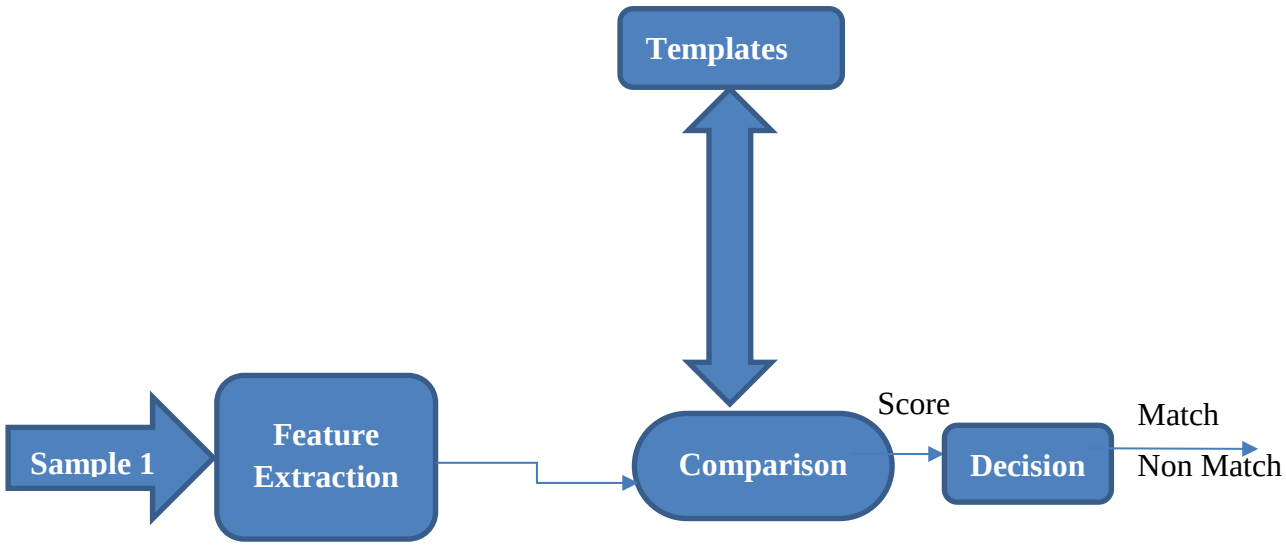
Εικόνα 8: Serial mode επεξεργασίας βιομετρικών δειγμάτων [52]

2.5.1 Συγχώνευση πληροφοριών σε multimodal βιομετρικά συστήματα

Ένα από τα θεμελιώδη ζητήματα στο σχεδιασμό των πολυτροπικών βιομετρικών συστημάτων είναι να προσδιοριστεί ο τύπος των πληροφοριών που πρέπει να συγχωνευτούν. Η συγχώνευση (fusion) πληροφορίων γίνεται σε διάφορα επίπεδα: sensor level, feature level, score level, rank level και decision level όπως περιγράφεται παρακάτω. Συμβατικά, η διαθεσιμότητα του περιεχομένου των πληροφοριών μειώνεται από το επίπεδο του sensor στο επίπεδο decision.

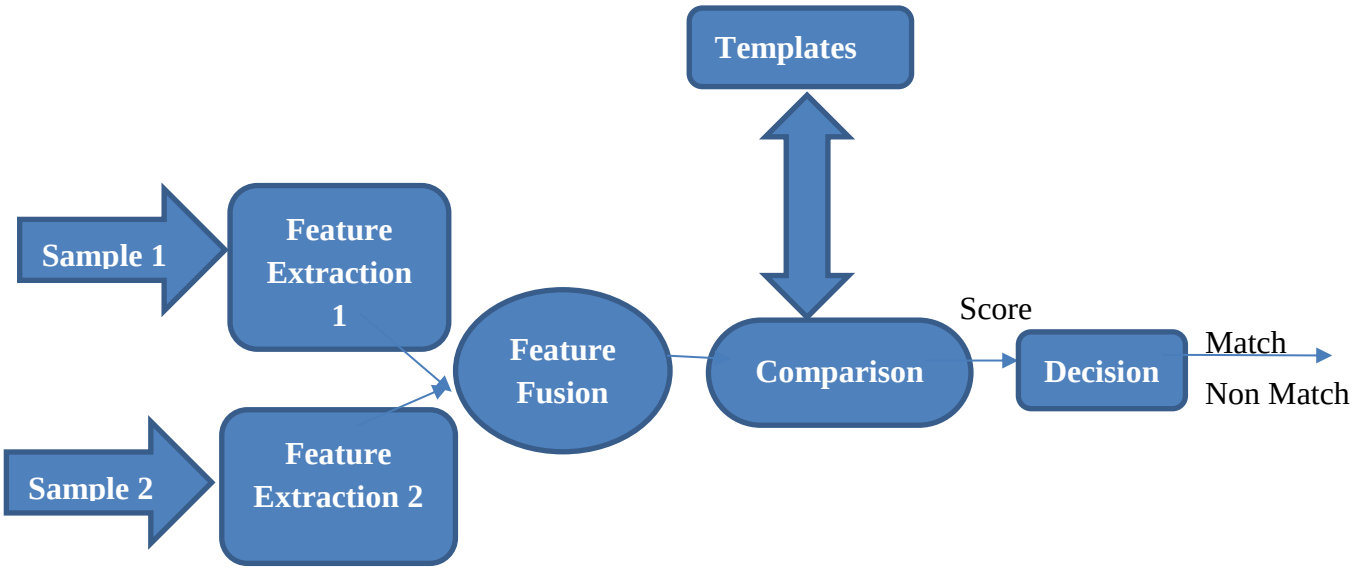
2.5.1.1 Επίπεδο συνδυασμού (fusion)

Στα πολυτροπικά βιομετρικά χαρακτηριστικά, ο συνδυασμός μεθόδων (fusion) μπορεί να γίνει αποτελεσματικά σε οποιοδήποτε σημείο εντός του βιομετρικού συστήματος. Σε αυτή την ενότητα παρουσιάζεται μια σύντομη περιγραφή των επίπεδων συνδυασμού.



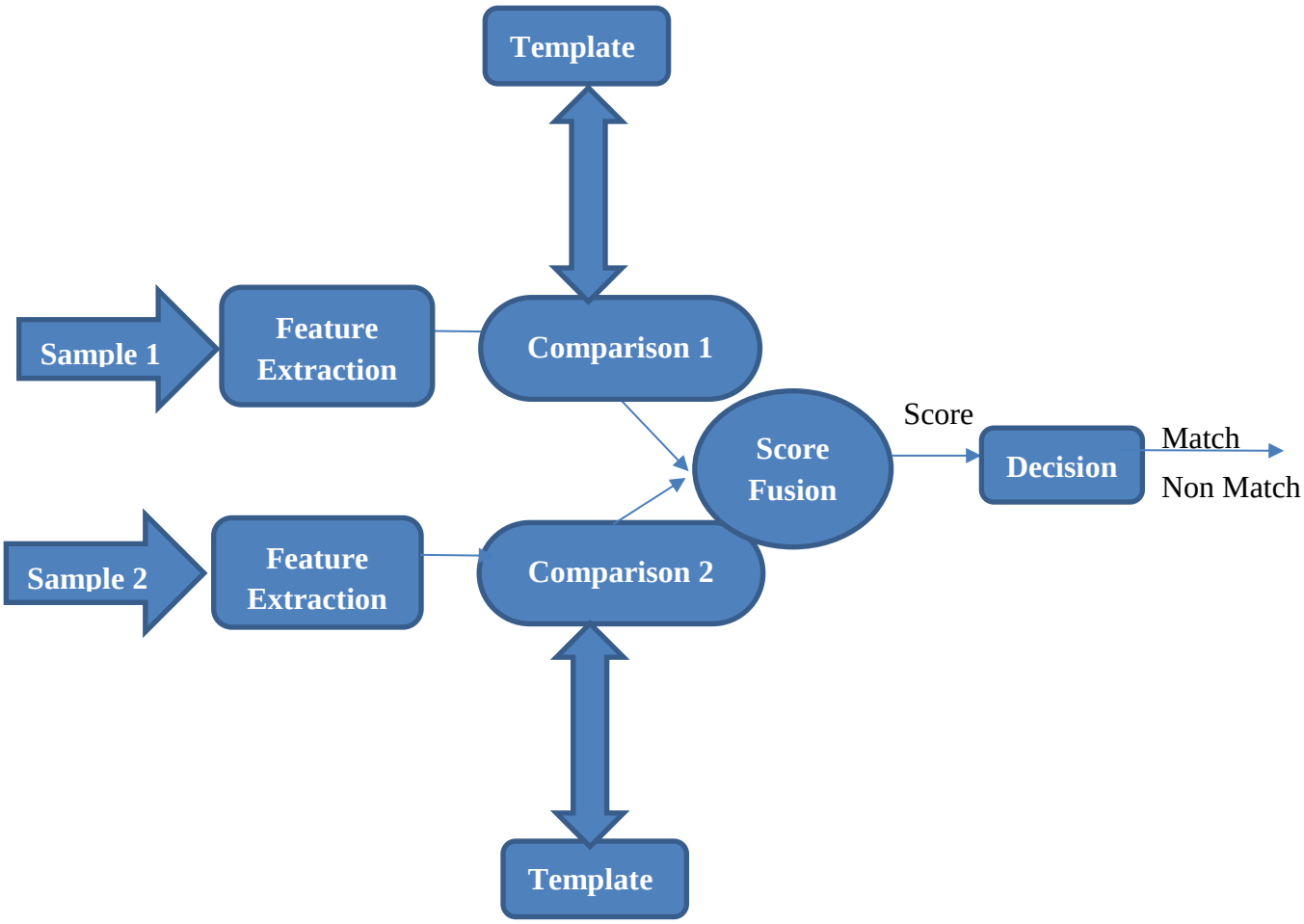
Εικόνα 9: Γενική αποτύπωση μίας (unimodal) βιομετρικής διαδικασίας [51]

1. Sensor level: τα πρωτογενή δεδομένα που αποκτήθηκαν από πολλαπλούς αισθητήρες συνδυάζονται στο sensor level πριν γίνει η εξαγωγή των χαρακτηριστικών τους γνωρισμάτων. Σε αυτό το είδος της συγχώνευσης, τα πολλαπλά στοιχεία πρέπει να είναι συμβατά, ως εκ τούτου συνήθως γίνεται συγχώνευση του ίδιου βιομετρικού χαρακτηριστικού, που λαμβάνεται με τη χρήση είτε ενός μεμονωμένου αισθητήρα ή διαφορετικών συμβατών. Για παράδειγμα, οι λήψεις δακτυλικών αποτυπωμάτων μπορούν να αποκτηθούν από οπτικούς και "solid state" αισθητήρες και μπορούν να συνδυαστούν για να σχηματίσουν μια ενιαία εικόνα που να είναι η είσοδος για την διαδικασία ταύτισης.
2. Feature level: το feature level αναφέρεται στην ενοποίηση στοιχείων που παρουσιάζονται από δύο βιομετρικά σετ χαρακτηριστικών του ίδιου ατόμου. Αυτά τα σετ ενοποιούνται για να δημιουργήσουν ένα μοναδικό σετ χαρακτηριστικών το οποίο πρέπει να συγκριθεί με το πρότυπο εγγραφής στη βάση δεδομένων του συστήματος.



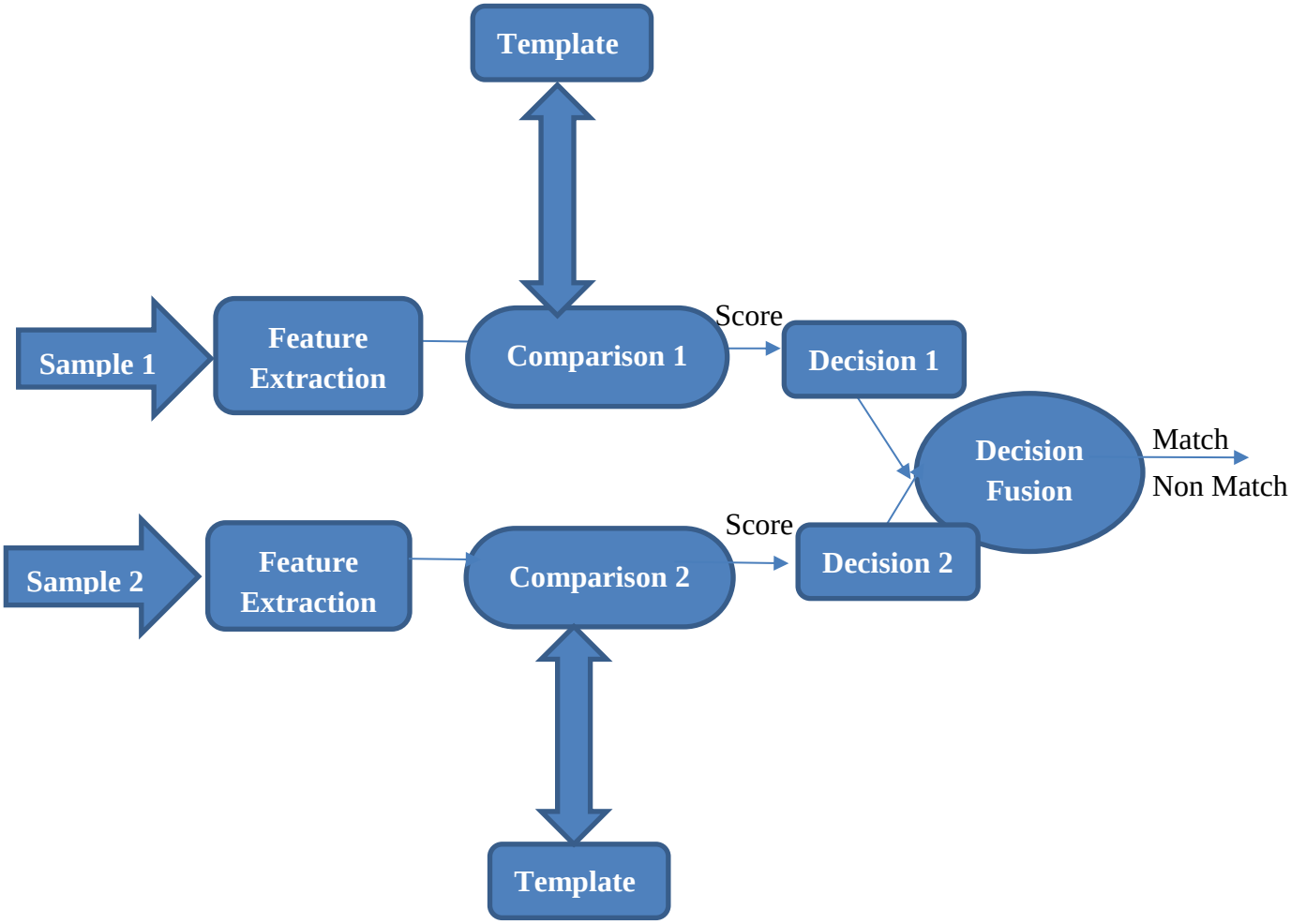
Εικόνα 10: Feature-level συγχώνευση [51]

3. Score level: στη score level συγχώνευση, τα σύνολα χαρακτηριστικών γνωρισμάτων εξάγονται ανεξάρτητα από κάθε υποσύστημα, που αργότερα συγκρίνεται με τα ξεχωριστά αποθηκευμένη αντίστοιχα πρότυπα. Ανάλογα με την εγγύτητα του συνόλου χαρακτηριστικών γνωρισμάτων και του πρότυπου, κάθε υποσύστημα υπολογίζει το δικό του σκορ ταύτισης. Το επιμέρους σκορ τελικά συγχωνεύεται για να παράγει ένα μοναδικό σκορ ταύτισης για την διαδικασία λήψης απόφασης.



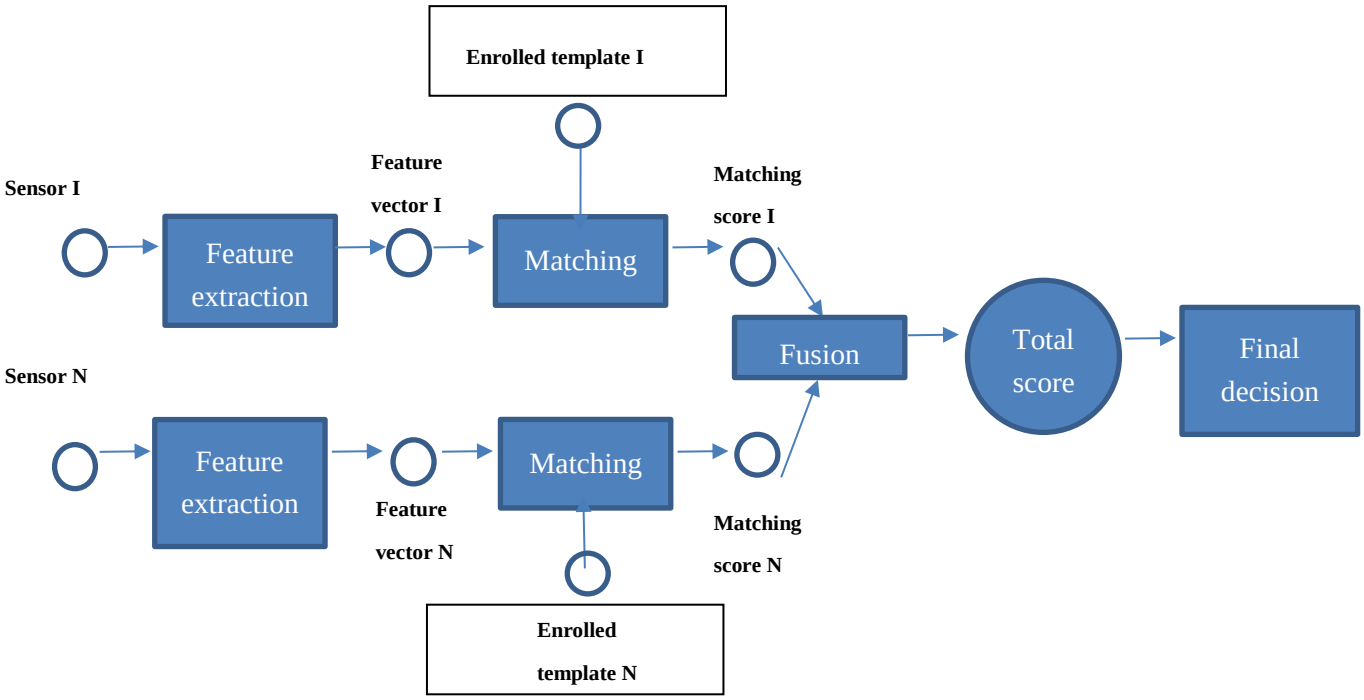
Εικόνα 11: Score-level συγχώνευση [51]

4. Rank level: αυτός ο τύπος της συγχώνευσης διεξάγεται στη λειτουργία αναγνώρισης, όπου κάθε υποσύστημα συσχετίζει μια κατάταξη με κάθε εγγεγραμμένη ταυτότητα. Έτσι, τα συστήματα κατάταξης συγχωνεύουν τα σχήματα ενώνοντας τις τάξεις που παράγονται από τα επιμέρους υποσυστήματα, προκειμένου να καταλήξει στην τελική απόφαση.
5. Decision level: επίσης γνωστό ως abstract level, η συγχώνευση γίνεται συνδυάζοντας την απόφαση αυθεντικοποίησης που ελήφθη από επιμέρους βιομετρικούς matchers. Η συγχώνευση σε αυτό το επίπεδο είναι υπερβολικά άκαμπτη, δεδομένου ότι μόνο περιορισμένες πληροφορίες είναι διαθέσιμες σε αυτό το επίπεδο.



Εικόνα 12: Decision-level συγχώνευση [51]

Όπως προαναφέρθηκε, ένα από τα πιο θεμελιώδη ζητήματα των πολυτροπικών βιομετρικών συστημάτων είναι να προσδιορίσουν τον τύπο των πληροφοριών που θα πρέπει να ενοποιηθούν από τη μονάδα συγχώνευσης. Δεδομένου ότι, η ποσότητα των πληροφοριών συνεχώς μειώνεται όταν πηγαίνουμε από το sensor level προς το decision level, τα πολυτροπικά βιομετρικά συστήματα τα οποία συγχωνεύουν πληροφορίες στα πρώτα στάδια της επεξεργασίας αναμένεται να επιφέρουν πιο ελπιδοφόρα αποτελέσματα από ό,τι τα συστήματα που συγχωνεύουν πληροφορίες σε μεταγενέστερο στάδιο. Υπάρχει μια πληθώρα εργασιών που συζητούν διαφορετικά σχήματα συγχώνευσης για να ενσωματώσουν πολλαπλές πηγές βιομετρικών πληροφοριών σε διαφορετικά επίπεδα. Συνήθως, τα οφέλη της τεχνικής συγχώνευσης αποτελούν αντικείμενο εκμετάλλευσης όταν οι επιμέρους πηγές πληροφοριών είναι συμπληρωματικής φύσης.



Εικόνα 13: Συνοπτικό multimodal fusion σε κάθε επίπεδο [53]

2.5.1.2 Τα πλεονεκτήματα των πολυτροπικών βιομετρικών συστημάτων

Συστήματα που ενσωματώνουν τα στοιχεία από δύο ή περισσότερα βιομετρικά χαρακτηριστικά, προκειμένου να είναι πιο αξιόπιστα για τον προσδιορισμό της ταυτότητα ενός ατόμου, είναι γνωστά ως πολυτροπικά βιομετρικά συστήματα. Τα πολυτροπικά βιομετρικά συστήματα προσφέρουν τα εξής πλεονεκτήματα έναντι των μονοτροπικών συστημάτων:

1. βελτίωση της συνολικής ακρίβειας που επιτυγχάνεται συνδυάζοντας τα βιομετρικά στοιχεία που προέρχονται από διαφορετικές πηγές, χρησιμοποιώντας μια τεχνική αποτελεσματικής συγχώνευσης.
2. η επίδραση του θορύβου στα εισερχόμενα δεδομένα μπορεί να μετριαστεί με την συγχώνευση πολλών βιομετρικών πηγών. Για παράδειγμα, σε ένα σύστημα που βασίζεται στην αναγνώριση προσώπου και δακτυλικών αποτυπωμάτων, εάν το δείγμα προσώπου που αποκτήθηκε δεν είναι επαρκούς ποιότητας, τότε το δείγμα του δακτυλικού αποτυπώματος μπορεί να εξακολουθεί να παρέχει επαρκή διάκριση πληροφορίων ώστε να εξασφαλίσει αξιόπιστη απόφαση για το σύστημα.
3. τα πολυτροπικά βιομετρικά συστήματα είναι επίσης σε θέση να αντιμετωπίσουν το πρόβλημα της μη-καθολικότητα και να βοηθήσουν να μειωθεί failure to enroll rate (FTER) και failure to capture rate (FTCR). Για παράδειγμα, εάν ένα άτομο δεν είναι σε θέση να εγγραφεί σε ένα σύστημα δακτυλικών αποτυπωμάτων λόγω πληγών και καψιμάτων που μπορεί να έχει, μπορεί και σε αυτή την περίπτωση να προσδιοριστεί χρησιμοποιώντας άλλα βιομετρικά χαρακτηριστικά όπως την ίριδα κλπ.

4. τα πολυτροπικά βιομετρικά συστήματα προσφέρουν έναν βαθμό ελευθερίας για την αυθεντικοποίηση του χρήστη. Για παράδειγμα, κατά τη διάρκεια της εγγραφής, το πρόσωπο, τα δακτυλικά αποτυπώματα και η ίριδα αποτυπώνονται. Αργότερα, κατά την διάρκεια της αυθεντικοποίησης, οποιοσδήποτε συνδυασμός αυτών των χαρακτηριστικών μπορεί να αποκτηθεί, ανάλογα με τη φύση της εφαρμογής ή την ευκολία του χρήστη.

   Επομένως, ένα σωστά σχεδιασμένο πολυτροπικό βιομετρικό σύστημα μπορεί να βελτιώσει την ακρίβεια και την αξιοπιστία των μονοτροπικών συστημάτων με την αύξηση της πληθυσμιακής κάλυψης. Εκτεταμένες εμπειρικές μελέτες έχουν δείξει ότι είναι αποτελεσματικά για το σκοπό αυτό.

   Ένα χαρακτηριστικό παράδειγμα ρεαλιστικής εφαρμογής multimodal χαρακτηριστικών σε κινητά τηλέφωνα αποτελεί το Samsung S9. Το Samsung S9 χρησιμοποιεί το λεγόμενο Intelligent Scan [54], [55] το οποίο συνδυάζει αναγνώριση προσώπου και ίριδας κάτι που αποτελεί μια εφαρμογή του multimodal συστήματος στα σύγχρονα κινητά τηλέφωνα. Σε αντίθεση για παράδειγμα το αντίστοιχο κινητό της Apple χρησιμοποιεί μόνο την αναγνώριση προσώπου σαν το μοναδικό βιομετρικό χαρακτηριστικό. Το Intelligent Scan χρησιμοποιεί την αναγνώριση προσώπου όταν ο χρήστης είναι σε φωτεινό περιβάλλον ενώ την αναγνώριση ίριδας όταν είναι σε περιβάλλον με χαμηλό φως και τον συνδυασμό και των δύο όταν είναι δύσκολο να αποφασίσει για την αυθεντικοποίηση του χρήστη. Μάλιστα και το τελευταίο μοντέλο της Apple, το Iphone Xs, που παρουσιάστηκε τον Σεπτέμβριο του 2018, δεν εφαρμόζει κάποια μορφή Multimodal αυθεντικοποιησης αλλά μόνο αναγνώριση προσώπου (Face ID) [56].

2.5.1.3 Σύνοψη για τα πολυτροπικά βιομετρικά συστήματα

Ραγδαίες εξελίξεις στα δίκτυα των υπολογιστών, στις επικοινωνίες, και στη φορητότητα σε συνδυασμό με τις έντονες ανησυχίες για την ασφάλεια και την κλοπή ταυτότητας έχουν ως αποτέλεσμα μια αδήριτη ανάγκη για πιο αξιόπιστα συστήματα αυθεντικοποίησης. Τα συμβατικά σχήματα διαχείρισης ταυτότητας που βασίζονται σε κωδικούς πρόσβασης ή κάρτες πρόσβασης, έχουν περιορισμένη ικανότητά ασφαλείας. Μερικοί από τους περιορισμούς των συμβατικών μεθόδων αυθεντικοποίησης μπορούν να αντιμετωπιστούν με τη χρήση βιομετρικών στοιχείων, που χρησιμοποιούν τα φυσιολογικά και τα συμπεριφορικά χαρακτηριστικά όπως το πρόσωπο, τα δακτυλικά αποτυπώματα, η ίριδα κ.λπ. Ως αποτέλεσμα, τα βιομετρικά συστήματα αναπτύσσονται σε διάφορες εφαρμογές, συμπεριλαμβανομένου αυτών του ταξιδιού και της μεταφοράς, χρηματοπιστωτικών ιδρυμάτων, υγειονομικής περίθαλψης, υπηρεσίες επιβολής του νόμου και συνοριακής διέλευσης, αυξάνοντας έτσι την ασφάλεια και μειώνοντας την πιθανότητα απάτης ως προς την ταυτότητα του χρήστη. Τα μονοτροπικά βιομετρικά συστήματα (που χρησιμοποιούν μόνο ένα βιομετρικό χαρακτηριστικό) υποφέρουν από διάφορους παράγοντες όπως ο θόρυβος στα δεδομένα, η λανθασμένη αλληλεπίδραση του χρήστη κλπ. Μερικοί από τους περιορισμούς των μονοτροπικών βιομετρικών συστημάτων μπορούν να μετριαστούν με τη χρήση πολυτροπικών βιομετρικών συστημάτων (συστήματα που χρησιμοποιούν περισσότερα από ένα βιομετρικά χαρακτηριστικά). Ένα συστηματικά σχεδιασμένο πολυτροπικό βιομετρικό σύστημα μπορεί να αυξήσει την ακρίβεια ταύτισης και την πληθυσμιακή κάλυψη σε σύγκριση με τα μονοτροπικά

συστήματα. Στα πολυτροπικά συστήματα τα στοιχεία παρουσιάζονται από πολλαπλές βιομετρικές πηγές και μπορούν να ενοποιηθούν σε διάφορα επίπεδα: sensor level, feature level, score level, rank level και decision level. Η συγχώνευση στο score level έχει λάβει τη μέγιστη προσοχή από την ερευνητική κοινότητα, λόγω της ευκολία στην πρόσβαση και του συνδυασμού του σκορ ταύτισης.

2.6 ***Σύνοψη***

Ο αυξανόμενος αριθμός των χρηστών smarthphones έχει ως αποτέλεσμα την αύξηση των ιδιωτικών πληροφοριών που αποθηκεύονται στα smarthphones. Έτσι δημιουργούνται συνεχώς πολυάριθμα προβλήματα ασφαλείας και προστασίας των προσωπικών δεδομένων. Για να επιλυθούν αυτά τα ζητήματα, οι ερευνητές έχουν υλοποιήσει πολλές μεθόδους, συμπεριλαμβανομένης της CA με βάση τη συμπεριφορά του χρήστη και των multimodal βιομετρικών χαρακτηριστικών. Οι νέες μέθοδοι πρέπει να επικεντρωθούν σε πολλαπλά χαρακτηριστικά έτσι ώστε να εξασφαλιστεί το σύστημα ενάντια σε μια ποικιλία επιθέσεων κάνοντας το ακόμη πιο ασφαλές και εύκολο στη χρήση, προσαρμοζόμενο σε κάθε χρήστη.

Εκτός από τις μεθόδους που περιγράφονται παραπάνω, μια πολλά υποσχόμενη προσέγγιση είναι η συμπεριφορά των χρηστών από την άποψη της χρήσης μιας εφαρμογής. Κάθε smartphone περιέχει εφαρμογές που μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς. Ως εκ τούτου, κάνοντας CA που βασίζεται στην χρήση της εφαρμογής μπορεί να είναι ένας τρόπος για την ενίσχυση της ασφάλειας και της ιδιωτικότητας. Για παράδειγμα, οι εφαρμογές μπορούν να ταξινομηθούν σε κοινωνικές εφαρμογές όπως το Twitter, το Facebook, το Google plus και το Linkedin, εφαρμογές πολυμέσων, όπως εκείνες που σχετίζονται με φωτογραφίες, βίντεο, εφαρμογές chat όπως το Viber, WhatsApp, Snapchat, Telegram. Μετρώντας το πώς, το πότε και για πόση διάρκεια αυτές οι εφαρμογές χρησιμοποιούνται από τον χρήστη είναι κάτι που μπορεί να βοηθήσει ένα σύστημα αυθεντικοποίησης σιωπηρά να μάθει και να ξεχωρίζει τους εξουσιοδοτημένους από τους μη εξουσιοδοτημένους χρήστες. Η δημιουργία ενός corpus για διαφορετικά μοτίβα χρήσης συγκεκριμένων εφαρμογών με ένα μεγάλο αριθμό θεμάτων για έναν μεγάλο αριθμό ημερών θα είναι ένας εξαιρετικός τρόπος για να βοηθήσει την μελλοντική ανάπτυξη αυτού του τύπου αυθεντικοποίησης.

3

Βιβλιογραφική ανασκόπηση

3.1 *Εισαγωγή*

Τα τελευταία χρόνια σημειώθηκε μια σημαντική αύξηση στην ακρίβεια και την αξιοπιστία της αυθεντικοποίησης μέσω βιομετρικών συστημάτων. Ωστόσο, τα περισσότερο αξιολογημένα και ελεγμένα βιομετρικά συστήματα έχουν επίσης κάποιους περιορισμούς, που σχετίζονται με τον τύπο των δεδομένων και τη μεθοδολογία. Πιο συγκεκριμένα, η απόδοση των βιομετρικών συστημάτων πάσχει λόγω της παρουσίας θορύβου σε δεδομένα εισόδου, της μη-καθολικότητα και άλλους πιθανούς παράγοντες που μπορούν να επηρεάσουν την απόδοση, την ασφάλεια και τη χρηστικότητα των συστημάτων αυτών. Για την χρηστικότητα, για παράδειγμα, έχουν προταθεί διάφορα συστήματα αξιολόγησης και ένα ευρέως αποδεκτό είναι το System usability scale (SUS) [57] που αποτελείται από ερωτήσεις με βαθμολογία από 1 έως 5 με 1 το διαφωνώ εντελώς και 5 το συμφωνώ απολύτως για να μετράτε η χρηστικότητα των προτεινόμενων μεθόδων από πραγματικούς χρήστες.

Ένα πολυτροπικό βιομετρικό σύστημα είναι ένας νεότερος τρόπος που αντιμετωπίζει κάποια από τα προβλήματα που συνδέονται με τα μονοτροπικά βιομετρικά συστήματα. Ενσωματώνει την ενοποίηση των δεδομένων που προέρχονται από πολλαπλές πηγές πληροφοριών. Τα πολυτροπικά συστήματα μπορούν να βελτιώσουν σημαντικά την απόδοση αναγνώρισης και να αυξήσουν την πληθυσμιακή κάλυψη (μειώνοντας έτσι το failure to enroll rate (FTER)), να αποτρέψουν τις επιθέσεις spoof και να αυξήσουν τον βαθμό της ελευθερίας. Παρόλο που τα συστήματα αυτά απαιτούν περισσότερο χώρο αποθήκευσης, χρειάζονται περισσότερο χρόνο επεξεργασίας και περισσότερη υπολογιστική ισχύ σε σύγκριση με τα μονοτροπικά βιομετρικά συστήματα, τα πλεονεκτήματα τους βοηθούν την ανάπτυξή τους σε μεγάλης κλίμακας συστήματα ελέγχου αυθεντικοποίησης .

3.2 *Μεθοδολογία*

Η μεθοδολογία μου βασίζεται στη συλλογή πολλών δημοσιευμένων πηγών οι οποίες είναι σχετικές με το θέμα της εργασίας μου. Οι πηγές αυτές συνοδεύονται από σχολιασμό και κριτική ανάλυση του περιεχομένου και των συμπερασμάτων τους. Δεν υπάρχει κάποιος περιορισμός σε βιβλία ή άρθρα καθώς συνέλεξα υλικό και από πολλές ιστοσελίδες. Σε μια προσπάθεια να αυξήσω την αποτελεσματικότητα της έρευνας μου χρησιμοποίησα προχωρημένες μεθόδους αναζήτησης στο

google και επίσης χρησιμοποίησα λέξεις όπως «and» / «or» / «not». Μερικές από τις λέξεις κλειδιά που χρησιμοποίησα ήταν Mobile Phones, Behavioural biometrics, Continuous Authentication, Walking gait, Touch gestures, Multi modal, Input patterns, Location familiarity, Power consumption. Οι κύριες κατηγορίες που προέκυψαν ήταν τα βιομετρικά χαρακτηριστικά (biometrics), η συνεχής αυθεντικοποίηση (Continuous Authentication – CA) και η πολυτροπική αυθεντικοποίηση (Multimodal).

3.3 *Τρόπος βάδισης (Walking gait)*

Το Walking gait είναι η αυθεντικοποίηση μέσω του τρόπου που περπατούν οι χρήστες [58]. Τα στοιχεία που απαιτούνται για την αυθεντικοποίηση βασίζονται στο βάδισμα που μετριέται από το ενσωματωμένο επιταχυνσιόμετρο και το γυροσκόπιο. Μόλις τα πρωτογενή (raw) δεδομένα μετρηθούν, εξάγονται τα χαρακτηριστικά γνωρίσματα που στη συνέχεια τροφοδοτούνται σε ταξινομητές οι οποίοι θα διακρίνουν τους χρήστες. Τα τελευταία χρόνια, έχουν αναπτυχθεί μια σειρά από διαφορετικές μεθόδους για αναγνώριση της βάδισης στις κινητές συσκευές [59], [60], [61], [62], [63] και [64]. Αυτές οι μέθοδοι διαφέρουν ουσιαστικά ως προς τους τύπους των χαρακτηριστικών που εξάγονται από τα πρωτογενή δεδομένα για κατάταξη ή από τους τύπους ταξινόμησης που χρησιμοποιούνται για την αυθεντικοποίηση. Για παράδειγμα, μέθοδοι που βασίζονται στη συσχέτιση, την ανάλυση συχνοτήτων και στη στατική κατανομή δεδομένων χρησιμοποιούνται στο [59], ενώ οι μέθοδοι που βασίζονται στην Dynamic Time Warping (DTW) χρησιμοποιούνται στην [62], [63]. Το [61] προτείνει το Hidden Markov Models (HMMs) για αναγνώριση της βάδισης. Ειδικότερα, ένας αισθητήρας προσανατολισμού που ονομάζεται Gait Dynamic Images (GDIs), προτάθηκε στο [64]. Στο [60] χρησιμοποιείται για την αναγνώριση της βάδισης η ανάλυση με φασματογράφημα.

Ο Muaaz και Mayrhofer [65] αξιολόγησαν την ασφάλεια της gait αναγνώρισης κάτω από ρεαλιστικές επιθέσεις μίμησης και πέτυχαν ένα EER 13% σε ένα σύνολο 35 συμμετεχόντων. Ωστόσο απαιτούνται περισσότερες δοκιμές ώστε να εξαχθεί ένα ασφαλές συμπέρασμα για την αντοχή τους σε επιθέσεις μίμησης.

Ο Benabdelkader et al. [66] παρουσίασε μια παραμετρική προσέγγιση για την ανθρώπινη αναγνώριση από βίντεο χαμηλής ανάλυσης χρησιμοποιώντας ως παραμέτρους το ύψος και το διασκελισμό του περπατήματος. Η προσέγγιση αυτή έδειξε ότι ένα πρόσωπο μπορεί να προσδιοριστεί σωστά με 49% ακρίβεια όταν χρησιμοποιούνται οι παράμετροι ύψος και διασκελισμός. Η μέθοδος αυτή δούλευε με εικόνες χαμηλής ανάλυσης και ήταν ανθεκτική στις αλλαγές φωτισμού, ειδών ένδυσης, καθώς και στον εντοπισμό σφαλμάτων.

Ο Mantyjarvi et al. [59], έδειξε ότι οι χρήστες μπορούν να προσδιοριστούν με μια νέα μέθοδο αναγνώρισης βηματισμού. Στο πείραμα εξέτασαν τους χρήστες να περπατάνε με γρήγορο, κανονικό και αργό ρυθμό σε ξεχωριστές ημέρες φορώντας μια συσκευή επιταχυνσιόμετρου στη ζώνη τους, στο πίσω μέρος. Χρησιμοποίησαν τρεις προσεγγίσεις: την συσχέτιση, την συχνότητα τομέα και την διασπορά των στατιστικών δεδομένων (correlation, frequency domain και data distribution statistics). Επιτεύχθηκε EER 7% με τη μέθοδο συσχέτισης ενώ η συχνότητα τομέα και δύο παραλλαγές διασποράς στατιστικών δεδομένων είχαν EER 10%, 18% και 19%, αντίστοιχα.

Ο Gafurov et al. [67], εισήγαγε μια προσέγγιση μελέτης της βάδισης, τα δεδομένα της οποίας προέρχονται από μια συσκευή συνδεδεμένη με την κνήμη των συμμετεχόντων. Χρησιμοποιώντας

την έξοδο της συσκευής έλαβαν επιταχύνσεις σε τρεις κατευθύνσεις: κατακόρυφη, εμπρός-πίσω και πλάγια κίνηση του κάτω μέρους του ποδιού. Μετά, χρησιμοποίησαν ένα συνδυασμό αυτών των επιταχύνσεων για αυθεντικοποίηση. Με την εφαρμογή δύο διαφορετικών μεθόδων, ιστόγραμμα ομοιότητας και μήκος κύκλου (histogram similarity και cycle length) πέτυχαν ποσοστά EER 5% και 9%, αντίστοιχα.

Ο Derawi et al. [58] σύλλεξε δεδομένα από μια εμπορικά διαθέσιμη κινητή συσκευή που περιείχε ενσωματωμένο επιταχυνσιόμετρο. Η κινητή συσκευή είχε τοποθετηθεί στο ισχίο κάθε εθελοντή για τη συλλογή δεδομένων βάδισης. Η απόδοση του συστήματος αξιολογήθηκε με 51 εθελοντές απέδωσε σε EER 20%.

Ο Kwapisz et al. [68] δημοσίευσε ένα σύστημα για την αυθεντικοποίηση των χρηστών βασιζόμενος σε δεδομένα επιταχυνσιόμετρου. Χρησιμοποίησαν δεδομένα από 36 χρήστες με δραστηριότητες όπως το περπάτημα, το τρέξιμο και το ανεβοκατέβασμα σε σκαλοπάτια και αυτές τις δραστηριότητες τους δώσανε κάποια συγκεκριμένη ετικέτα. Για εξαγωγή χαρακτηριστικών γνωρισμάτων χώρισαν τους 3 άξονες από το επιταχυνσιόμετρο σε χρονικά παράθυρα των 10-δευτερόλεπτων και για κάθε παράθυρο από αυτά εξήγαγαν χαρακτηριστικά όπως μέση τιμή, τυπική απόκλιση και δυαδική διανομή. Για την ταυτοποίηση, οι συγγραφείς εκτέλεσαν μια ταξινόμηση 36 τάξεων ενώ για την αυθεντικοποίηση οι συγγραφείς μείωσαν το πρόβλημα σε ένα πρόβλημα 2 τάξεων. Πέτυχαν μια ακρίβεια ταξινόμησης 72.2% για τα χρονικά παράθυρα των 10 δευτερολέπτων. Ενώ κατέληξαν στο συμπέρασμα βάσει των αποτελεσμάτων τους πως δεν είναι κρίσιμο να γνωρίζουμε ποια δραστηριότητα εκτελεί ο χρήστης ωστόσο τα δεδομένα τους δημιουργήθηκαν από χρήστες που επαναλάμβαναν ένα περιορισμένο σύνολο από προκαθορισμένες δραστηριότητες.

Ο Feng et al [69] εκμεταλλεύτηκε τα δεδομένα κίνησης των κινητών με ένα καινοτόμο τρόπο και τα αποτελέσματα των πειραμάτων αυτών έδειξαν ότι οι κινήσεις των χρηστών (π.χ. περπάτημα) έχουν υψηλό αντίκτυπο στην αυθεντικοποίηση. Χρησιμοποιώντας 31 χρήστες στο πείραμα τους πέτυχαν EER 6.13%.

Method	Works	Platform	Classification	Performance (%)				
				FAR	TAR	Accuracy	FRR	EER
Walking gait	[59] in 2005	Portable devices	correlation, frequency domain and data distribution statistics					7%
	[58] in 2012	smartphone	statistical					20%
	[68] in 2010	smartphone	Correlation, frequency domain and data distribution statistics			72.2%		
	[62] in 2012	smartphone	Dynamic Time Warping (DTW), Support Vector Machine (SVM)			92.7%		
	[63] in 2013	smartphone	Dynamic Time Warping (DTW), Gaussian Dynamic Time Warp (GDTW)			63.18%		
	[61] in 2011	smartphone	Hidden Markov Models					
	[60] in 2012	smartphone	spectrogram analysis	0.1%		99.4%		
	[64] in 2015	smartphone	Gait Dynamic Images (GDIs)					3.88%
	[65] in 2017	smartphone	statistical					13%
	[66] in 2002		statistical			49%		
	[67] in 2006	smartphone	histogram similarity and cycle length					5%
	[69] in 2013	smartphone	Statistic Method and the Trajectory Reconstruction Method					6.13%

Πίνακας 2: Σύνοψη των Walking gait μεθόδων

3.4 *Χειρονομίες επί της οθόνης αφής (Touch gestures)*

Αυτή η προσέγγιση καταγράφει τον μοναδικό τρόπο αφής του κάθε χρήστη όπως για παράδειγμα την πίεση των δακτύλων, την τροχιά τους πάνω στην οθόνη αφής, την ταχύτητα και την επιτάχυνση κίνησης του χεριού του χρήστη καθώς αυτός αλληλοεπιδρά με το κινητό [70]. Στο [70] χρησιμοποιώντας ως δείγμα 40 χρήστες πέτυχαν FAR 4.66% και FRR 0.13%.

Ο Saevanee et al [71] διερεύνησε την ενδεχόμενη χρήση τριών συμπεριφορικών βιομετρικών χαρακτηριστικών ως μέρος του συστήματος αυθεντικοποίησης των κινητών συσκευών. Τα συμπεριφορικά βιομετρικά χαρακτηριστικά ήταν ο χρόνος πατήματος της οθόνης, η συμπεριφορά στην οθόνη και η πίεση των δάχτυλων. Τα αποτελέσματα έδειξαν ότι χρησιμοποιώντας μόνο την πίεση των δάχτυλων στην οθόνη μπορεί να αυθεντικοποιήσει τους χρήστες με ποσοστό ακρίβειας

99%, καθώς είναι το ίδιο με το συνδυασμό πατήματος οθόνης σε συνδυασμό με την πίεση των δάχτυλων.

Ο Frank et al. [72], διερεύνησε κατά πόσον ένας ταξινομητής (classifier) μπορεί συνεχώς να αυθεντικοποιεί τους χρήστες με βάση τον τρόπο που αλληλοεπιδρούν με την οθόνη αφής του κινητού τους τηλεφώνου. Πρότεινε 30 χαρακτηριστικά συμπεριφοράς ως προς την αφή, που μπορεί να προέρχονται από raw δεδομένα και απέδειξε ότι οι διαφορετικοί χρήστες αγγίζουν με διαφορετικό τρόπο την οθόνη. Το συγκεκριμένο σύστημα ταξινόμησης μαθαίνει τη συμπεριφορά αφής ενός χρήστη κατά τη διάρκεια της φάσης εγγραφής (enrollment phase) και είναι σε θέση να αποδεχτεί ή να απορρίψει τον τρέχοντα χρήστη, παρακολουθώντας την αλληλεπίδραση του χρήστη με την οθόνη αφής. Ο ταξινομητής επιτυγχάνει ένα ποσοστό διάμεσου (median) σφάλματος 0% για την αυθεντικοποίηση εντός μιας υπάρχουσας συνεδρία, 2% - 3% για την αυθεντικοποίηση μεταξύ συνεδρίων και κάτω του 4%, όταν η δοκιμή αυθεντικοποίησης πραγματοποιήθηκε μία εβδομάδα μετά τη φάση της εγγραφής. Η μέθοδος αυτή προτάθηκε να εφαρμόζεται ως μέσο για να επιμηκυνθεί ο χρόνο κλειδώματος της οθόνης ή ως μέρος ενός πολυτροπικού βιομετρικού συστήματος αυθεντικοποίησης.

Ο Li et al. [73], πρότεινε ένα νέο βιομετρικό σύστημα για την επίτευξη συνεχούς και μη παρατηρήσιμης επαναυθεντικοποίησης για smartphones. Το συγκεκριμένο σύστημα χρησιμοποιεί έναν ταξινομητή για να μάθει τις κινήσεις των δάχτυλων του ιδιοκτήτη και ελέγχει συνεχώς αν οι κινήσεις του τωρινού χρήστη ταυτίζονται με τα πρότυπα κίνησης του ιδιοκτήτη. Το σύστημα αυθεντικοποιεί συνεχώς εκ νέου τον τρέχων χρήστη χωρίς να διακόπτει την χρήση του smartphone. Τα πειράματα έδειξαν ότι το σύστημα αυτό είναι αποτελεσματικό σε smartphones, ενώ πέτυχε επίσης υψηλή ακρίβεια. Η ακρίβεια του για την ολίσθηση επάνω ήταν 95.78%, από την ολίσθηση κάτω 95.30%, από την ολίσθηση αριστερά 93.06%, συρόμενη δεξιά 92.56%, το επάνω κάτω 93.02%, αριστερά και κάτω 88.28%, και δεξιά και κάτω 89.66%.

Ο Zhao et al. [74], πρότεινε ένα σύστημα γραφικού σχεδιασμού αφής (Graphic Touch Gesture Feature-GTGF) για να εξαγάγει τα χαρακτηριστικά της ταυτότητας από τα ίχνη της αφής. Τα ίχνη της κίνησης και η πίεση παρουσιάστηκαν με τιμές πίεσης και σχήματα στην GTGF. Για να αξιολογήσουν τη χρησιμότητά για αυθεντικοποίηση συλλέξαν δεδομένα που περιλάμβαναν τρία σύνολα που χρησιμοποιούνται συνήθως στις χειρονομίες αφής (κίνηση επάνω / κάτω, κίνηση δεξιά / αριστερά, ζουμ in / out). Πέτυχαν ένα EER 2,62% συνδυάζοντας έξι κινήσεις, κάτι που απέδειξε την αποτελεσματικότητα των μεθόδων τους.

Εν συνεχεία, ο Bo et al. [75] έδειξε ότι μπορεί μέσω της οθόνης αφής να επιτρέπεται η εναλλαγή χεριών μεταξύ του ιδιοκτήτη της συσκευής και ενός επισκέπτη που μπορεί ή δεν μπορεί να είναι μια γνωστή οντότητα (entity). Διενεργώντας εκτεταμένες αξιολογήσεις από τις προσεγγίσεις τους, έδειξαν ότι η ακρίβεια της αναγνώρισης χρήστη είναι πάνω από 99%. Ο μηχανισμός τους ήταν σε θέση να προσδιορίσει με επιτυχία το χρήστη με μια κατά μέσο όρο καθυστέρηση 2.26 ενέργειες του χρήστη με ακρίβεια 98%.

Ο Xu et al. [76], βασιζόμενος στην οθόνη αφής, υιοθέτησε ένα μηχανισμό συνεχούς και παθητικού ελέγχου αυθεντικοποίησης. Τα αποτελέσματά τους επαληθεύσαν ότι τα βιομετρικά χαρακτηριστικά αφής μπορεί να χρησιμεύσουν ως μια πολλά υποσχόμενη μέθοδο για την συνεχή και παθητικού ελέγχου αυθεντικοποίηση. Το βιομετρικό τους σύστημά ήταν σε θέση να επιτύχει γενικά τιμές EER κατώτερο του 10% για όλους τους τύπους λειτουργίας. Η λειτουργία slide εκτελούνταν καλύτερα επιτυγχάνοντας EER χαμηλότερο από 1%.

Ο Sitova et al. [77], εισήγαγε μια σειρά από συμπεριφορικά χαρακτηριστικά για συνεχή αυθεντικοποίηση στους χρήστες smartphone, όπως την κίνηση του χεριού, τον προσανατολισμό και τον τρόπο πιασίματος (Hand Movement, Orientation, and Grasp - HMOG). Τα HMOG διακριτικά συλλαμβάνουν μικροκινήσεις του χρήστη και τον προσανατολισμό που προκύπτουν από το πώς ένας χρήστης κρατάει, αρπάζει και αφήνει το smartphone. Συγκεντρώθηκαν στοιχεία υπό δύο προϋποθέσεις: όταν ο χρήστης κάθεται και όταν περπατάει. Πέτυχαν EER αυθεντικοποίησης τόσο χαμηλά όσο 7,16% (περπάτημα) και 10.05% (κάθεται), όταν συνδύασαν τις HMOG, μικροκινήσεις του χρήστη και τις λειτουργίες πληκτρολόγησης.

Ο Buriro et al. [78], πρότεινε ένα μηχανισμό που κατασκευάζει προφίλ χρήστη βάσει του πώς αυτός κρατά το τηλέφωνο και λαμβάνοντας υπόψη του, τις μικροκινήσεις του τηλεφώνου και τις κινήσεις των δακτύλων του χρήστη κατά τη διάρκεια της γραφής ή της υπογραφής στην οθόνη αφής. Πιο συγκεκριμένα, ο μηχανισμός βασίζεται στα χαρακτηριστικά σημεία που πατιούνται στην οθόνη αφής, και όχι από την εικόνα που παράγεται. Αυτά υλοποιήθηκαν και αξιολογήθηκαν σε εμπορικά διαθέσιμα smartphones. Πέτυχαν ποσοστό 95% πραγματικής αποδοχής (True Acceptance Rate - TAR) με 3.1% False Acceptance Rate (FAR) σε δείγμα 30 εθελοντών.

Ο SEO et al. [79], προτείνουν μια ειδικά σχεδιασμένη βιομετρική μέτρηση αυθεντικοποίησης για κινητές συσκευές, αναλύοντας τα μοτίβα εισόδου του χρήστη, όπως τη διάρκεια αφής του δαχτύλου, το επίπεδο πίεσης και το πλάτος του δαχτύλου στην οθόνη αφής. Συνέλεξαν τα μοτίβο εισόδου διαφόρων ατόμων για να τεστάρουν εμπειρικά την μέθοδος τους. Τα αποτελέσματα έδειξαν ότι η μέθοδος αυτή εντοπίζει αποτελεσματικά τους χρήστες με ποσοστό ακριβείας κοντά στο 99.7%.

Ο Shen et al. [80], διερευνήσαν την σκοπιμότητα και τη δυνατότητα εφαρμογής των αισθητήρων κίνηση για χρήση για τον έλεγχο σε smartphones. Τα δεδομένα από αισθητήρες κίνησης αναλύθηκαν σε βάθος, ώστε να εντοπιστούν οι ενέργειες που έκανε ο χρήστης κατά τη διάρκεια εισαγωγής του κωδικού πρόσβασης. Τα αποτελέσματά τους πέτυχαν ποσοστό FRR 6,85% και FAR 5,01%.

Ο De Luca et al. [81], εισήγαγαν μια προσέγγιση αυθεντικοποίησης όπου οι χρήστες δεν ελέγχονται μόνο από το σχήμα του μοτίβο εισόδου τους αλλά επίσης και από τον τρόπο που το κάνουν. Χρησιμοποιώντας dynamic time warping (DTW) για την ανάλυσή τους, απέδειξαν ότι είναι δυνατό να διακρίνεις τους διαφορετικούς χρήστες και να χρησιμοποιηθούν αυτές οι πληροφορίες για να αυξηθεί η ασφάλεια διατηρώντας παράλληλα την φιλικότητα στον χρήστη. Η ακρίβεια προσέγγισης αυτής ήταν 77% με FRR 19% και FAR 21%.

Method	Works	Platform	Classification	Performance (%)				
				FAR	TAR	Accuracy	FRR	EER
Touch gestures	[70] in 2012	smartphone	FAST (Fingergestures Authentication System using Touchscreen)	4.66%			0.13%	
	[71] in 2008	smartphone	k-NN			99%		
	[72] in 2012	smartphone	statistical					<4%
	[73] in 2013	smartphone	SVM			>88.28%		
	[74] in 2013	smartphone	Graphic Touch Gesture Feature (GTGF)					2.62%
	[75] in 2014	smartphone	SVM			99%		
	[76] in 2014	smartphone	Support Vector Machine (SVM)					<10%
	[77] in 2016	smartphone	Hand Movement, Orientation, and Grasp - HMOG					<10.05%
	[78] in 2016	smartphone	Multilayer Perceptron (MLP)	3.1%	95%			
	[79] in 2012	smartphone	Back Propagation Neural network (BPN)			99.7%		
	[80] in 2016	smartphone	SVM	5.01%			6.85%	
	[81] in 2012	smartphone	Dynamic time warping (DTW)	21%		77%	19%	

Πίνακας 3: Σύνοψη των touch gestures μεθόδων

3.5 *Συμπεριφορικό προφίλ (Behavior-based Profiling)*

Οι τεχνικές behavior profiling (δημιουργίας προφίλ) διενεργούν την αυθεντικοποίηση του χρήστη με βάση την συμπεριφορά του στις εφαρμογές και υπηρεσίες που χρησιμοποιεί. Η έρευνα behavior profiling ξεκίνησε στα τέλη της δεκαετίας του 90 κυρίως για την ανάπτυξη συστημάτων ανίχνευσης εισβολών (Intrusion Detection System - IDS) για να ανιχνεύουν απάτες παρακολουθώντας τη συμπεριφορά του χρήστη κατά την διάρκεια των κλήσεων [82], [83], [84]. Σε αυτά τα συστήματα, το προφίλ του χρήστη δημιουργείται από την παρακολούθηση των δραστηριοτήτων του για ένα χρονικό διάστημα και συγκρίνεται με το τρέχον προφίλ του. Όταν παρατηρείται σημαντική απόκλιση, ανιχνεύεται πιθανή παρείσφρηση.

Πρόσφατα, μια σειρά από διαφορετικές τεχνικές έχουν αναπτυχθεί στη βιβλιογραφία που εστιάζουν στη χρήση τέτοιων μεθόδων για συνεχή αυθεντικοποίηση [85], [86], [87]. Σε αυτές τις μεθόδους, το επίπεδο εφαρμογής καθώς και συγκεκριμένα χαρακτηριστικά της εφαρμογής όπως το αναγνωριστικό κυψέλης (cell ID), η ημερομηνία, η ώρα και ο αριθμός κλήσης, η διάρκεια της κλήσης, το όνομα και χρόνο χρήσης της εφαρμογής χρησιμοποιούνται για να παρακολουθούν συνεχώς την ταυτότητα του χρήστη. Για παράδειγμα, ένα EER 5,4%, 2,2% και 13,5% έχουν αναφερθεί στο [85] για την τηλεφωνία, την αποστολή μηνυμάτων κειμένου και για την γενική χρήση της εφαρμογής, το ίδιο και για το dataset του MIT [88]. Ιστορικά δεδομένα χρήσης της εφαρμογής έχουν επίσης χρησιμοποιηθεί για την συνεχή αυθεντικοποίηση των χρηστών κινητής τηλεφωνίας. Το [86] ανέπτυξε μια τεχνική που βασίζεται σε ιστορικά δεδομένα χρήσης που κατάφεραν ένα EER 9,8%. Πρόσφατα μια μέθοδος behavior profiling που εστιάζει στο τι, πού, πότε και πώς χρησιμοποιήθηκαν οι κινητές συσκευές αναπτύχθηκε στο [87]. Στο [89] προτάθηκε μια μέθοδος για συνεχή έλεγχο αυθεντικοποίησης που βασίζεται στην αυξανόμενη εκπαίδευση του συστήματος.

Επιπλέον, μέθοδος behavior profiling που βασίζεται στην χρήση εφαρμογών, bluetooth και Wi-Fi παρουσιάστηκε στο [90]. Στη συγκεκριμένη μέθοδο αναφέρθηκαν ποσοστά 80% 77%, 93% και 85% των μέσων αναγνώρισης όταν χρησιμοποιούνταν εφαρμογές, Bluetooth, Wi-Fi, καθώς και ο συνδυασμός των τριών αυτών συμπεριφορικών χαρακτηριστικών, αντίστοιχα.

Οι μελέτες σχετικά με την πατρότητα των εγγράφων έχουν διεξαχθεί ακολουθώντας την παραδοχή ότι οι άνθρωποι έχουν ένα χαρακτηριστικό μοτίβο της χρήσης της γλώσσας, ένα είδος «δακτυλικών αποτυπωμάτων συγγραφέα» που μπορούν να ανιχνευθούν στα γραπτά τους. Οι πρώτες προσπάθειες να ποσοτικοποιηθεί το στυλ γραφής πηγαίνει πίσω στο 19ου αιώνα με την πρωτοποριακή μελέτη του Mendenhall [91] σε έργα του Σαίξπηρ. Η πιο δημιουργική δουλειά στον τομέα αυτό πραγματοποιήθηκε από τους Mosteller και Wallace [92]. Η έρευνα τους μελέτησε την πατρότητα των εγγράφων The Federalist Papers. Χρησιμοποίησαν μια μέθοδο που βασίζεται στην Bayesian στατιστική ανάλυση των συχνοτήτων από ένα μικρό σύνολο από κοινές λέξεις (δηλαδή «και», «να» κλπ.) ώστε να γίνουν διακρίσεις μεταξύ των υποψηφίων συγγραφέων. Τα αποτελέσματα έδειξαν ότι 12 από τα συζητημένα έγγραφα γράφτηκαν από τον Madison. Το συμπέρασμα αυτό έγινε δεκτό από τους ιστορικούς μελετητές και αποτέλεσε στη συνέχεια ορόσημο σε αυτόν τον τομέα έρευνας. Την τελευταία δεκαετία, η έρευνα στον τομέα αυτό έχει προχωρήσει, καθώς εκμεταλλεύεται την state-of-the-art έρευνα σε τομείς όπως η μηχανική μάθηση, η ανάκτηση πληροφοριών και η επεξεργασία της φυσικής γλώσσας. Με την πληθώρα των διαθέσιμων ηλεκτρονικών κειμένων (π.χ. μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα σε φόρουμ και blog), η τεχνική αυτή έχει μελετηθεί ευρέως.

Στην έρευνα τους οι De Vel et al [93] μελέτησαν την ικανότητα να γίνονται διακρίσεις μεταξύ των συγγραφέων από το θέμα των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Το corpus εγγράφων ηλεκτρονικού ταχυδρομείου που χρησιμοποιήθηκε στο πείραμα περιείχε συνολικά 156 έγγραφα που προέρχονται από τρεις συγγραφείς με μητρική γλώσσα την αγγλική, με κάθε συγγραφέα να συμβάλλει στα emails με τρία θέματα (περίπου 12.000 λέξεις ανά συντάκτη για όλα τα θέματα). Τα θέματα που επιλέγονταν ήταν ταινίες, τρόφιμα και ταξίδια. Το σώμα του κάθε εγγράφου του ηλεκτρονικού ταχυδρομείου αναλύθηκε με βάση μια γραμματική για το ηλεκτρονικό ταχυδρομείο που είχε προταθεί από τους συντάκτες και εξήχθησαν τα χαρακτηριστικά του σώματος του email. Το σώμα ήταν προεπεξεργασμένο για να αφαιρεθούν οποιουδήποτε είδους χαιρετισμοί, στάνταρ κείμενο απαντήσεων και οι υπογραφές. Τα συνημμένα αποκλείονταν και μόνο το ίδιο το σώμα του ηλεκτρονικού ταχυδρομείου χρησιμοποιούνταν. Συνολικά 170 χαρακτηριστικά δείκτη (markers) χρησιμοποιήθηκαν (δηλαδή μέσο μήκος πρότασης, μέσος όρος μήκους λέξεων, ο αριθμό των κενών γραμμών κλπ.) και 21 διαρθρωτικά (structural) χαρακτηριστικά (δηλαδή αν έχει μια επιβεβαίωση χαιρετισμού, αριθμός συνημμένων, αν περιέχουν κείμενο της υπογραφής) εξήχθησαν από κάθε μήνυμα ηλεκτρονικού ταχυδρομείου και το έγγραφο στη συνέχεια αναλύθηκε χρησιμοποιώντας έναν ταξινομητή Support Vector Machines (SVM). Τα αποτελέσματα έδειξαν ότι μια τάξη SVM σε συνδυασμό με τα χαρακτηριστικά markers και structural είναι σε θέση να διακρίνουν τους συντάκτες ανεξαρτήτως θέματος ακόμα και όταν χρησιμοποιούνται πολλαπλές κατηγορίες θεμάτων. Επιπλέον, παρατήρησαν ότι οι δείκτες του στυλ (style markers) είναι τα δεσπόζοντα χαρακτηριστικά που συμβάλλουν στην απόδοση της ταξινόμησης σε σχέση με τα διαρθρωτικά χαρακτηριστικά. Εξετάσθηκε επίσης η απόδοση των λέξεων λειτουργίας (function). Σε αυτό το πείραμα, δημιουργήθηκαν συνολικά 320 function λέξεις και το σύνολο αυτών των δυνατοτήτων χωρίστηκαν σε δύο κατηγορίες: λέξεις μέρη του λόγου (parts-of-speech, POS) και λοιπές. Παράδειγμα λέξεων POS περιλαμβάνουν τα επιρρήματα, τα βοηθητικά ρήματα, οι προθέσεις κλπ. Τα αποτελέσματα αυτού του πειράματος έδειξαν ότι δεν υπήρχε καμία βελτίωση στην απόδοση ταξινόμησης όταν συμπεριλαμβάνονται συνδυασμοί λέξεων και συνακόλουθα παρατηρήθηκε μια μείωση στην απόδοση, όταν η απόσταση των λέξεων function αυξανόταν.

Οι Koppel και Schler [94] πρότειναν τη χρήση των πληροφορίων σύνταξης τόσο από μόνες τους όσο και σε συνδυασμό με άλλα είδη χαρακτηριστικών για αναγνώριση πατρότητας. Το corpus που χρησιμοποιήθηκε σε αυτό το πείραμα αποτελούνταν από 480 μηνύματα ηλεκτρονικού ταχυδρομείου γραμμένα από 11 διαφορετικούς συγγραφείς κατά τη διάρκεια περίπου ενός χρόνου. Τρεις τάξεις των χαρακτηριστικών γνωρισμάτων, συμπεριλαμβανομένων των λεκτικών Part-of-Speech (POS) (δηλαδή λειτουργία των λέξεων: «η», «και», «που»), ετικέτες (δηλαδή ουσιαστικά, ρήματα) και η ιδιοσυγκρασιακή (idiosyncratic) χρήση (δηλαδή το συντακτικό, η μορφοποίηση και ο ορθογραφικός έλεγχος) χρησιμοποιήθηκαν. Ένα τυποποιημένο σύνολο 480 λέξεων λειτουργίας (function) χρησιμοποιήθηκε για να δημιουργηθεί ένα λεκτικό σύνολο. Ένα σύνολο 99 ορθογραφικών λαθών (π.χ. παραλείψεις σε επιστολή και εισαγωγές) και σφάλματα μορφοποίησης (π.χ. πολλά ερωτηματικά και άλλα σημεία στίξης) ορίστηκαν χρησιμοποιώντας ένα εμπορικό ορθογράφο. Ατομικοί συνδυασμοί αλλά και συνδυασμοί διάφορων χαρακτηριστικών τύπων αναλύθηκαν με χρήση αλγορίθμων ταξινόμησης με δέντρα (C4.5 classification algorithms). Τα πειραματικά αποτελέσματα έδειξαν ότι ο συνδυασμός των τριών τύπων χαρακτηριστικών είναι καλύτερος από ό,τι όταν είχαμε χρήση ενός μοναδικού χαρακτηριστικού ή οποιαδήποτε άλλου συνδυασμού.

Ο Gamon [95] απέδειξε ότι ένας συνδυασμός των χαρακτηριστικών βάσει απλής γλωσσολογικής ανάλυσης (π.χ. συχνότητα των λέξεων λειτουργίας) και ενός συνόλου από χαρακτηριστικά με βαθύτερη γλωσσική ανάλυση (συχνότητες παραγωγής κειμένου και χαρακτηριστικά που προέρχονται από σημασιολογικά γραφήματα) παράγουν πολύ υψηλής ακρίβειας αποτελέσματα ακόμη και σε ένα τυχαίο σύντομο κείμενο. Το πείραμα έγινε με βάση 1441 έγγραφα κειμένου από τρεις συντάκτες. Τα πειραματικά αποτελέσματα έδειξαν ότι τα σημασιολογικά χαρακτηριστικά που αποτελούν την πιο αφηρημένη και γλωσσολογικά εξελιγμένη τάξη σε συνδυασμό με τις λεξιλογικές και συντακτικές πληροφορίες βελτίωσαν την ακρίβεια ταξινόμησης.

Ο Zheng et al [29] πρότεινε ένα πλαίσιο αναγνώρισης πατρότητας σε online μηνύματα. Στο πλαίσιο αυτό, τέσσερα χαρακτηριστικά είδη γραφής - ύφους (λεξιλογικά, συντακτικά, δομής, και περιεχομένου - lexical, syntactic, structural, και content-specific features) εξήχθησαν και ένας αλγόριθμος επαγωγικής μάθησης χρησιμοποιήθηκε για την αναγνώριση των online μηνυμάτων. Η δύναμη διαχωρισμού (discriminating) από τους τέσσερις τύπους των χαρακτηριστικών και των τριών τεχνικών ταξινόμησης συγκρίθηκαν: δένδρα αποφάσεων (C4.5), οπίσθιας διάδοσης νευρωνικά δίκτυα και support vector machines (SVM). Πράγματι, τα χαρακτηριστικά διάρθρωσης και τα χαρακτηριστικά συγκεκριμένου περιεχόμενου έδειξαν ιδιαίτερες δυνατότητες για αναγνώριση του δημιουργού του online μηνύματος. Επιπλέον, ο συνδυασμός νευρωνικών δικτύων και SVM ξεπέρασε το συνδυασμό C4.5 και νευρωνικών δικτύων σημαντικά για το έργο της ταυτοποίηση του συγγραφέα. Ωστόσο, διαφορετικές ρυθμίσεις των παραμέτρων (δηλαδή αριθμός συντακτών, αριθμός κατάρτισης και data για τις δοκιμές) των δημιουργών αναγνώρισης είχε αντίκτυπο στις επιδόσεις.

Έρευνα από τον Halteren [28] εξέτασε το γλωσσικό προφίλ για τη διάκριση μεταξύ κειμένων γραμμένων από διαφορετικούς συντάκτες. Το πείραμα έδειξε ότι τα λεξιλογικά χαρακτηριστικά βοηθούν περισσότερο από τα συντακτικά χαρακτηριστικά για να επιλεχθεί ο σωστός συγγραφέας κατά 93% και 86% αντίστοιχα. Επιπλέον, ένα σύστημα προφίλ χρησιμοποιώντας συνδυασμό από λεξιλογικά και συντακτικά χαρακτηριστικά επέλεγε το σωστό συγγραφέα με 97% ακρίβεια. Ήταν επίσης σε θέση να εκτελέσει την εργασία επαλήθευσης με τρόπο που δεν απέρριπτε κείμενα που πρέπει να γίνουν αποδεκτά και αποδεχόταν μόνο το 8,1% των κειμένων που έπρεπε να απορριφθούν. Ως αποτέλεσμα, η μελέτη υπογράμμισε ότι το γλωσσικό προφίλ μπορεί να χρησιμοποιηθεί και για αναγνώριση πατρότητας κειμένου αλλά και για αυθεντικοποίηση.

Έρευνα από τον Mohan et al [96] διερεύνησε μια προσέγγιση με βάση το N-gram για τον προσδιορισμό της πατρότητας μηνυμάτων SMS. Η μελέτη χρησιμοποίησε ένα corpus SMS που τους παρείχε το National University of Singapore. Το τελικό σύνολο δεδομένων του SMS αποτελούνταν από ένα σύνολο 1400 μηνυμάτων από 28 συγγραφείς. Ερευνήθηκε η ποικιλία των N-grams (μεταξύ 1 και 5). Χρησιμοποιήθηκαν μια σειρά από τεχνικές ταξινόμησης, όπως η Ευκλείδεια απόσταση, η απόσταση των μπλοκ κλπ. Ο καταλογισμός πατρότητας των SMS χρησιμοποιώντας προσέγγιση N-grams αποκάλυψε θετικά αποτελέσματα, επιτυγχάνοντας ακρίβεια 72%.

Έρευνα του Goodman et al [97] μελέτησε τη χρήση του stylometry για εύρεση του συντάκτη ηλεκτρονικού ταχυδρομείου. Stylometry είναι η μελέτη του μοναδικού στυλ της γλωσσικής συμπεριφοράς και της γραφής των ατόμων προκειμένου να καθοριστεί η πατρότητα. Το πείραμα βασίστηκε σε 596 μηνύματα ηλεκτρονικού ταχυδρομείου από 134 χρήστες. Για κάθε μήνυμα

ηλεκτρονικού ταχυδρομείου, συνολικά 66 stylometric χαρακτηριστικά είχαν εξαχθεί όπως ο αριθμός των προτάσεων ανά παράγραφο, ο μέσος όρος μήκους λέξεων, ο αριθμός των λέξεων και ο μέσος αριθμός των λέξεων ανά παράγραφο. Βάσει είκοσι μηνυμάτων ηλεκτρονικού ταχυδρομείου δοκιμής, τα πειραματικά αποτελέσματα έδειξαν ότι τα μηνύματα ηλεκτρονικού ταχυδρομείου προσδιορίστηκαν σωστά κατά 80%.

Ο Castro et al [98] διερεύνησε τη χρήση του τρόπου πληκτρολόγησης (keystroke dynamics) και τα στιλιστικά χαρακτηριστικά με σκοπό τον έλεγχο ταυτότητας σε online εξεταζόμενους. Η μελέτη χρησιμοποίησε χαρακτηριστικά χρόνου για πληκτρολόγηση και 55 λεκτικά (49 από χαρακτηριστικά γνωρίσματα χαρακτήρα και 6 από δυνατότητες του Word) χαρακτηριστικά που εξήχθησαν από έγγραφα εξετάσεων. Το πείραμα χρησιμοποίησε ένα dataset που περιέχει 15 φοιτητές και κάθε μαθητής απάντησε σε 8 ερωτήσεις. Τα μεγέθη του δείγματος ήταν μεταξύ 1.710 και 70.300 χαρακτήρων. Η αξιολόγηση του πειράματος πραγματοποιήθηκε χρησιμοποιώντας ένα K-Nearest Neighbour (KNN) ταξινομητή. Τα αποτελέσματα έδειξαν ότι με την χρήση ενός συνδυασμού πλήκτρων και γλωσσικών χαρακτηριστικών επιτυγχάνεται ένα καλό επίπεδο απόδοσης 85-94%.

Ο Iqbal et al [99] μελέτησε την πατρότητα ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας τέσσερις τύπους γλωσσικών χαρακτηριστικών: λεκτικά, συντακτικά, δομικά και συγκεκριμένου τομέα . Συνολικά 419 διαφορετικά χαρακτηριστικά εξήχθησαν από κάθε μήνυμα ηλεκτρονικού ταχυδρομείου. Η μελέτη απασχόλησε 5 συντάκτες από το dataset Enron. Για κάθε συγγραφέα, επιλέχθηκαν 40 μηνύματα ηλεκτρονικού ταχυδρομείου. Το πείραμα αξιολογήθηκε με τη χρήση τριών αλγορίθμων ομαδοποίησης: Expectation Maximization, k-means και bisecting k-means. Τα αποτελέσματα έδειξαν μια καλή ορθή κατάταξη απόδοση με ακρίβεια από 77,6% έως 82.9% .

Οι Ouamour και Sayoud [100] διερεύνησαν την αναγνώριση πατρότητας σε αραβικά κείμενα. Τα αποτελέσματα έδειξαν μια καλή ακρίβεια 80%, χρησιμοποιώντας μία από τις ακόλουθες τρεις δυνατότητες: character bigram, character trigram και rare words. Επιπλέον, αυτή η μελέτη έδειξε ότι το γλωσσικό προφίλ για απόδοση πατρότητας μπορεί επίσης να εφαρμοστεί στην αραβική γλώσσα, χρησιμοποιώντας τον ίδιο κανόνα που χρησιμοποιείται και στη αγγλική γλώσσα.

Η έρευνα στα κινητά για το Behavioural Profiling (σκιαγράφηση συμπεριφοράς) ξεκίνησε περίπου το 1995, εστιάζοντας στην περιοχή των συστημάτων ανίχνευσης εισβολών (Intrusion Detection Systems - IDSs) για την ανίχνευση απάτης σε υπηρεσίες τηλεφωνίας. Αυτά τα IDS δημιουργούσαν ένα κανονικό προφίλ του χρήστη με την παρακολούθηση των δραστηριοτήτων των χρηστών για ένα χρονικό διάστημα και το συνέκριναν έναντι της τρέχουσας δραστηριότητας. Όταν παρατηρείται σημαντική απόκλιση, ανιχνεύεται πιθανή παρείσφρηση.

Εντός του χώρου της ανίχνευσης απάτης, μία από τις πιο σημαντικές αρχικές μελέτες την ανέλαβε η European Advanced Security for Personal Communications (ASPeCT) (Gosset, 1998), η οποία επιδίωξε να αναπτύξει ένα σύστημα ανίχνευσης απάτης για τις επικοινωνίες των κινητών. Τα πειραματικά αποτελέσματα έδειξαν ένα ποσοστό ανίχνευσης του 50% και FAR 0,02%.

Έρευνα του Boukerche και Nitare [101] προτείνει ένα online μοντέλο εντοπισμού απάτης για το κινητό τηλέφωνο με την χρήση Radial Basis Function (RBF) neural network (νευρωνικών δικτύων). Το μοντέλο είναι σε θέση να εντοπίσει πιθανή κλήση υπηρεσίας απάτης χρησιμοποιώντας τα χαρακτηριστικά του χρήστη. Μόλις εντοπιστεί μια πιθανή απάτη, το μοντέλο στέλνει αυτόματα ειδοποιήσεις τόσο στους μεμονωμένους χρήστες όσο και στους διαχειριστές του δικτύου.Το dataset

του πειράματος περιέχει 4,255,973 τηλεφωνικές κλήσεις που συλλέχθηκαν από ένα ανώνυμο τηλεπικοινωνιακό φορέα παροχής υπηρεσιών. Το αποτέλεσμα έδειξε EER 4,2%.

Ο Sun et al [102] πρότεινε ένα πρότυπο ανίχνευσης που βασίζεται στην ανίχνευση ανωμαλίας για κυψελοειδή δίκτυα κινητής αξιοποιώντας διάφορους αλγορίθμους (Exponentially Weighted Moving Model – EWMA, Markov model, Ziv- Lempel data compression algorithm κλπ.). Τα ποσοστά FAR ήταν περίπου 25% και 5% και τα ποσοστά ανίχνευσης ήταν περίπου 80% και 95%, όταν ένας χρήστης ταξιδεύει με ταχύτητα 20 μιλίων / ώρα και 60 μιλίων / ώρα αντίστοιχα. Ωστόσο, αυτό το σύστημα δεν μπορεί να είναι ακριβές όσον αφορά ορισμένα ιδιαίτερα είδη χρηστών οι οποίοι δεν παρουσιάζουν κανονική κίνηση όπως ο οδηγός ταξί.

Έρευνα από τον Li et al [85] εξέτασε την ικανότητα να ταξινομούν τους χρήστες με βάση τον τρόπο που χρησιμοποιούν υπηρεσίες και εφαρμογές σε ένα κινητό τηλέφωνο. Η έρευνα χρησιμοποίησε ένα δημόσια διαθέσιμο dataset, το MIT Reality Mining project. Το dataset περιέχει διάφορα δεδομένα κινητής τηλεφωνίας που συλλέχθηκαν από συμμετέχοντες που χρησιμοποιούσαν κινητά τηλέφωνα Nokia 6600. Αναλύθηκαν τα παρακάτω πειράματα: της γενικής χρήσης της εφαρμογής και της ειδικής χρήσης από εφαρμογές φωνής και κειμένου. Δύο τύποι προφίλ χρησιμοποιήθηκαν: στατική και δυναμική. Για την στατική ανάλυση χαρακτηριστικών, κάθε επιμέρους dataset ήταν χωρισμένο σε δύο σύνολα: το πρώτο μισό χρησιμοποιήθηκε για τη δημιουργία του προφίλ και το δεύτερο μισό είχε χρησιμοποιηθεί για τη δοκιμή. Το δυναμικό προφίλ περιέχει δραστηριότητα του χρήστη 7/10/14 ημερών. Μια σειρά από αναλύσεις πραγματοποιήθηκαν μέσω Feed Forward Multi-Layered Perceptron network (FF MLPs) και Radial basis function network (RBF) με διαφορετικές διαμορφώσεις.

Για το πείραμα της γενικής εφαρμογής, το dataset περιέχει συνολικά 101 μεμονωμένων εφαρμογών με 30428 δεδομένα εισόδου για 76 συμμετέχοντες. Ανάμεσα σε αυτές τις 101, τα ακόλουθα χαρακτηριστικά έχουν εξαχθεί από το dataset: όνομα εφαρμογής, ημερομηνία έναρξης και η θέση του χρήση. Τα αποτελέσματα έδειξαν το καλύτερο EER που ήταν 13,5% και έχει ληφθεί με τη χρήση δυναμικών δεδομένων προφίλ με 14 ημέρες δραστηριότητας του χρήστη με 6 καταχωρήσεις του αρχείου καταγραφής.

Για το πείραμα εφαρμογή τηλεφωνικών κλήσεων, το dataset περιέχει συνολικά 13719 κλήσεων με 2.317 μοναδικούς τηλεφωνικούς αριθμούς από 71 συμμετέχοντες. Για κάθε αρχείο καταγραφής, αποσπάστηκαν τα ακόλουθα χαρακτηριστικά γνωρίσματα: τηλεφωνικός αριθμός, η ημερομηνία και η τοποθεσία της κλήσης. Το καλύτερο πειραματικό αποτέλεσμα είναι ένα EER 5,4% και έχει ληφθεί με τη χρήση δυναμικών δεδομένων προφίλ με 14 ημέρες δραστηριότητας του χρήστη με 6 καταχωρήσεις του αρχείου καταγραφής.

Για το πείραμα μηνυμάτων, το dataset περιέχει 1382 αρχεία και 258 μοναδικούς τηλεφωνικούς αριθμούς. Για κάθε αρχείο καταγραφής, αποσπάστηκαν τα ακόλουθα χαρακτηριστικά γνωρίσματα: ο αριθμός τηλεφώνου του παραλήπτη, η ημερομηνία και η τοποθεσία του χρήστη. Το καλύτερο πειραματικό αποτέλεσμα είναι ένα EER 2.2% και έχει ληφθεί με τη χρήση δυναμικών δεδομένων προφίλ με 14 ημέρες δραστηριότητας του χρήστη με 3 καταχωρήσεις του αρχείου καταγραφής.

Το όνομα της εφαρμογής και η θέση αποδείχθηκαν πολύτιμα χαρακτηριστικά που παρέχουν επαρκή διακρίσεις για τους χρήστες να είναι χρήσιμες για την αυθεντικοποίηση, με την θέση να είναι το πιο σημαντικό χαρακτηριστικό. Σε γενικές γραμμές, στο δυναμικό προφίλ επιτυγχανόταν μια ελαφρώς

καλύτερη απόδοση από την στατική ανάλυση των χαρακτηριστικών, καθώς περιέχει πιο πρόσφατες δραστηριότητες του χρήστη.

Η Sultana et al. [103] συνδύασε πληροφορίες για συμπεριφορές χρηστών που εξήχθησαν από social media λογαριασμούς και τα συνδύασε με τις παραδοσιακές μεθόδους αποτυπωμάτων και προσώπου για να βελτιώσει την απόδοση των παραδοσιακών βιομετρικών συστημάτων.

Ο Wei-Han Lee et al [104] προτείνει το SmarterYou το οποίο βασίζεται σε συμπεριφορικά βιομετρικά χαρακτηριστικά χρησιμοποιώντας στοιχεία από τους ήδη υπάρχοντες αισθητήρες του κινητού τηλεφώνου. Για να πετύχει την μέγιστη απόδοση χρειάζεται να συνδυαστεί και με κάποια συσκευή που να την φοράει ο χρήστης (π.χ. ένα smartwatch). Στη συγκεκριμένη μέθοδο συλλέγονται και αναλύονται στοιχεία από τους αισθητήρες του κινητού και του smartwatch τα οποία έχουν ακρίβεια αυθεντικοποίησης 98.1% και μόνο 2.4% παραπάνω κατανάλωση μπαταρίας.

Ο Gupta el al. [105], περιγράφουν ένα profiler περιεχομένου όπου χρησιμοποιούνται ίχνη τοποθεσίας για να εντοπιστούν σημεία ενδιαφέροντος για τον χρήστη και να εισαχθούν σε αυτό το προφίλ οι συσκευές Bluetooth και WiFi σε τέτοια μέρη όπου συνδέεται συχνά ο χρήστης. Η ακρίβεια και η αναγνώριση των ασφαλών τοποθεσιών ήταν αρκετά υψηλή. Οι περιπτώσεις λάθους αυθεντικοποίησης στην συγκεκριμένη τεχνική ήταν 15%.

Στο [106] η ανάλυση γλωσσολογικών (linguistic profiling) χαρακτηριστικών χρησιμοποιήθηκε για την αυθεντικοποίηση χρηστών με βάση το λεξιλόγιο που χρησιμοποιούν όταν γράφουν και το ύφος του μηνύματος SMS. Πειραματικά αποτελέσματα σε 30 συμμετέχοντες έδειξαν ότι το linguistic profiling μπορεί να χρησιμοποιηθεί επιτυχώς για αυθεντικοποίηση του χρήστη με χαμηλό EER.

Ο Feng et al [107] πρότεινε μια νέα μέθοδο που βασίζεται στη φωνή. Η φωνή έχει γίνει πολύ δημοφιλής ως κανάλι αλληλεπίδρασης με το χρήστη (User Interaction) καθώς όλα τα σύγχρονα λειτουργικά υποστηρίζουν και προωθούν την συγκεκριμένη μέθοδο. Παραδείγματα αποτελούν οι βοηθοί φωνής (voice assistants) όπως η Siri (IOS), το Google Now (Android) και η Cortana (Windows). Στη συγκεκριμένη έρευνα προτείνετε το VAuth ένα σύστημα που παρέχει CA για τους voice assistants. Εξαιτίας του ότι η φωνή μπορεί εύκολα να υποκλαπεί, ένα τέτοιο σύστημα είναι πολύ χρήσιμο ώστε να γίνει πιο ασφαλής η συγκεκριμένη μέθοδος. Σε αυτή την μέθοδο χρησιμοποιούνται και επιπλέον χαρακτηριστικά όπως πληροφορίες από το επιταχυνσιόμετρο και από κινήσεις του προσώπου, του λαιμού και του στήθους για να βοηθήσουν στη αυθεντικοποίηση του χρήστη.

Method	Works	Platform	Classification	Performance (%)				
				FAR	TAR	Accuracy	FRR	EER
Behavior-based Profiling	[85] in 2011	smartphone						<13.5%
	[86] in 2014	smartphone	Neural Networks					9.8%
	[90] in 2015	smartphone	statistical			>77%		
	[93] in 2001	PC	SVM					
	[94] in 2003	PC	linear SVM and decision trees (C4.5)			72%		
	[95] in 2004	PC	SVM			45.8%		
	[29] in 2005	PC	SVM and decision trees (C4.5)			>70%		
	[28] in 2004	PC	statistical	8.1%		97%		
	[96] in 2010	smartphone	statistical			72%		
	[97] in 2007	PC	Nearest Neighbor classifier, using Euclidean distance			80%		
	[98] in 2011	PC	K-Nearest Neighbour (KNN)			85%		
	[99] in 2010	PC	SVM, Expectation Maximization, k-means και bisecting k-means			77.6%		
	[100] in 2012	PC	Sequential Minimal Optimization, Support Vector Machine (SMO-SVM)			80%		
	[101] in 2002	smartphone	Radial Basis Function (RBF) neural network (NN)					4.2%
	[102] in 2004	smartphone	Exponentially Weighted Moving Average (EWMA), Markov model, Ziv- Lempel data compression algorithm	<25%				
	[104] in 2017	smartphone	statistical			98.1%		
	[105] in 2012	smartphone	statistical	15%				
	[107] in 2017	smartphone	SVM			97.1%		

Πίνακας 4: Σύνοψη των behavior-based profiling μεθόδων

3.6 *Η δυναμική της αφής (Keystroke dynamics)*

Η προκαταρκτική μελέτη που εκπονήθηκε από τους Clarke και Furnell [108] διερεύνησε τη σκοπιμότητα της χρήσης δυναμικής πληκτρολόγησης ως μιας προσέγγισης ελέγχου αυθεντικοποίησης σε κινητές συσκευές. Η μελέτη τους χρησιμοποίησε δύο παραδοσιακά χαρακτηριστικά πληκτρολόγησης, το inter-key time (τον χρόνο μεταξύ δύο διαδοχικών πατημάτων πλήκτρων) και το hold time (ο χρόνος μεταξύ πατήματος και που ο χρήστης ελευθερώνει ένα πλήκτρο). Δύο διαφορετικοί τύποι εισόδου: βασιζόμενοι σε αριθμητικά δεδομένα και σε αλφαβητικά δεδομένα ερευνήθηκαν στα πειράματα. Για τα δύο πειράματα, η συλλογή δεδομένων πραγματοποιήθηκε χρησιμοποιώντας ένα τροποποιημένο κινητό τηλέφωνο (Nokia 5110), διασυνδεδεμένο με έναν επιτραπέζιο υπολογιστή μέσω της σύνδεσης πληκτρολογίου. Οι δοκιμές ταξινόμησης είχαν εκτελεστεί με ένα χρήστη, που ενεργούσε ως έγκυρος εξουσιοδοτημένος χρήστης, ενώ όλοι οι άλλοι χρήστες ενήργησαν ως απατεώνες (μια τυπική και καλά αποδεκτή μεθοδολογία που εφάρμοσαν για keystroke dynamics μελέτες). Μια σειρά από αναλύσεις έγιναν χρησιμοποιώντας ένα Forward Multi-Layered Perceptron network (FF MLPs), ένα Radial basis function network (RBF) και ένα Generalised regression neural network (GRNNs) με διαφορετικές διαμορφώσεις. Το πείραμα αριθμητικής-πληκτρολόγησης αξιοποίησε το inter-key time και εφαρμόστηκε με στατική (εξαρτώμενη από τους αριθμούς) και με δυναμική (ανεξάρτητη από τους αριθμούς) είσοδο. Ένα σύνολο 32 συμμετεχόντων κλήθηκαν να εισάγουν τρία σενάρια εισόδου, συμπεριλαμβανομένου του σταθερού 4-ψήφιου αριθμού (που αντιπροσωπεύει έναν αριθμό τύπου PIN), τον σταθερό 11-ψήφιο αριθμό και μία σειρά από 11-ψήφιο αριθμό (που αντιπροσωπεύει την έναρξη ενός αριθμού τηλεφώνου). Για κάθε σύνολο δεδομένων, 30 δείγματα εισόδου πάρθηκαν από κάθε χρήστη σε μια μεμονωμένη περίοδο λειτουργίας. Τα δύο τρίτα των εισροών αυτών χρησιμοποιήθηκαν στην παραγωγή του προφίλ αναφοράς, με το υπόλοιπο να χρησιμοποιείται ως ένα επικυρωμένο δείγμα. Τα πειραματικά αποτελέσματα έδειξαν ότι οι επιδόσεις κυμαινόταν από ένα EER του 4,9% με την εγγραφή στατικής εισόδου και ένα EER 25,6% με την καταχώρηση δυναμικής εισόδου. Η απόδοση που βασίζεται σε δυναμική τεχνική για έναν αλγόριθμο ταξινόμησης είναι πολύ φτωχότερη από την τεχνική που βασίζεται στη στατική μέθοδο, δεδομένου ότι απαιτεί ένα μεγάλο αριθμό δεδομένων εκπαίδευσης. Η απόδοση ενός μεμονωμένου χρήστη ποικίλει από τις διαφορετικές τεχνικές και διαμορφώσεις ενός νευρωνικού δικτύου (neural network techniques), με ορισμένους χρήστες να εκτελούν καλύτερα το ένα από το άλλο. Αξιοποιώντας τις ξεχωριστές διαμορφώσεις του νευρωνικού δικτύου , η απόδοση βελτιώνεται με EER της τάξης του 8,5% και 4,9%, για τις τετραψήφιες και τις έντεκα ψηφίων αριθμητικές εισροές αντίστοιχα. Παρόλο που αυτές οι μέσες αποδόσεις ήταν πολλά υποσχόμενες, είναι εμφανές ότι η απόδοση πέφτει 35% για ένα συγκεκριμένο χρήστη σε αυτό το πείραμα. Το πείραμα αλφαβητικής-πληκτρολόγησης αξιοποιεί το hold time και εφαρμόστηκε σε στατική καταχώρηση. Σε αυτή τη συγκεκριμένη μελέτη, ο χρόνος κράτησης ορίζεται ως χρόνος που λαμβάνεται από το αρχικό πάτημα πλήκτρου μέχρι το τελικό πάτημα του πλήκτρου (π.χ. το γράμμα «c» απαιτεί το κουμπί με τον αριθμό 2 για να πιεστεί τρεις φορές στα τότε πληκτρολόγια). Συμμετείχαν συνολικά 30 άτομα στη μελέτη, με κάθε συμμετέχοντα να εισάγει 30 μηνύματα κειμένου που χωρίζονται σε τρεις συνεδρίες. Ως αποτέλεσμα, πέντε δίκτυα δημιουργήθηκαν με από δύο ως έξι χαρακτήρες από τα περισσότερο επαναλαμβανόμενους (δηλαδή, e, t, a, o, n, i), με κάθε είσοδο να αντιπροσωπεύει έναν χαρακτήρα. Τα πειραματικά αποτελέσματα έδειξαν ότι κατά μέσο όρο αποδείχθηκε πιο επιτυχημένη μια είσοδο

του φορέα των πέντε χαρακτήρων, επιτυγχάνοντας ένα EER 18%. Την καλύτερη απόδοση του μεμονωμένου χρήστη να επιτυγχάνει ένα EER 7,2%. Ωστόσο, η χειρότερη επίδοση μεμονωμένου χρήστη πέτυχε ένα EER 42,6%.Ο Clarke και Furnell [108] έχουν δείξει την ικανότητα και του inter-keystroke και του hold time για αλγορίθμους ταξινόμησης για να ξεχωρίσει συλλογικά την πλειοψηφία των χρηστών με έναν σχετικά καλό βαθμό ακρίβειας.

Μια περαιτέρω μελέτη από τους Karatzouni και Clarke [109] εξέτασε άλλους τύπους της διασύνδεσης και του τρόπου αφής. Η έρευνα εξέτασε τη δυνατότητα δυναμικής πληκτρολόγησης βάσει πληκτρολόγιων των κινητών τηλεφώνων σχεδιασμένα για γράψιμο με τον αντίχειρα. Η καλύτερη απόδοση ήταν EER 12,2%. Ωστόσο, ένας συγκεκριμένος χρήστης είχε EER 32,4%. Αν και το hold-time εκτελούνταν καλά σε κανονικό κινητό τηλέφωνο με αριθμητικά πληκτρολόγια στην προηγούμενη έρευνα (Clarke και Furnell, [108]), αυτό το χαρακτηριστικό δεν έδωσε καμία υπόσχεση για μια πιθανή χρήση σε πληκτρολόγια αντίχειρα. Αυτό ήταν επειδή η μέθοδος υπολογισμού του hold-time ήταν διαφορετική. Επιπλέον, η έρευνα διαπίστωσε ότι η διεπαφή αφής του πληκτρολογίου και οι κινήσεις των χεριών μπορούν επίσης να επηρεάσουν το χρόνο της πληκτρολόγησης.

Σε έρευνα του Maiorana et al [110] διερευνάται η δυνατότητα keystroke dynamics για την παροχή ενός συστήματος αυθεντικοποίησης σε κινητά τηλέφωνα. Μια βάση δεδομένων που αποτελείται από έξι κωδικούς πρόσβασης, καθένας μήκους δέκα αλφαβητικών γραμμάτων. Συνολικά σε 40 χρήστες ζητήθηκε να εισάγουν κάθε κωδικό 20 φορές χρησιμοποιώντας ένα κινητό τηλέφωνο Nokia 6680 σε τέσσερις ξεχωριστές συνεδρίες. Βάσει 4800 εγγραφών, τα πρώτα 10 keystrokes καταγράφηκαν (του κάθε χρήστη) και χρησιμοποιήθηκαν ως μια διαδικασία εγγραφής (enrollment) ενώ τα υπόλοιπα δεδομένα χρησιμοποιήθηκαν για την εκτίμηση της απόδοσης επαλήθευσης. Τα αποτελέσματα έδειξαν ότι το keystroke dynamics είναι σε θέση να εκτελέσει έλεγχο αυθεντικοποίησης χρήστη ακόμη όταν τα δείγματα της φάσης εγγραφής είναι λίγα. Ωστόσο, οι επιδόσεις της ταξινόμησης απέδωσαν καλύτερα αποτελέσματα όταν αυξήθηκε ο αριθμός των δειγμάτων της φάσης εγγραφής. Οι πιο επιτυχημένες ταξινομήσεις εφάρμοσαν ένα συνδυασμό τόσο inter-key όσο και hold-time.

Έρευνα του Chang et al [111] ερεύνησε την απόδοση του keystroke dynamics για αυθεντικοποίηση του χρήστη σε κινητό τηλέφωνο με οθόνη αφής. Στο [111] δύο τύποι χαρακτηριστικών μελετώνται, ο χρόνο μεταξύ δύο διαδοχικών πατημάτων πλήκτρων και ο χρόνος μεταξύ πατήματος και απελευθέρωσης ενός πλήκτρου. Ειδικότερα, μελετήθηκε ο τρόπος που ο χρήστης πληκτρολογεί τον κωδικό πρόσβασης και πώς αυτός βοηθάει στην αυθεντικοποίηση του χρήστη. Η μελέτη πρότεινε τη χρήση keystroke dynamics βασισμένη στον τρόπο που ο χρήστης πληκτρολογεί τον κωδικό πρόσβασης που βασίζεται σε γραφικά (pattern) για την ταξινόμηση του. Χρησιμοποιήθηκαν συνολικά τέσσερα χαρακτηριστικά keystroke dynamics: inter-key (1), hold time (2), το χρονικό διάστημα μεταξύ του πατήματος του γράμματος i και του αμέσως επόμενου γράμματος (3), και το χρονικό διάστημα της απελευθέρωσης του γράμματος i και της απελευθέρωσης του επόμενου γράμματος (4). Συνολικά 100 χρήστες που συμμετείχαν στη μελέτη, με κάθε χρήστη να παρέχει 10 δείγματα για κάθε 5 κωδικούς πρόσβασης. Για κάθε χρήστη, πέντε δείγματα συλλέχθηκαν ταυτόχρονα μέσω του ίδιου κινητού τηλεφώνου και χρησιμοποιούνται κατά τη διαδικασία εγγραφής. Τα άλλα πέντε δείγματα συλλέχθηκαν κατά τη διάρκεια περιόδου πέντε εβδομάδων με την χρήση δύο άλλων κινητών τηλέφωνων. Τα αποτελέσματα έδειξαν ότι τα keystroke dynamics μπορούν να χρησιμοποιηθούν για αναγνώριση του χρήστη με ένα αποδεκτό EER 12,2%. Επιπλέον, το EER μειώνεται σε 6,9%, όταν εφαρμόζεται και η μέτρηση της πίεσης στην οθόνη αφής εκτός

από τις λειτουργίες πληκτρολόγησης. Η μελέτη αυτή κατέδειξε, επίσης, ότι η απόδοση της προτεινόμενης τεχνικής δεν θα επηρεαστεί από το μέγεθος της οθόνης.

Ερευνητές απέδειξαν την αποτελεσματικότητα της μεθόδου αυτής τόσο σε συγκεκριμένα κείμενα όσο και σε κείμενα με ανεξάρτητα σενάρια [112]. Δεδομένου ότι τέτοια συστήματα δεν απαιτούν έξτρα εξειδικευμένο hardware στα smartphones και μπορούν να συλλεχθούν «διαφανώς» για τον χρήστη, έχουν δοκιμαστεί και αξιολογηθεί ευρέως [112]. Μία ακόμη πολυτροπική μέθοδος η οποία χρησιμοποιεί το σύστημα client-server για τα online οικονομικά περιβάλλοντα πέτυχε 96% TAR και 0.01% FAR χρησιμοποιώντας 15 παραδείγματα εκπαίδευσης από ένα σύνολο 95 χρηστών [112]. Το συγκεκριμένο σχήμα χρησιμοποίησε μια βιομετρική μέθοδο βασιζόμενη στην κίνηση της αφής στην οθόνη αφής δηλαδή στις κινήσεις των χρηστών των κινητών τηλεφώνων που συλλέχθηκαν «διαφανώς» ενώ οι χρήστες πληκτρολογούσαν τα credentials τους ώστε να μπουν μέσω της εφαρμογής της τράπεζας τους από το κινητό τηλέφωνο χρησιμοποιώντας ένα 8 ψήφιο κωδικό [112].

Ένα «γλίστρημα» (swipe) στην οθόνη ή ένα ελαφρύ χτύπημα στην οθόνη αφής είναι μια ακολουθία δεδομένων αφής. Κάθε swipe s μπορεί να κωδικοποιηθεί ως μια ακολουθία διανυσμάτων

$$si = (xi,yi,ti,pi,Ai,Of\ i,Oph\ i),\ i = \{1,2,\cdots,N\},\ [72]$$

όπου xi, yi είναι τα σημεία ενδιαφέροντος, και τα ti, pi, Ai, Of, Oph έχουν τη σφραγίδα του χρόνου, η πίεση στην οθόνη, η περιοχή που καλύπτει το δάχτυλο, ο προσανατολισμός του δακτύλου και ο προσανατολισμός του τηλεφώνου (landscape ή portrait), αντίστοιχα. Εδώ, N είναι ο συνολικός αριθμός swipes. Με βάση αυτές τις μετρήσεις, προτάθηκε ένα 30-διαστάσεων χαρακτηριστικό διάνυσμα το [72] για κάθε swipe. Έχει αποδειχθεί ότι με αυτούς τους ταξινομητές μπορεί να επιτευχθούν ποσοστά EER μεταξύ 0% και 4%, ανάλογα με το σενάριο εφαρμογής [72]. Παρόμοια χαρακτηριστικά έχουν επίσης χρησιμοποιηθεί σε [73], [113] και [114] για την συνεχή αυθεντικοποίηση με αφή. Για την ταξινόμηση χρησιμοποιήθηκαν μη γραμμικοί αλγόριθμοι, ενώ δέκα διαφορετικοί αλγόριθμοι κατάταξης αξιολογήθηκαν στο [113].

Οι μέθοδοι που παρουσιάζονται στο [72], [73], [113] και [114] βασίζονται στο γεγονός ότι μόνο ένα δάχτυλο είναι σε επαφή με την οθόνη αφής, όταν οι χρήστες εκτελούν βασικές λειτουργίες. Στην πράξη, πολλές εφαρμογές απαιτούν τους χρήστες να χρησιμοποιούν δυο ή περισσότερα δάκτυλα για να εκτελέσουν μια συγκεκριμένη εργασία, όπως η μεγέθυνση και η σμίκρυνση στις οποίες χρησιμοποιούνται και τα δύο δάχτυλα. Γενικότερα, ο συνεχής έλεγχος αυθεντικοποίησης με multitouch αφή έχει επίσης προταθεί στη βιβλιογραφία [70], [115]. Παρόμοια με την περίπτωση χειρονομίας ενός δάχτυλου χρησιμοποιήθηκαν στο [70] και [115] οι x και y συντεταγμένες, οι κατευθύνσεις του δάχτυλου κίνησης, η ταχύτητα κίνησης του δάχτυλου, η πίεση σε κάθε σημείο αφής και η απόσταση μεταξύ multitouch για να εξαχθούν συμπεράσματα.

Κάτι διαφορετικό από τα χαρακτηριστικά της χειρονομία αφής που συζητήθηκε παραπάνω, είναι ένα χαρακτηριστικό βασισμένο σε φωτογραφίες που ονομάζεται Graphic Touch Gesture Feature (GTGF) προτάθηκε στο [74] για τη μοντελοποίηση της δυναμικής της αφής. Σε αυτήν την προσέγγιση, τα χαρακτηριστικά της γεωμετρίας του swipe μετατρέπονται σε εικόνες, έτσι ώστε να μπορούν να μοντελοποιηθούν. Επιπλέον, γίνεται σύνθεση της πίεσης στην οθόνη με την κίνηση στην οθόνη. Αυτή η μέθοδος αργότερα επεκτάθηκε στο [116] δημιουργώντας το μοντέλο της εμφάνισης των χειρονομιών από την GTGF. Αυτό το μοντέλο χρησιμοποιεί στατιστική ανάλυση και είναι εφαρμόσιμη τόσο σε χρήστες που χρησιμοποιούν ένα δάχτυλο στην οθόνη αφής όσο και για αυτούς που χρησιμοποιούν περισσότερα.

Σε πολλές εργασίες έχουν χρησιμοποιηθεί τα συμφραζόμενα για βελτίωση της απόδοσης της συνεχούς αυθεντικοποίησης. Για παραδείγματα, το [117] διερευνά πώς η θέση στην οποία κρατάει ο χρήστης το smartphone επηρεάζει την αυθεντικοποίηση. Μια άλλη μέθοδος που στηρίζεται πάλι στα συμφραζόμενα [118] προτείνει τη χρήση παθητικών όσο και ενεργητικών παραγόντων για συνεχή αυθεντικοποίηση. Στο [119] τα συμφραζόμενα χρησιμοποιούνται για τη βελτίωση αυθεντικοποίησης του χρήστη σε συνδυασμό με τις χειρονομίες αφής.

Ο Aljohani et al [120] πρότεινε ένα σύστημα τεχνητής νοημοσύνης (Artificial Immune System (AIS)) για CA με βάση την αφή στην οθόνη αφής. Τα αποτελέσματα τους έδειξαν ότι στο 96.89% το AIS πραγματοποιούσε σωστή αυθεντικοποίηση. Το AIS είναι πολλά υποσχόμενο ειδικά για αυθεντικοποίηση του χρήστη σε ευαίσθητες εφαρμογές και βελτιώνεται όσο αυξάνονται οι διαθέσιμοι νέοι αισθητήρες στα κινητά τηλέφωνα.

Method	Works	Platform	Classification	Performance (%)				
				FAR	TAR	Accuracy	FRR	EER
Keystroke Dynamics	[108] in 2006	smartphone	Forward Multi-Layered Perceptron network (FF MLPs), Radial basis function network (RBF), Generalised regression neural network (GRNNs)					12.8%
	[109] in 2007	smartphone	statistical					12.2%
	[110] in 2011	smartphone	Bayes Classifier, Support Vector Machines (SVMs), Principal Component Analysis (PCA)					14%
	[111] in 2012	smartphone	statistical					1.8%
	[112] in 2017	smartphone	Naive Bayes (NB), Neural Net (NN), and Random Forest (RF) Classifers	0.01%	96%			
	[74] in 2013	smartphone	SVM					2.62%
	[120] in 2017	smartphone	Negative Selection (NS), Clonal Selection (CS), Immune Network			96.89%		

Πίνακας 5: Σύνοψη των Keystroke dynamics μεθόδων

3.7 *Κατανάλωση ενέργειας (Power Consumption)*

Ο Shye et al. [121] παρουσίασαν ένα μοντέλο εκτίμησης ενέργειας αξιοποιώντας την συμπεριφορά του πραγματικού χρήστη. Παρουσίασαν στοιχεία ότι η κατανάλωση είναι ιδιαίτερα σχετιζόμενη με τη συμπεριφορά του χρήστη, αλλά η έρευνα δεν συνεχίστηκε περαιτέρω.

Ο Murmuria et al. [122] κατέδειξαν ότι η κατανάλωση ενέργειας από drivers στη συσκευή ενός smartphone ποικίλουν από την κατάσταση της λειτουργίας τους αυτού του συγκεκριμένου driver. Στο [123] πρότειναν μια συνεχή παρακολούθηση του χρήστη χρησιμοποιώντας τρία χαρακτηριστικά: την κατανάλωση ενέργειας, τις χειρονομίες αφής, και την φυσική κίνηση του χρήστη. Ήταν σε θέση έτσι να βεβαιωθούν ότι το σύστημά τους είναι λειτουργικό σε πραγματικό χρόνο ενώ ο τελικός χρήστη χρησιμοποιούσε παράλληλα δημοφιλείς εφαρμογές, επιτυγχάνοντας καλή απόδοση με ποσοστό ERR 6,1% και 6,9% για 59 επιλεγμένους χρήστες που είχαν δημιουργηθεί επαρκή δεδομένα για την αξιολόγηση.

3.8 ***Multimodal***

Τα πολυτροπικά βιομετρικά στοιχεία είναι ο συνδυασμός των διαφόρων βιομετρικών χαρακτηριστικών κατά τη λειτουργία εξαγωγής χαρακτηριστικών γνωρισμάτων, στο σκορ ταύτισης ή κατά το επίπεδο απόφασης (extraction, match score, ή decision level) [124].

Μια έρευνα των Kim et al [125] πρότεινε ένα ενισχυμένο σύστημα πολυτροπικών βιομετρικών χαρακτηριστικών για κινητές συσκευές, το οποίο συνδυάζει πληροφορίες που λαμβάνονται από το πρόσωπο, τα δόντια και την φωνή για να βελτιώσει τις επιδόσεις του. Τα αποτελέσματα του πειράματος συνδυάζοντας τους τρεις αυτούς τρόπους έδειξαν τα ποσοστά σφάλματος (EER) 1.64%, 4,70% και 3,06%. Αντίθετα, τα ποσοστά σφάλματος (EER) σχετικά με ένα μόνο χαρακτηριστικό ήταν 5.09%, 7,75% και 8,98% για το πρόσωπο, τα δόντια και τις λεπτομέρειες της φωνής, αντίστοιχα.

Ο Saevanee et al. [126] ερεύνησε τρεις συμπεριφορικές βιομετρικές τεχνικές βάσει της δραστηριότητας των γραπτών μηνυμάτων SMS προσπαθώντας να εφαρμόσει αυτές τις τεχνικές ως πολυτροπικές μεθόδους βιομετρικής αυθεντικοποίησης για κινητές συσκευές. Τα αποτελέσματα έδειξαν ότι το προφίλ συμπεριφοράς, η δυναμική πληκτρολόγηση και τα γλωσσικά χαρακτηριστικά (behavior profiling, keystroke dynamics και linguistic profiling) μπορούν να χρησιμοποιηθούν για να διακρίνουμε τους χρήστες με συνολικό ποσοστό σφάλματος 20%, 20% και 22% αντίστοιχα. Χρησιμοποιήθηκαν δύο συνδυαστικοί μέθοδοι: το απλό άθροισμα και το μέσο βάρος. Τα αποτελέσματα έδειξαν ότι ο συνδυασμός του επιπέδου ταύτισης (matching level) μπορεί να βελτιώσει την απόδοση ταξινόμησης με 8% EER.

Ο Shi et al. [127] παρουσίασε μια προσέγγιση που βασίστηκε στην ιδέα ότι οι περισσότεροι χρήστες από την φύση τους παρασύρονται από τη συνήθεια και είναι επιρρεπείς στην εκτέλεση παρόμοιων εργασιών σε ένα ορισμένο χρονικό διάστημα της ημέρας. Οι ερευνητές συνέλεξαν ένα ευρύ φάσμα πληροφοριών συμπεριφοράς όπως η τοποθεσία, η επικοινωνία και η χρήση των εφαρμογών, προκειμένου να δημιουργήσουν ένα προφίλ χρήστη. Η μέθοδος βασίζεται στην αναγνώριση των θετικών γεγονότων και ενισχύει το σκορ αυθεντικοποίησης, όταν παρατηρείται μια «καλή» ή συνήθης συμπεριφορά. Αν το ανώτερο όριο που έχει οριστεί ώστε ο νόμιμος χρήστης μπορεί να χρησιμοποιεί τη συσκευή περίπου 100 φορές πριν από μια αποτυχία της αυθεντικοποίησης, τότε με πιθανότητα 50%, ο κακόβουλος χρήστης θα κλειδωθεί απέξω μετά τη χρήση της συσκευής το πολύ δύο φορές. Με πιθανότητα 95%, ο κακόβουλος χρήστης θα κλειδωθεί μετά από 16 ή λιγότερες χρήσεις της συσκευής.

Ο Riva et al. [128] παρουσίασε μια αρχιτεκτονική που χορηγεί στους χρήστες πρόσβαση σε οποιοδήποτε περιεχόμενο της συσκευής, μόνο όταν το σύστημα αυθεντικοποίησης αξιολογήσει το επίπεδο γνησιότητας ότι είναι υψηλότερο από ό,τι απαιτείται για να αποκτήσει πρόσβαση στο συγκεκριμένο περιεχόμενο. Αυτό το σύστημα χρησιμοποιεί την αναγνώριση προσώπου και φωνής, τη χρήση γνωστών τοποθεσιών και την αναγνώριση κατοχής από αισθητήρες που αναζητούν κοντινές ηλεκτρονικές συσκευές του νόμιμου χρήστη, για να αυθεντικοποιήσουν το χρήστη και το επίπεδο γνησιότητας. Κίνητρο τους αποτέλεσε μια μελέτη ενός χρήστη που ερευνούσε μοντέλα όπου υπάρχουν τουλάχιστον 3 επίπεδα ασφάλειας: δημόσιο, ιδιωτικό και εμπιστευτικό. Με αυτό τον τρόπο, εξέτασαν εννέα χρήστες, και ήταν σε θέση να μειώσουν τον αριθμό των άμεσων αυθεντικοποιήσεων κατά 42%.

Ο Crawford et al. [129] παρουσίασε ένα πλαίσιο για την συνεχή και διαφανή αυθεντικοποίηση στις κινητές συσκευές που χρησιμοποιούν συμπεριφορικά βιομετρικά χαρακτηριστικά για να

προσδιορίσουν τον κάτοχο της συσκευής. Δοκιμάστηκε το συγκεκριμένο πλαίσιο μέσα από μια προσομοίωση όπου χρησιμοποιήθηκαν πληροφορίες πληκτρολόγησης και φωνής, οι οποίες έδειξαν ότι ένας νόμιμος χρήστης συσκευής μπορεί να εκτελέσει όλες τις εργασίες της συσκευής, μειώνοντας την άμεση αυθεντικοποίηση της συσκευής κατά 67%, χωρίς να απαιτείται μια συγκεκριμένη μέθοδος αυθεντικοποίησης. Επιπλέον, η αξιολόγησή τους έδειξε ότι οι επιτιθέμενοι αντιμετωπίζουν αμέσως άρνηση πρόσβασης στις λειτουργίες της συσκευής, τη στιγμή που συλλέγονται τα συμπεριφορικά βιομετρικά χαρακτηριστικά.

Ο Wolff [130] έδειξε ότι η συλλογή δεδομένων από επιταχυνσιόμετρα, οθόνες αφής και πληκτρολόγια μπορούν να χρησιμοποιηθούν για να διαφοροποιήσουμε τους χρήστες βασιζόμενοι στον μοναδικό τρόπο που χρησιμοποιούν το κινητό. Η έρευνα αυτή ήταν επιτυχής με ακριβή ταυτοποίηση των ατόμων σε ποσοστό 83% χρησιμοποιώντας μια απλή κατανομή του κάθε χαρακτηριστικού.

Ο Zheng et al. [131], πρότειναν μία μη παρεμβατική από τον χρήστη μέθοδο αυθεντικοποίησης, χρησιμοποιώντας το συνδυασμό τεσσάρων χαρακτηριστικών (επιτάχυνση, πίεση, μέγεθος και χρόνος) που προέρχονται από αισθητήρες του smartphone (επιταχυνσιόμετρο, γυροσκόπιο και αισθητήρες οθόνης αφής). Εξέτασαν κατά πόσον ένας εξουσιοδοτημένος χρήστης είναι ο πραγματικός χρήστης του smartphone ή ένας εισβολέας που απλά τυχαίνει να γνωρίζει τον κωδικό πρόσβασης. Τα πειραματικά αποτελέσματα έδειξαν ότι το σύστημα αυθεντικοποίησης πέτυχαν επαλήθευση υψηλή ακρίβειας με EER 3,65%.

Επιπλέον, ο Bo et al. [132] παρουσίασαν ένα πλαίσιο εργασίας το οποίο αυθεντικοποιούσε χρήστες αξιοποιώντας τη βάδιση σε συνδυασμό με τη συμπεριφορά αφής και τις μικροκινήσεις της κινητής συσκευής που προκαλούνται από ενέργειες του χρήστη στην οθόνη αφής. Η έρευνα έδειξε ότι η ακρίβεια της αναγνώρισης χρήστη ήταν πάνω από 99%.

Ο Buriro et al [133], προτείναν ένα πολυτροπικό συμπεριφορικό βιομετρικό σύστημα που χρησιμοποιεί δεδομένα που συλλέγονται από τον τρόπο που ο χρήστης ξεκλειδώνει το smartphone για να απαντήσει σε μια κλήση. Αυτά τα χαρακτηριστικά είναι η κύλιση ξεκλειδώματος, η κίνηση του χεριού που φέρνει το τηλέφωνο κοντά στο αυτί και η αναγνώριση φωνής. Εφάρμοσαν την μέθοδο τους σε ένα πραγματικό τηλέφωνο και το χρησιμοποίησαν σε 26 συμμετέχοντες σε διάφορα σενάρια προκειμένου να αξιολογήσουν το πρωτότυπο τους. Το πολυτροπικό σύστημα τους, είχε FAR 11.01% FRR 4,12%. Και το HTER ήταν 7.57%.

Για παράδειγμα, μια άλλη πολυτροπική μέθοδος χαρακτηριστικών βασιζόμενη σε πολλαπλές χαμηλού βαθμού αναπαραστάσεις προτάθηκε πρόσφατα στο [134] για να συνδυαστούν οι χειρονομίες αφής και η αναγνώριση προσώπου για συνεχή αυθεντικοποίηση. Μια συνδυαστική μέθοδος επιπέδου απόφασης προτάθηκε στο [135] για τον συνδυασμό τεσσάρων τρόπων εφαρμογής με βάση την ανάλυση κειμένων, τα μοτίβα χρήσης των εφαρμογών, την περιήγηση στο ίντερνετ και την φυσική θέση της συσκευής για συνεχή αυθεντικοποίηση. Η ανάλυση που έγινε σε ένα dataset 200 κινητών συσκευών Android, των οποίων τα δεδομένα συλλέχθηκαν για μια περίοδο τουλάχιστον 30 ημερών έδειξε ότι αυτή μέθοδος μπορεί να επιτύχει ένα EER 0,05 χρησιμοποιώντας χρονικό παράθυρο 1 λεπτού και ένα EER κάτω 0.01 χρησιμοποιώντας χρονικό παράθυρο 30 λεπτών. Ομοίως στο [136], προτάθηκε ένα σύστημα SenGuard στην οποία πολλά στοιχεία συνδυάζονται σε επίπεδο απόφασης για συνεχή αυθεντικοποίηση. Δεδομένα από το επιταχυνσιόμετρο, την οθόνη αφής, το μικρόφωνο, καθώς και το ιστορικό τοποθεσίας χρησιμοποιούνται για να παρακολουθούν συνεχώς την ταυτότητα του χρήστη σε μια κινητή

συσκευή. Επιπλέον οι μέθοδοι τους που βασίζονται στην αφή μπορούν να χειριστούν τόσο την αφή με ένα δάχτυλο όσο και με πολλά (multi-touch).

Μια μέθοδος δι-τροπικής συνεχούς αυθεντικοποίησης βάσει αναγνώρισης προσώπου και αναγνώρισης ομιλητή προτάθηκε στο [137]. Παρόμοια σκορ ταύτισης για έλεγχο ταυτότητας προσώπου και σκορ ταύτισης εισόδου στο σύστημα κανονικοποιούνται για να παράγουν πιθανότητες με μεγαλύτερη δυνατότητα σωστού αποτελέσματος.

Πρόσφατα, μια σειρά από συμπεριφορικά χαρακτηριστικά όπως η κίνηση του χεριού, ο προσανατολισμός και τρόπος πιασίματος του κινητού (Hand Movement, Orientation, and Grasp - HMOG) προτάθηκε στο [77] για συνεχή αυθεντικοποίηση χρηστών smartphones. Η HMOG βασίζεται σε δεδομένα από το επιταχυνσιόμετρο, το γυροσκόπιο, το μαγνητόμετρο σχετικά με απαλές μικρό-κινήσεις των χεριών και τον προσανατολισμό της συσκευής όταν ένας χρήστης ακουμπά την οθόνη. Ένα σύνολο 96 HMOG χαρακτηριστικών προτάθηκε και αξιολογήθηκε σε ένα σύνολο δεδομένων που αποτελούνταν από δεδομένα πληκτρολόγησης 100 χρηστών. Αποδείχθηκε ότι μπορεί να επιτύχει EER 7,16% (περπάτημα) και 10.05% (στάσιμη θέση) όταν τα HMOG χαρακτηριστικά συνδυάζονται με το άγγιγμα της αφής και την πληκτρολόγηση.

Στο [138] τρεις διαφορετικές μέθοδοι βασιζόμενες σε κείμενο - γλωσσικό προφίλ, το συμπεριφορικό προφίλ και τη δυναμική πληκτρολόγησης χρησιμοποιήθηκαν για πολυτροπική αυθεντικοποίηση. Δεδομένου ότι δεν υπήρχε κανένα dataset που να αποτελείται από αυτά τα τρία χαρακτηριστικά για το ίδιο άτομο, αυτά συνδυάστηκαν από διαφορετικά σύνολα δεδομένων για να δημιουργηθεί ένα εικονικό σύνολο δεδομένων των 30 χρηστών. Με βάση αυτό το dataset, ανέφεραν EER 3,3% όταν υπήρχε συνδυασμός των τριών χαρακτηριστικών.

Ο Akhtar et al [139] παρουσίασαν μια μέθοδο που βασίζεται στις κινήσεις του προσώπου, την κίνηση του τηλεφώνου και την αφή. Η συγκεκριμένη μέθοδος αυθεντικοποιεί το χρήστη λαμβάνοντας υπόψη στο παρασκήνιο τις μικροκινήσεις του τηλεφώνου, τις κινήσεις των δαχτύλων του χρήστη όταν γράφει στην οθόνη και επίσης τα χαρακτηριστικά του προσώπου του χρήστη. Η συγκεκριμένη μέθοδος πέτυχε EER 1%. Επίσης επειδή η συγκεκριμένη μέθοδος είναι γενική μπορεί να εφαρμοστεί στο κινητό τηλέφωνο για να ξεκλειδωθεί αλλά και ως πρόσθετη δικλείδα ασφαλείας σε εφαρμογές όπως για παράδειγμα το mobile banking.

Ο Khamis et al [140] πρότεινε μια μέθοδο για να δυσκολέψει κυρίως επιθέσεις τύπου shoulder surfing καθώς και thermal attacks [141] και πρότεινε το GazeTouchPIN. Η συγκεκριμένη μέθοδος συνδυάζει το PIN και το βλέμμα [142] για αυθεντικοποίηση του χρήστη και για αποτροπή υποκλοπής του κωδικού. Το GazeTouchPIN εφαρμόζεται σε Android συσκευές και δεν απαιτεί έξτρα hardware αλλά χρησιμοποιεί την ήδη υπάρχουσα μπροστινή κάμερα του κινητού τηλεφώνου. Το GazeTouchPIN είναι ιδιαίτερα χρήσιμο σε περιπτώσεις όπου ο χρήστης αισθάνεται ότι παρακολουθείται ή όταν έχει πρόσβαση σε ευαίσθητες πληροφορίες (π.χ. σε Μέσα Μαζικής Μεταφοράς [143]). Το GazeTouchPIN απαιτεί μεγαλύτερο χρόνο αυθεντικοποίησης και γι' αυτό πρέπει να χρησιμοποιείται από το χρήστη μόνο όταν υπάρχει ανάγκη. Για το shoulder attack έχουμε μια μείωση της υποκλοπής του κωδικού από τις γνωστές μεθόδους από 68% σε 10.4% [144]. Στη συγκεκριμένη μέθοδο πρέπει ο επιτιθέμενος να παρατηρεί τα μάτια του χρήστη και την οθόνη ταυτόχρονα. Στο συγκεκριμένο παράδειγμα ο χρήστης πληκτρολογεί τον κωδικό 6641. Πρώτα ο χρήστης πληκτρολογεί τα πρώτα δυο ψηφία στην οθόνη, μετά κοιτάζει αριστερά και δεξιά του και

μετά ξανακοιτάζει την οθόνη για να πληκτρολογήσει τα άλλα δύο ψηφία καθότι το πληκτρολόγιο αλλάζει μόνο του σε τυχαία σειρά τους αριθμούς.

Ο Brosso et al. [145], παρουσίασαν ένα σύστημα συνεχούς αυθεντικοποίησης που μπορεί να εμπιστευτεί το χρήστη ή όχι βασιζόμενο στα στοιχεία της συμπεριφοράς του. Τα επίπεδα αξιοπιστίας μετριόνται σύμφωνα με τη συμπεριφορά του χρήστη, προκειμένου να έχει πρόσβαση στο λογισμικό εφαρμογής. Το σύστημα κάνει χρήση περιβαλλοντικών πληροφοριών, της ανάλυση της συμπεριφοράς των χρηστών και χρήση λογικής Neuro-Fuzzy. Η Neuro-Fuzzy λογική επιτρέπει να ενημερώνεται συνεχώς η βάση συμπεριφοράς του χρήστη, έτσι ώστε να διατηρεί τα επίπεδα εμπιστοσύνης ενημερωμένα, με έναν τρόπο πιο ακριβή και έμπιστο.

Η κίνηση της κινητής συσκευής καθώς και ο θόρυβος του περιβάλλοντος που μετριέται από τα μικρόφωνα χρησιμοποιήθηκαν στο [146] για έλεγχο αυθεντικοποίησης των χρηστών. Με βάση τα δεδομένα που συλλέχθηκαν από 9 χρήστες αναφέρθηκε ακρίβεια αναγνώρισης της τάξης των 88,3% και 47,8%, 90,1% για κίνηση, ήχο και συνδυασμός των δύο αυτών χαρακτηριστικών, αντίστοιχα.

Method	**Works**	**Platform**	**Classification**	**Performance (%)**				
				FAR	**TAR**	**Accuracy**	**FRR**	**EER**
Multimodal	[125] in 2010	smartphone	weighted-summation rule, K-NN, Fisher and Gaussian classifiers					<8.98%
	[126] in 2011	smartphone	neural network (Feed-Forward Multilayer Perception Neural Network)					8%
	[127] in 2010	smartphone	Gaussian Mixture Model (GMM)			95%		
	[128] in 2012	smartphone	SVM			>76%		
	[130] in 2013	smartphone	statistical			83%		
	[131] in 2014	smartphone	statistical					3.65%
	[132] in 2013	smartphone	SVM			99%	<1%	
	[133] in 2015	smartphone	One-class BayesNET (BN), One-class Random Forest (RF) and One-class Sequential Minimal Optimization (SMO)-a Weka version of support vector machine (SVM)	11.01%			4.12%	
	[135] in 2015	smartphone	SVM					5%

	[137] in 2012	smartphone	local binary patterns (LBPs), modified census transform (MCT)					<10.9%
	[77] in 2016	smartphone	Scaled Manhattan, Scaled Euclidean, SVM verifiers, and score-level fusion					<10.05%
	[138] in 2014	smartphone	K-Nearest Neighbor (K-NN), the Radial Basis function (RBF) and Feed-Forward Multi-Layered Perceptron (FF-MLP)					3.3%
	[139] in 2017	smartphone	statistical					1%
	[146] in 2011	smartphone	statistical			90.1%		
	[144] in 2017	smartphone	Decision Tree Algorithm			95%		

Πίνακας 6: Σύνοψη των multimodal μεθόδων

3.9 *Ανοικτά ζητήματα έρευνας και ανάπτυξης*

Πραγματοποίησα μια επισκόπηση της βιβλιογραφίας σχετικά με το θέμα της συνεχούς αυθεντικοποίησης (CA) χρησιμοποιώντας συμπεριφορικά βιομετρικά χαρακτηριστικά, όπου ένας μεγάλος αριθμός μελετών προτείνουν διάφορες μεθόδους για τον εντοπισμό χρηστών μέσω των αλληλεπιδράσεών τους με τη συσκευή. Όσον αφορά τα ανοιχτά ζητήματα έρευνας και ανάπτυξης, το πεδίο της CA χρησιμοποιώντας μοτίβο συμπεριφορών χρήσης των εφαρμογών είναι μια πολλά υποσχόμενη λύση και απαιτεί περαιτέρω έρευνα, προκειμένου να αξιολογηθεί η αποτελεσματικότητά της.

Πράγματι, ο Stylios et al. [147] παρείχαν ισχυρές ενδείξεις ότι κάθε χρήστης έχει το δικό του ιδιαίτερο και ξεχωριστό τρόπο που χρησιμοποιεί την κινητή συσκευή, πέρα από τις γενικές παρόμοιες τάσεις, καθώς και από αυτές που σχετίζονται με την ηλικία. Για παράδειγμα, αποδεικνύεται ότι δεν υπάρχει καμία περίπτωση χρήστες που χρησιμοποιούν ακριβώς το ίδιο σύνολο των εφαρμογών, τις ίδιες ώρες της ημέρας, να μην έχουν διαφοροποίηση μεταξύ τους. Επιπλέον, οι χρήστες διαφοροποιούνται κατά τη χρήση των εφαρμογών ή τη διάρκεια της χρήσης, καθώς επίσης υπάρχουν διαφοροποιήσεις ακόμα και στον τρόπο που αποθηκεύονται τα δεδομένα π.χ., χρησιμοποιώντας μια λύση αποθήκευσης στο cloud, όπως το Dropbox ή την αποθήκευση τους στη μνήμη του τηλεφώνου, καθώς και τη γλώσσα γραφής, τον τρόπο αναζήτησης, τον αριθμό των SMS και των τηλεφωνικών κλήσεων, η σειρά προτεραιότητας και με τον τρόπο που χρησιμοποιούν

τις εφαρμογές. Αυτές οι παρατηρήσεις στηρίζουν την υπόθεση ότι η συμπεριφορά του κάθε χρήστη μπορεί να δημιουργήσει ένα προφίλ με βάση τα πρότυπα χρήσης των εφαρμογών.

Σε κάθε περίπτωση, ένα από τα μειονεκτήματα του CA που χρησιμοποιούν μοτίβο χρήσης των εφαρμογών είναι ότι λαμβάνει δεδομένα εισόδου από γεωγραφικές τοποθεσίες, τηλεφωνικές κλήσεις, μηνύματα κειμένου και διευθύνσεων URL. Έτσι οι πληροφορίες που συλλέγονται είναι ιδιαίτερα διεισδυτικές από άποψη προστασίας προσωπικών δεδομένων και πρέπει να ληφθούν μέτρα για τη διαφύλαξη της ιδιωτικής ζωής των χρηστών.

Η πρακτική εφαρμογή των σχημάτων CA έχει περιορισμένη έκταση λόγω δύο θεμελιωδών ανεπαρκειών στις υφιστάμενες προσεγγίσεις: των θεμάτων ιδιωτικότητας και του κινδύνου θετικών ψευδών και αρνητικών ψευδών αυθεντικοποιήσεων. Οι ελλείψεις αυτές είναι υπό εξέταση που έχει ως στόχο να σχεδιάσει και να αξιολογήσει διαφορετικές προσεγγίσεις CA χρησιμοποιώντας ένα θεωρητικό υπόβαθρο, προκειμένου να δώσει ένα υψηλό επίπεδο εμπιστοσύνης, για να φτάσουμε στο επιθυμητό αποτέλεσμα [148].

3.10 ***Σύνοψη***

Υπάρχουν τέσσερις συμπεριφορικές βιομετρικές τεχνικές: linguistic profiling, walking gait, keystroke dynamics και behaviour profiling που έχουν αναγνωριστεί ως οι πιο κατάλληλες τεχνικές που μπορούν να παρέχουν αυθεντικοποίηση - που μπορεί να πιστοποιήσει τους χρήστες βάσει της πιο συχνά χρησιμοποιούμενης γραπτής επικοινωνίας στην κινητή συσκευή. Ένας σημαντικός αριθμός από προηγούμενες μελέτες έχουν δείξει ότι αυτές οι τέσσερις τεχνικές μπορούν να χρησιμοποιηθούν για να αυθεντικοποιηθεί ένας χρήστης με υψηλό βαθμό απόδοσης. Παρέχουν, επίσης, σαφείς αποδείξεις ότι η απόδοση των πολυτροπικών συστημάτων υπερτερεί σημαντικά των μονοτροπικών προσεγγίσεων. Ως εκ τούτου, η χρήση πολυτροπικών βιομετρικών τεχνικών που βασίζονται στα γλωσσικά χαρακτηριστικά, τη δυναμική πληκτρολόγηση και το προφίλ συμπεριφοράς αποτελούν μια ενδιαφέρουσα πρόταση που δίνεται για αυθεντικοποίηση στηριζόμενης σε οποιαδήποτε μορφή πληκτρολόγησης, όπως η πληκτρολόγηση ενός αριθμού τηλεφώνου, ενός μηνύματος, ενός email και κατά τη χρήση μέσων κοινωνικής δικτύωσης.

Παρουσιάστηκαν τα αποτελέσματα μιας σειράς πειραμάτων που διεξήχθησαν για να εξετάσουν τη σκοπιμότητα της αξιοποίησης γλωσσικών χαρακτηριστικών, της δυναμικής πληκτρολόγησης, τη σκιαγράφηση συμπεριφοράς και τα πολυτροπικά βιομετρικά χαρακτηριστικά για την αυθεντικοποίηση των χρηστών στις κινητές συσκευές.

4

Επιθέσεις σε Smartphones

4.1 *Διάφοροι τύποι επιθέσεων σε smartphones*

Όλα τα συστήματα και οι συσκευές είναι απαραίτητο να διασφαλίζονται μέσω των μεθόδων αυθεντικοποίησης. Μη εξουσιοδοτημένοι χρήστες είναι δυνατόν να λάβουν τον έλεγχο και να αντικαταστήσουν τους «νόμιμους» χρήστες μέσω επιθέσεων κατά της αυθεντικοποίησης τους από την συσκευή. Στο όνομα των νόμιμων χρηστών, οι εισβολείς μπορούν να προβούν σε ενέργειες χρησιμοποιώντας εγκατεστημένα συστήματα και λειτουργίες, πλήττοντας έτσι την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα τους [149]. Στη συνέχεια αναλύονται συνοπτικά διάφορα είδη επιθέσεων [150]:

4.1.1 Capturing Attacks

Όλα τα πράγματα που μπορούν να αποτυπωθούν μπορούν να δεχτούν capturing attacks. Παραδείγματα τέτοιου είδους επιθέσεων είναι τα shoulder surfing, eavesdropping και social engineering. Social engineering είναι η τέχνη κατά την οποία οι χρήστες χειραγωγούνται ώστε να προβούν σε συγκεκριμένες πράξεις ή να αποκαλύψουν εμπιστευτικές πληροφορίες. Είναι ένας πολύ διαδεδομένος παράγοντας ασφαλείας που περιλαμβάνει την καθοδήγηση των ανθρώπων να αποκαλύψουν προσωπικά δεδομένα όπως π.χ. το PIN ή το password τους. Το social engineering μπορεί, επίσης, να χρησιμοποιήσει την αποκάλυψη μίας εικόνας για την αυθεντικοποίησης του προσώπου του χρήστη μέσω Face Unlock. Επίσης εάν ο εισβολέας μπορέσει να πλησιάσει επαρκώς ώστε να τα διαβάσει, είναι δυνατό να έχει πρόσβαση στα NFC tags. Το Gesture Puzzle αντιθέτως, θεωρείται πιο δύσκολο να πέσει θύμα social engineering καθώς χρησιμοποιεί πολλούς κωδικούς, μία ακολουθία εικόνων συν την αντίστοιχη χειρονομία, τα οποία θα πρέπει να εκτεθούν για (την επίθεση σε) κάθε κωδικό [149].

Σε εταιρικό επίπεδο, πού συχνά, οι άνθρωποι δεν γνωρίζουν προσωπικά όλα τα μέλη του προσωπικού ή την ομάδα τεχνικής υποστήριξης είναι πολύ συχνό το φαινόμενο του social engineering. Μερικές φορές μία μόνο κλήση είναι αρκετή ώστε να αποκτηθούν σημαντικές πληροφορίες. Όταν παρακολουθείς κάποιον να καταχωρεί απόρρητες πληροφορίες, αυτό ορίζεται ως shoulder surfing. Κατά το Shoulder surfing είναι πιο εύκολο για αυτόν που παρακολουθεί να αναγνωρίσει ένα PIN ή ένα μοτίβο ξεκλειδώματος που χρησιμοποιεί ο χρήστης. Ένας μακροσκελής

κωδικός είναι δυσκολότερο να αναγνωριστεί εξαιτίας του μήκους του, σε αντίθεση με τα μοτίβο ξεκλειδώματος που είναι πιο επιδεκτικά shoulder surfing ακόμα και από απόσταση καθώς αποτυπώνονται στην οθόνη. Όλοι οι άλλοι μηχανισμοί δεν ενέχουν κίνδυνο σε περίπτωση που παρακολουθούνται από τρίτους [149].

Για παράδειγμα, η χειρονομία - μοτίβο είναι ένας συχνός τρόπος αυθεντικοποίησης στα κινητά και μπορεί πολύ εύκολα να τη μαντέψει κάποιος τρίτος.

Το Spyware / Malware είναι άλλη μία μέθοδος υποκλοπής, όπως ένα κακόβουλο λογισμό που συγκεντρώνει πληροφορίες των χρηστών εν αγνοία τους. Το Malware είναι παλιά και συχνή απειλή ασφαλείας που μπορεί να εμφανιστεί με διάφορες μορφές. Πιο συγκεκριμένα, ένα λογισμικό υποκλοπής spyware ή Malware ή μία ψεύτικη εφαρμογή μπορεί να εκτελείται στο παρασκήνιο ενόσω ο χρήστης εισάγει κωδικούς πρόσβασης και να τους στέλνει σε server που ελέγχει ο εισβολέας. Ο εισβολέας μπορεί επίσης να προσπαθήσει να αποκτήσει φυσική πρόσβαση στη συσκευή αν τα δεδομένα της αυθεντικοποίησης πάνε στο server και όταν ο χρήστης βάζει το pin ή password τότε είναι εύκολο κάποιος που έχει πρόσβαση στο server να καταγράψει / κλέψει τα στοιχεία εισόδου του χρήστη.

Στην περίπτωση του NFC το μόνο που χρειάζεται είναι μία εικόνα ή ο αριθμός πιστοποίησης του. Είναι, επίσης, εύκολο να δημιουργηθεί ένα πλαστό περιβάλλον εργασίας χρήστη παρόμοιο με το παράθυρο διαλόγου της οθόνης του κινητού ώστε να ληφθεί το PIN ή ο κωδικός πρόσβασης που εισάγει ο χρήστης μέσω ενός κακόβουλου λογισμικού. Το gesture puzzle διασφαλίζει κάποια προστασία διότι βασίζεται σε εικόνες που δίδονται στον χρήστη. Η αυθεντικοποίηση στις κινητές συσκευές είναι ευάλωτη σε αυτού του είδους επιθέσεις (capturing attacks), όπως είναι το social engineering, το shoulder surfing και το κακόβουλο λογισμικό (spyware). Οι υποκλοπές θα μπορούσαν να αποτελούν ζήτημα εάν η αυθεντικοποίηση γινόταν ασύρματα, κάτι όμως που δεν συμβαίνει επί του παρόντος [149].

Εδώ επίσης πρέπει να αναφερθεί η περίπτωση του 2-step verification ή two factor authentication όπου σαν συσκευή χρησιμοποιείται το κινητό τηλέφωνο αλλά με την αποδοχή SMS και όχι μέσω κάποιας OTP εφαρμογής. Αυτό έχει αποδειχτεί ότι ενέχει πολλούς κινδύνους υποκλοπής μέσω κάποιου κακόβουλου κώδικα και πλέον δεν θεωρείται ασφαλής μέθοδος και γι' αυτό το λόγο ο National Institute of Standards and Technology (NIST) πλέον δεν προτείνει την χρήση 2-step verification μέσω SMS [151], [152]. Υπάρχει και σχετική έρευνα από τους Thomas Zink και Marcel Waldvogel [153] όπου προκύπτει ότι πλέον το 83.3 % των χρηστών δεν θεωρεί βολική λύση το SMS για αυθεντικοποίηση.

4.1.2 Cracking Attacks και Guessing

Σε αντίθεση με τις capturing επιθέσεις, στις cracking attacks δεν απαιτείται η παρεμβολή του αυθεντικού χρήστη. Το cracking περιλαμβάνει συστηματικές προσεγγίσεις που προσπαθούν να ανακαλύψουν επιτυχείς μεθόδους αυθεντικοποίησης που θα αποδεχτεί το σύστημα. Εάν ο χρήστης δεν δημιουργήσει ένα ισχυρό password είναι πολύ πιθανό το «μάντεμα» αυτού του κωδικού να είναι επιτυχές. Τους αδύναμους κωδικούς δεν μπορεί μόνο να τους θυμάται κανείς εύκολα αλλά και να τους μαντέψει! Οι επιθέσεις τύπου guessing ομοιάζουν και με το social engineering, όπου ο επιτιθέμενος επιδιώκει να αποκτήσει όσο το δυνατόν περισσότερες πληροφορίες από τον χρήστη.

Οι επιτιθέμενοι αρχικά δοκιμάζουν εύκολους και κοινούς κωδικούς, ως εκ τούτου, αδύναμοι κωδικοί είναι πιο ευάλωτοι σε αυτές τις επιθέσεις. Όταν δημιουργούμε έναν κωδικό πρέπει να αποφεύγουμε να χρησιμοποιούμε προσωπικά δεδομένα όπως η ημερομηνία γέννησης, ο τόπος κατοικίας, το όνομα του συζύγου ή των παιδιών κλπ.

Ο εισβολέας είναι πιθανό να χρησιμοποιεί εφαρμογή η οποία παράγει τυχαία PIN και κωδικούς οι οποίοι δοκιμάζονται σε κάποιο χρονικό διάστημα. Εάν το διάστημα αυτό είναι σύντομο η συσκευή μπορεί να απενεργοποιηθεί λόγω του αυξημένου αριθμού ανεπιτυχών προσπαθειών. Καθώς τα δάχτυλα αφήνουν ίχνη πάνω στη οθόνη αφής, είναι πιθανό να εντοπιστεί το μοτίβο που χρησιμοποιείται για το ξεκλείδωμα της συσκευής (Unlock pattern). Οι μέθοδοι αυθεντικοποίησης Face Unlock, NFC tags και Secure Lock δεν επιδέχονται καμίας μορφής εικασίας [149].

Στις επιθέσεις λεξιλογίου (dictionary attacks) χρησιμοποιείται μία λίστα με ευρέως διαδεδομένους κωδικούς ενώ στις brute force attacks χρησιμοποιούνται συνδυασμοί από πιθανούς χαρακτήρες. Και οι δύο αυτές μορφές επίθεσης είναι από κοινού υβριδικές επιθέσεις. Τροποποιήσεις όπως η προσθήκη ενός χαρακτήρα, η εναλλαγή κεφαλαίων μικρών γραμμάτων στους κωδικούς, γίνονται από έναν πιθανό κατάλογο κωδικών. Οι επιθέσεις dictionary και brute-force γίνονται αυτόματα, το οποίο τις διαφοροποιεί από την κατηγορία των επιθέσεων guessing [149].

4.1.3 False Identity Attack

Οι εισβολείς μπορούν να παραπλανούν τους αυθεντικούς χρήστες παρουσιάζοντας τους ψεύτικη ταυτότητα. Στις επιθέσεις spoofing κάποιος χρησιμοποιεί πλαστά δεδομένα και παρουσιάζεται ψευδώς σαν ένας άλλος χρήστης. Το Email spoofing, IP spoofing, website spoofing και referrer spoofing είναι παραδείγματα διαφόρων μορφών απάτης.

Για παράδειγμα, η δημιουργία μίας πλαστής ιστοσελίδας που θα είναι πανομοιότυπη με μία αυθεντική ιστοσελίδα είναι το γνωστό σε όλους website spoofing. Ο στόχος αυτής της πρακτικής είναι να αποσπάσει ευαίσθητα δεδομένα όπως π.χ. τα στοιχεία της πιστωτικής κάρτας του χρήστη. Μια ιδιαίτερη μορφή αυτής της επίθεσης είναι η επίθεση man-in-the-middle. Σε αυτή τη μορφή spoofing γίνεται μία ανεξάρτητη σύνδεση από τον εισβολέα μεταξύ χρήστη και server. Ο επιτιθέμενος μπορεί να ελέγχει τα δύο συνδεόμενα μέρη εφόσον δύναται να παρεμβαίνει στην μεταξύ τους επικοινωνία. Με αυτό τον τρόπο αποκτά πρόσβαση σε ευαίσθητες πληροφορίες ακόμα και αν αυτές είναι κρυπτογραφημένες. Λαμβάνοντας όλα αυτά υπόψιν, το phishing μπορεί να θεωρηθεί ως πρόβλημα καθώς η ευρεία εφαρμογή του δίνει μία ψεύτικη εικόνα πιστοποίησης και αναγκάζει τον χρήστη να αποκαλύψει τα δεδομένα του. Όσον αφορά τις κινητές συσκευές οι επιθέσεις man-in-the-middle attack δεν είναι κατάλληλες [149]. Για το spoofing υπάρχει περαιτέρω ανάλυση παρακάτω.

4.1.4 Physical attacks και Duplicates

Παραδείγματα φυσικών επιθέσεων είναι η κλοπή και ο κλώνος (Theft and duplicates). Πράγματα τα οποία μας ανήκουν μπορούν να κλαπούν από εμάς η να κλωνοποιηθούν. Οι εισβολείς δεν μπορούν να κλέψουν κάτι από εμάς το οποίο βρίσκεται στο μυαλό μας όπως ένας κωδικός αλλά μπορεί να κλέψουν μια smart card, ένα token ή ένα smartphone. Ένας κωδικός μπορεί να κλαπεί μόνο αν το γράψουμε κάπου για παράδειγμα σε ένα κομμάτι χαρτί. Κάτι που μπορεί να συμβεί και χωρίς την θέληση μας. Αυτό επίσης είναι εφικτό και για την κλωνοποίηση.

Είναι πιθανό να κλωνοποιήσουμε την φωτογραφία ξεκλειδώματος με αναγνώριση προσώπου και τα nfc tags. Είναι επίσης πιθανό να παρακάμψεις το ξεκλείδωμα προσώπου χρησιμοποιώντας μια φωτογραφία του νόμιμου χρήστη. Σε περίπτωση για παράδειγμα κλοπής του laptop και του κινητού τηλεφώνου του χρήστη είναι πιθανό να έχεις πρόσβαση στις φωτογραφίες του ιδιοκτήτη του κινητού (από το laptop) οι οποίες μπορούν να χρησιμοποιηθούν αργότερα για την αυθεντικοποίηση του εισβολέα στη συσκευή [149].

4.1.5 Dumpster diving

Το dumpster diving είναι η περίπτωση κατά την οποία ο χρήστης γράφει κάπου τον κωδικό του και αργότερα το πετάει. Ένας εισβολέας μπορεί να κρατήσει το χαρτί και να το χρησιμοποιήσει ώστε να εισάγει τα δεδομένα στη συσκευή. Αυτό είναι εφικτό στις περιπτώσεις του pin ή του password ενώ στις περιπτώσεις των nfc tags είναι σχεδόν απίθανο ο χρήστης να πετάξει τα tags του [149].

4.1.6 Unawareness

Η άγνοια του χρήστη είναι κίνδυνος ασφαλείας σε πολλές περιπτώσεις. Πολλοί χρήστες δεν θεωρούν ότι είναι απαραίτητο να περιφρουρούν τις συσκευές τους με κλείδωμα της συσκευής. Θεωρούν ότι οι συσκευές τους είναι ασφαλής με μόνο το γεγονός ότι της κουβαλούν μαζί τους. Η άγνοια είναι επίσης πρόβλημα στη περίπτωση που χρησιμοποιούνται ακατάλληλα pin ή password για την αυθεντικοποίηση του χρήστη. Με τον όρο ακατάλληλα εννοούμε την χρήση ενός αδύναμου pin ή password το οποίο είναι πολύ εύκολο να το μαντέψεις ή να το καταλάβεις εύκολα όταν τον εισάγει ο χρήστης (shoulder surf). Τα μοτίβο ξεκλειδώματος μπορεί επίσης να έχουν το ίδιο πρόβλημα όταν δεν επιλέγονται σχολαστικά και μπορεί κάποιος να τα ανακαλύψει εύκολα. Τα face unlock, nfc tags και security lock έχουν λιγότερα προβλήματα με το θέμα της άγνοιας του χρήστη [149].

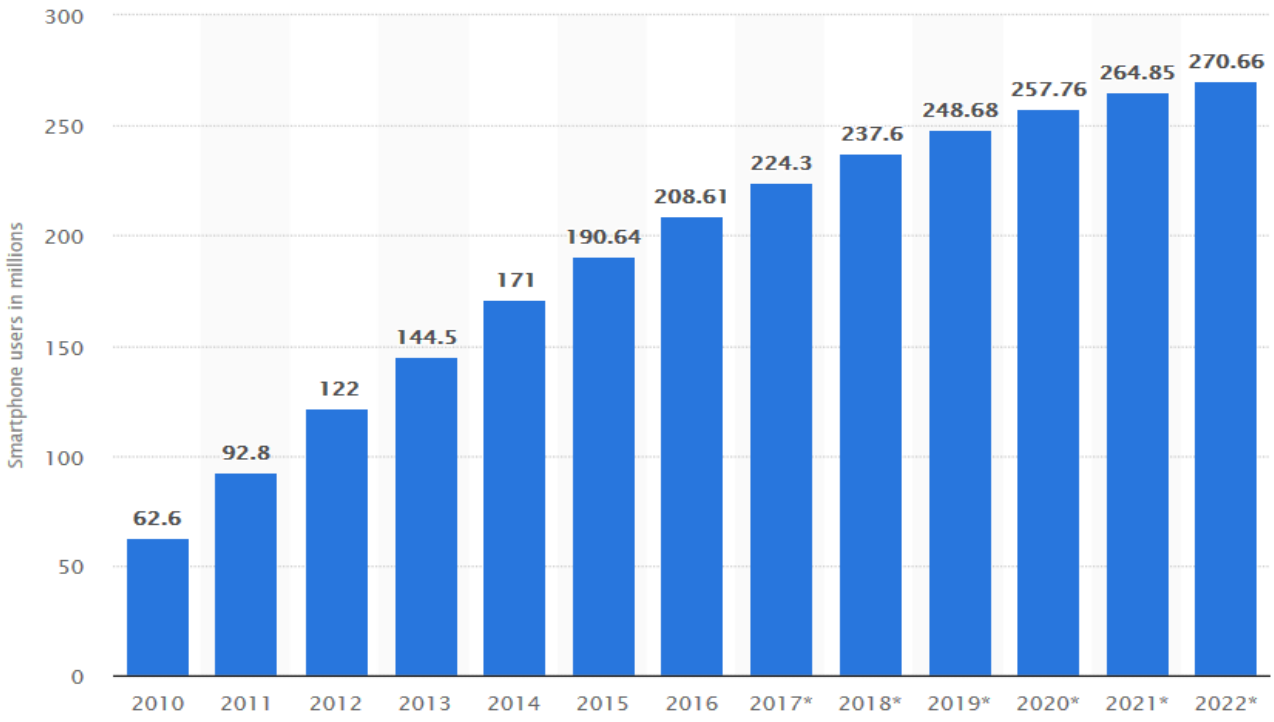
4.1.7 User studies

Η ανάγκη για συνεχής αυθεντικοποίηση (continuous authentication) μπορεί να παρατηρηθεί μέσα από δύο έρευνες χρηστών [154]. Σύμφωνα με αυτές τις έρευνες, έχει αποδειχθεί ότι σχεδόν όλοι οι συμμετέχοντες ανησυχούν για τα αποθηκευμένα δεδομένα στα τηλέφωνά τους ενώ οι περισσότεροι έχουν παρατηρήσει κάποιου άλλου χρήστη το PIN κάτι που δείχνει, ότι οι υπάρχοντες μηχανισμοί ελέγχου αυθεντικοποίησης δεν είναι αρκετά ισχυροί. Έτσι, οι έρευνες έδειξαν την αναγκαιότητα για την ανάπτυξη εναλλακτικών λύσεων εκτός των κλασσικών όπως το PIN ή το μοτίβο. Στην πρώτη έρευνα έλαβαν μέρος 47 συμμετέχοντες ενός Πανεπιστημίου και στην δεύτερη έρευνα που διεξήχθη online πήραν μέρος 267 συμμετέχοντες [154]. Και οι δύο έρευνες είχαν εστιάσει στη χρήση της κινητής συσκευής και τη χρήση των μηχανισμών αυθεντικοποίησης από τους συμμετέχοντες. Έχει διαπιστωθεί από μελέτες ότι οι περισσότεροι από τους συμμετέχοντες τηρούν τα τηλέφωνα τους κλειδωμένα με τη βοήθεια κάποιου μηχανισμού αυθεντικοποίησης. Τα ποσοστά αυτά ήταν 87% στην πρώτη μελέτη και 82% στη δεύτερη. Και στις δύο έρευνες, οι περισσότεροι από τους συμμετέχοντες ανησυχούσαν για κάποιον τρίτο που θα είχε πρόσβαση στα δεδομένα του κατά την απουσία του (55% για την πρώτη έρευνα και 71% στην δεύτερη έρευνα). Επιπλέον, 73% των συμμετεχόντων στην δεύτερη έρευνα παρατήρησαν το PIN από έναν φίλο ή ένα μέλος της

οικογένειας και το 79% δήλωσε ότι γνώριζαν το PIN κάποιου άλλου. Αυτό εγείρει μια ερώτηση σχετικά με την ασφάλεια των υφιστάμενων μηχανισμών αυθεντικοποίησης.

Έχει παρατηρηθεί ότι οι περισσότεροι χρήστες ανησυχούν για την προστασία των προσωπικών δεδομένων τους και χρησιμοποιούν κάποιο μηχανισμό αυθεντικοποίησης για τις κινητές συσκευές τους. Είναι ενδιαφέρον, ότι στη δεύτερη μελέτη έχει διαπιστωθεί ότι οι περισσότεροι από τους χρήστες είχαν κοιτάξει το PIN κάποιου άλλου κάποια στιγμή [154].

Το παρακάτω γράφημα (Εικόνα 14) δείχνει την αύξηση των χρηστών κινητής τηλεφωνίας από το 2007. Το γράφημα δίνει σαφή αύξηση των χρηστών κινητής τηλεφωνίας στον κόσμο και ότι αυτός έχει ξεπεράσει τον αριθμό των χρηστών desktop μετά το 2014 και συνεχίζει να αυξάνεται.



Εικόνα 14: Αριθμός κινητών τηλεφώνων στις ΗΠΑ από το 2010 έως το 2022 (σε εκατομμύρια) [155]

Στη συνέχεια ακολουθεί ο Πίνακας 7 με τους γνωστούς μεθόδους αυθεντικοποίησης και την χρήση του κάθε τρόπου και τα γνωστά προβλήματα της κάθε μεθόδου.

Μέθοδος Αυθεντικοποίησης	**Χρήση**	**Προβλήματα**
PIN	Συνήθως εισάγεται ένας 4-ψήφιος μυστικός αριθμός για αυθεντικοποίηση στο smartphone.	- Χρειάζεται να απομνημονεύεται - Εύκολο να το μαντέψει ο εισβολέας
Κωδικός πρόσβασης	Γενικά, 6 έως 12 χαρακτήρες αλφαριθμητικοί για αυθεντικοποίηση στο smartphone	- Πιο δύσκολο να απομνημονευθούν από το PIN - Δύσκολο να πληκτρολογηθούν - Παίρνει περισσότερο χρόνο να τα πληκτρολογήσετε σε σύγκριση με τα PIN
Μοτίβο	Ένα σχέδιο που πρέπει να «ζωγραφιστεί» στην οθόνη του smartphone για αυθεντικοποίηση	- Χρειάζεται να απομνημονεύεται - Εύκολο να το μαντέψει ο εισβολέας - Αφήνει στίγματα στην οθόνη, τα οποία συνήθως διευκολύνουν κάποιον εισβολέα να το μαντέψει
Δακτυλικά αποτυπώματα	Ένας σαρωτής διαβάζει το δακτυλικό αποτύπωμα και επιτρέπει στο χρήστη να πραγματοποιήσει έλεγχο αυθεντικοποίησης στο smartphone	- Βρώμικο δάχτυλο / σαρωτής οδηγεί σε αποτυχία αυθεντικοποίησης - Βρεγμένα χέρια, γάντια κλπ. αποτελούν εμπόδιο για αυθεντικοποίηση
Αναγνώριση προσώπου	Μια εικόνα του χρήστη συλλαμβάνεται από την κάμερα του κινητού και συγκρίνεται με μία προηγούμενη-αρχική εικόνα του χρήστη. Ταύτιση των δύο εικόνων δίνει αυθεντικοποίηση	- Ο έλεγχος ταυτότητας δεν είναι εφικτός σε σκοτεινά μέρη - Μια απλή εικόνα του χρήστη μπορεί να χρησιμοποιηθεί από τους επιτιθέμενους και μπορεί να οδηγήσει σε μη εξουσιοδοτημένη αυθεντικοποίηση
Αναγνώριση ίριδας	Η ίριδα ενός χρήστη θα πρέπει να σαρωθεί από μια ισχυρή κάμερα και εν συνεχεία το συγκρίνουμε με την αρχική ίριδα μοτίβο	-Οι χρήστες με γυαλιά αντιμετωπίζουν προβλήματα -το φωτεινό φως του ήλιου μπορεί να προκαλέσει πρόβλημα

	του χρήστη, για την αυθεντικοποίηση	- σχετικά ακριβή τεχνολογία και εισάγεται στα ακριβά μοντέλα κινητών τηλεφώνων
Αναγνώριση ομιλητή (φωνής)	Η φωνή του χρήστη και ένα ηχογραφημένο δείγμα συγκρίνεται για αυθεντικοποίηση	-Δεν είναι κατάλληλη σε ένα περιβάλλον όπου ο χρήστης πρέπει να παραμείνει ήσυχος (να μην μιλάει) -Ομοίως, εξωτερικός θόρυβος μπορεί να επηρεάσει την αυθεντικοποίηση

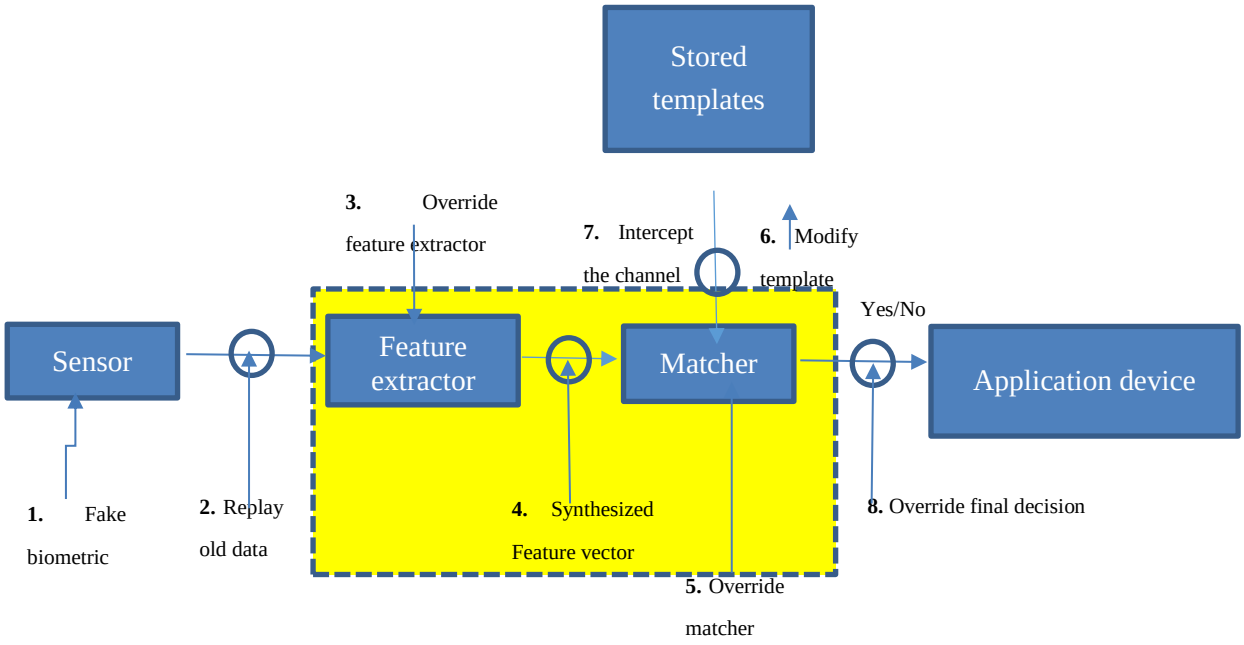
Πίνακας 7: Μέθοδοι Αυθεντικοποίησης στα κινητά τηλέφωνα

4.2 *Επιθέσεις εναντίον Βιομετρικών Συστημάτων*

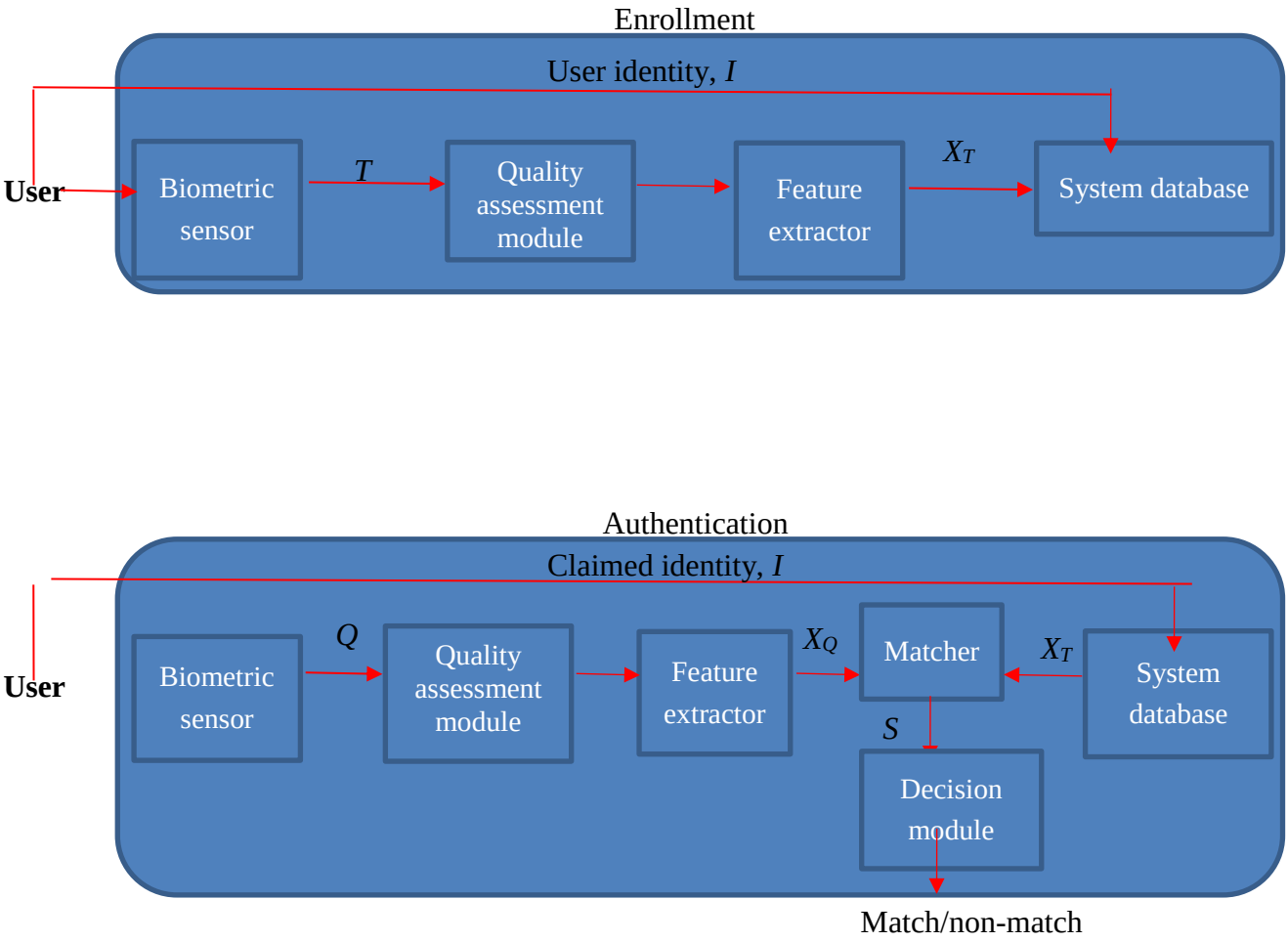
Οκτώ πιθανά διαφορετικά σημεία που μπορούν να επηρεάσουν την ασφάλεια των βιομετρικών συστημάτων έχουν προσδιοριστεί σε έρευνα [156] όπως περιγράφεται παρακάτω:

1. ένα ψεύτικο βιομετρικό χαρακτηριστικό μπορεί να υποβληθεί στον αισθητήρα όπως ένα ψεύτικο δάχτυλο, ένα αντίγραφο μιας υπογραφής ή μια μάσκα προσώπου.
2. ψηφιακά αποθηκευμένα βιομετρικά δεδομένα μπορεί να υποβληθούν εκ νέου στο σύστημα. Σε αυτό του είδους τις επιθέσεις, ένα προ-καταγεγραμμένο βιομετρικό δεδομένο επαναλαμβάνεται (replayed) στο σύστημα παρακάμπτοντας τον αισθητήρα, μια επίθεση που ονομάζεται επίσης ως "replay attack". Για παράδειγμα, παρουσιάζοντας ένα ψηφιακό αντίγραφο της εικόνας των δακτυλικών αποτυπωμάτων ή ένα εγγεγραμμένο ηχητικό σήμα ενός ομιλητή.
3. το χαρακτηριστικό extractor μπορεί να προσβληθεί με ένα πρόγραμμα Trojan το οποίο παράγει προκαθορισμένα σύνολα χαρακτηριστικών γνωρισμάτων.
4. Νόμιμα χαρακτηριστικά sets που εξάγονται από το βιομετρικό εισόδου μπορεί να αντικατασταθούν με πλαστά χαρακτηριστικά sets. Για παράδειγμα, εάν μικρολεπτομέρειες των δακτυλικών αποτυπωμάτων διαβιβάζονται σε ένα απομακρυσμένο matcher (ας πούμε μέσω του Internet) τότε αυτή η απειλή είναι πραγματική.
5. Επίσης οι matcher, που παράγουν πάντα άμεσα ένα συγκεκριμένο αποτέλεσμα – ταύτιση (match), όχι ταύτιση ή ένα αριθμό ταύτισης μπορεί να προσβληθεί με ένα πρόγραμμα Trojan
6. τα εγγεγραμμένα πρότυπα στη βάση δεδομένων μπορεί να αφαιρεθούν ή να τροποποιηθούν, ή νέα πρότυπα να εισαχθούν στη βάση, τα οποία θα μπορούσαν να οδηγήσουν στην αυθεντικοποίηση για ένα δόλιο άτομο, ή τουλάχιστον σε άρνηση υπηρεσίας για το πρόσωπο που συνδέεται με το κατεστραμμένο πρότυπο.
7. τα εγγεγραμμένα πρότυπα στην αποθηκευμένη βάση δεδομένων που αποστέλλονται στο matcher μέσα από ένα κανάλι επικοινωνίας θα μπορούσε να δεχθεί επίθεση για να αλλαχθούν τα περιεχόμενα των πρότυπων, πριν φτάσουν στο matcher.
8. η οριστική απόφαση εξόδου από το βιομετρικό σύστημα μπορεί να παρακαμφθεί με την επιλογή του αποτελέσματος από έναν χάκερ. Ακόμη και αν το extraction και το match έχουν μια εξαιρετική απόδοση, μπορεί αυτό να πέσει σε αχρηστία από την απλή παράκαμψη του αποτελέσματος.

Στην Εικόνα 15 παρουσιάζω μια αναπαράσταση των 8 ειδών επιθέσεων.



Εικόνα 15: Σημεία επίθεσης σε ένα multimodal σύστημα



Εικόνα 16: Στάδια εγγραφής και αναγνώρισης σε ένα βιομετρικό σύστημα

Στην ανωτέρω Εικόνα 16 το T αντιπροσωπεύει το βιομετρικό δείγμα που λαμβάνεται κατά τη διάρκεια της εγγραφής, Q είναι το ερώτημα στο βιομετρικό δείγμα που λαμβάνεται κατά τη διάρκεια της αναγνώρισης, XT και XQ είναι το πρότυπο (template) και το ερώτημα (query) σύνολα χαρακτηριστικών γνωρισμάτων, αντίστοιχα, και S αντιπροσωπεύει το σκορ ταύτισης.

4.3 *Spoof Attacks*

Μεταξύ των πιθανών επιθέσεων που έχουν μελετηθεί στη βιβλιογραφία, αυτή με την μεγαλύτερη πρακτική αξία είναι η "spoof attack", η οποία συνίσταται στην υποβολή ενός κλεμμένου, αντιγραμμένου ή συνθετικά αναπαραγόμενου βιομετρικού χαρακτηριστικού στον αισθητήρα για να εξαπατήσει τα βιομετρικά συστήματα ασφαλείας προκειμένου να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Πρόσφατα, έχει αποδειχθεί ότι οι spoof attacks μπορούν να γίνουν ενάντια σε πολλές μορφές βιομετρικών στοιχείων, όπως δακτυλικά αποτυπώματα, πρόσωπο και ίριδα [157], [158], [159], [160]. Αυτού του είδους η επίθεση είναι επίσης γνωστή ως «άμεση επίθεση» ('direct attack'), δεδομένου ότι πραγματοποιείται άμεσα στο βιομετρικό αισθητήρα. Μία spoofing attack είναι μια

επίθεση τύπου 1 όπου ένα κλεμμένο, αντιγραμμένο βιομετρικό χαρακτηριστικό υποβάλλεται στον αισθητήρα για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο βιομετρικό σύστημα. Η επιτυχία μιας spoof attack είναι πολύ μεγαλύτερη από άλλου είδους επιθέσεις κατά των βιομετρικών συστημάτων, καθώς δεν απαιτεί οποιαδήποτε γνώση για το σύστημα, όπως το extract χαρακτηριστικό (extractor feature) ή τον αλγόριθμο ταύτισης (matcher) που χρησιμοποιείται. Τεχνικές ψηφιακής προστασίας όπως κατακερματισμός (hashing), η κρυπτογράφηση και η ψηφιακή υπογραφή, δεν είναι αποτελεσματικές λόγω της φύσης της spoof attack διότι γίνονται στον αναλογικό κομμάτι, έξω από τα ψηφιακά όρια του συστήματος.

Μέθοδοι «ζωντανών» (liveness) δοκιμών (ανίχνευση ζωτικότητας) έχουν προταθεί ως εφικτό αντίμετρο στις spoof attacks από πολλούς ερευνητές. Η ανίχνευση ζωτικότητας που έχει ως στόχο να εντοπίσει κατά πόσον το βιομετρικό χαρακτηριστικό που υποβλήθηκε είναι ζωντανό ή τεχνητό, γίνεται είτε από μονάδα λογισμικού (software) που βασίζεται στην επεξεργασία σήματος ή από υλικό (hardware) που έχει ενσωματωθεί στη συσκευή εισόδου [161], [162], [163], [164], [165], [166], [167].

Όμως, η επισκόπηση της βιβλιογραφίας επισημαίνει ότι μέχρι στιγμής δεν υπάρχει αποτελεσματική μέθοδος. Επιπλέον, υπάρχει παράπλευρη επίδραση όταν βιομετρικά συστήματα χρησιμοποιούν συνδυασμό με την ανίχνευση ζωτικότητας καθότι αυξάνεται το ποσοστό εσφαλμένης απόρριψης (false rejection rate (FRR)), δηλαδή το ποσοστό των αληθινών χρηστών που απορρίφθηκαν από το σύστημα. Άλλοι αλγόριθμοι ανίχνευσης spoof attacks έχουν προταθεί και για άλλα βιομετρικά χαρακτηριστικά, αλλά οι επιδόσεις τους επίσης δεν είναι ικανοποιητικές.

4.3.1 Fingerprint spoofing

Αξίζει να τονίσουμε ότι η ιδέα του fingerprint spoof χρησιμοποιώντας ένα αντιγραμμένο πλαστό αποτύπωμα δαχτύλου δεν είναι κάτι καινούριο.

Τα τελευταία χρόνια, αρκετές έρευνες έχουν διεξαχθεί για το πώς τα πλαστογραφημένα δακτυλικά αποτυπώματα μπορούν να παρακάμψουν τα τελευταίας τεχνολογίας συστήματα αναγνώρισης αποτυπωμάτων. Ερευνητές [168] εξέτασαν την ευαισθησία των αισθητήρων σε διαφορετικά δακτυλικά αποτυπώματα που συντίθεται από σιλικόνη και πλαστελίνη. Πέντε από τους έξι αισθητήρες επέτρεψαν τη μη εξουσιοδοτημένη πρόσβαση στο σύστημα με την πρώτη προσπάθεια, ενώ ο έκτος με την δεύτερη προσπάθεια.

Ο Matsumoto et al. [158], διεξάγοντας παρόμοια πειράματα κατέληξε [168], ότι τα ψεύτικα δακτυλικά αποτυπώματα που κατασκευάζονται με τη ζελατίνη είναι τα πιο αποτελεσματικά. Οι ερευνητές δοκίμασαν έντεκα αισθητήρες δακτυλικών αποτυπωμάτων, με ένα ποσοστό επιτυχίας άνω του 60%, ακόμη και όταν τα ψεύτικα δακτυλικά αποτυπώματα είχαν αναπαραχθεί από το λανθάνον δακτυλικό αποτύπωμα.

Ομοίως, εξετάστηκαν σε [169] συστήματα με διαφορετικούς γνωστούς αισθητήρες (συμπεριλαμβανομένων των συσκευών που παράγονται από Biometrika, Fujitsu, Identix, Siemens) δάχτυλα που είχαν κατασκευαστεί από υλικά και τεχνικές πλαστογράφησης.

Η υπάρχουσα βιβλιογραφία υποδηλώνει ότι το fingerprint spoofing μπορεί να ταξινομηθεί σε δύο ευρείες κατηγορίες: «συναινετικό/συνεργατικό/άμεσων εκμαγείων» και «μη-συναινετικό /μη-συνεργατικό /έμμεση εκμαγεία». Στη συναινετική μέθοδο, τα ψεύτικα δακτυλικά αποτυπώματα

δημιουργούνται με την συναίνεση και τη συνεργασία του ιδιοκτήτη των δακτυλικών αποτυπωμάτων. Στις μη συναινετικές μεθόδους η συνεργασία του χρήστη δεν είναι απαραίτητη, δεδομένου ότι τα δαχτυλικά αποτυπώματα του χρήστη υποκλέπτονται από κάποια επιφάνεια και χρησιμοποιούνται για να κατασκευαστούν τα πλαστογραφημένα αποτυπώματα. Αξίζει να σημειωθεί ότι οι περισσότερες ερευνητικές μελέτες έχουν διεξαχθεί χρησιμοποιώντας πλαστά δακτυλικά αποτυπώματα που κατασκευάζονται με τη συναινετική μέθοδο .

4.3.2 Face spoofing

Παρά την πρόοδο στα βιομετρικά συστήματα αναγνώρισης προσώπου, το face spoofing, γνωστό και ως "copy attack", εξακολουθεί να αποτελεί σοβαρή απειλή για την ασφάλεια του συστήματος. Οι μέθοδοι πλαστογράφησης προσώπου μπορεί να ποικίλλουν ανάλογα με το σύστημα αναγνώρισης στο οποίο θέλουν να επιτεθούν. Τα συστήματα αναγνώρισης προσώπου μπορούν να καταταχθούν σε δύο ομάδες: (δισδιάστατα) 2D και 3D (τρισδιάστατα) συστήματα.

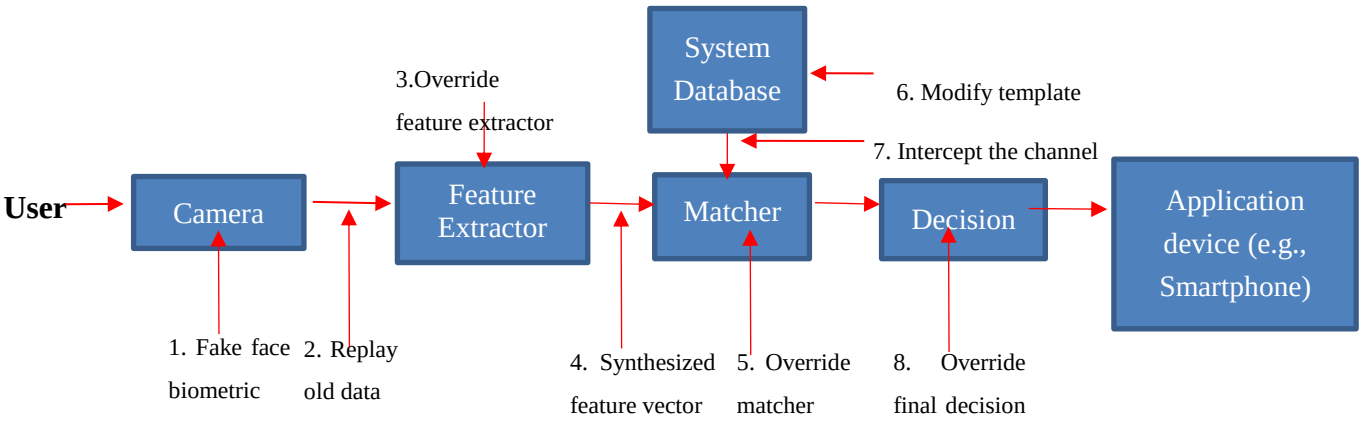
Ένα σύστημα αναγνώρισης προσώπου 2D λαμβάνει υπόψη εικόνες του προσώπου μόνο δύο διαστάσεων. Τα συστήματα 3D είναι σαφώς πιο περίπλοκα, και αναγνωρίζουν πρόσωπα βάσει χαρακτηριστικών που προέρχονται από όλο το πρόσωπο, χρησιμοποιώντας μεθόδους όπως paraxial view ή patterned illumination light [170]. Τυπικά, τα συστήματα αναγνώρισης προσώπου μπορούν να πλαστογραφηθούν, με τρείς τρόπους (i) με μια φωτογραφία, (ii) με ένα βίντεο, ή (iii) με ένα 3D αντίγραφο του κανονικού χρήστη.

Η επίθεση face spoof μέσω φωτογραφίας ή του βίντεο είναι η πιο κοινή, η φθηνότερη και η ευκολότερη μέθοδος να παρακαμφθούν τα συστήματα αναγνώρισης προσώπου [163], [171]. Οι spoof attacks μέσω φωτογραφίας, γνωστές ως "photo-attacks", γίνονται όταν υποβάλουν μια φωτογραφία του νόμιμου χρήστη στο σύστημα αναγνώρισης προσώπου, εμφανίζοντας την έντυπη ή στην οθόνη ενός φορητού υπολογιστή ή σε ένα κινητό τηλέφωνο [163], [171] . Το πρόσωπο είναι φανερό άρα και ευκολότερο να αποτυπωθεί σε μία φωτογραφία π.χ. χρησιμοποιώντας εν αγνοία του χρήστη απομακρυσμένες κάμερες. Επιπλέον, λόγω της κυκλοφορίας προσωπικών φωτογραφιών στα μέσα κοινωνικής δικτύωσης πολλοί χρήστες είναι εύκολα προσβάσιμοι στο ευρύ κοινό. Το ίδιο συμβαίνει και με την απόκτηση βίντεο που περιλαμβάνει το πρόσωπο του χρήστη. [172]

Στα συστήματα αναγνώρισης προσώπου 3D, το πρόσωπο μπορεί να πλαστογραφηθεί με τη χρήση κατασκευασμένων προσώπων από ελαστικό, πλαστικό ή σιλικόνη [171] . Προϋπόθεση για να εξαπατηθεί ένα συστήματα 3D πρέπει το ομοίωμα που θα παρουσιαστεί στην κάμερα να είναι τρισδιάστατο, καθιστώντας έτσι τη 3D πλαστογράφηση πιο περίπλοκη από ό, τι τη 2D. Λόγω της ευκολίας του spoof attack σε 2D συστήματα οι "photo attacks" και "video attacks" εξακολουθούν να είναι πιο κοινές τεχνικές του face spoofing [173].

Πρόσφατες έρευνες έδειξαν ότι ακόμη και οι ναυαρχίδες κάθε εταιρείας μπορεί εύκολα να πέσουν θύματα αυτού του είδους της επίθεσης. Το face ID του iPhone X μπορεί να εξαπατηθεί με μία 3D εκτυπωμένη μάσκα κόστους μόλις 150 $ [174] ενώ η τεχνολογία αναγνώρισης προσώπου του Samsung S8 εξαπατήθηκε απλά με την χρήση μιας φωτογραφίας του ιδιοκτήτη του κινητού τηλεφώνου [175]. Ομοίως η German Chaos Computer Club κατάφερε να «σπάσει» τον αισθητήρα ίριδας του Samsung Galaxy S8 με ένα ψεύτικο μάτι που φτιάχτηκε από φωτογραφία της ίριδας, η οποία λήφθηκε από κάμερα με νυχτερινή λήψη, και καλύφθηκε με ένα φακό επαφής για να ταιριάζει

η καμπυλότητα του ματιού [176]. Ο ερευνητής Isao Echizen του Japan National Institute of Informatics (NII) έδειξε ότι τα δαχτυλικά αποτυπώματα μπορούν εύκολα να δημιουργηθούν ακόμη και από μία φωτογραφία που πάρθηκε από απόσταση τριών μέτρων χωρίς να είναι απαραίτητη η χρήση οποιουδήποτε εξειδικευμένης διαδικασίας και προειδοποίησε όσους κάνουν το σήμα της ειρήνης μπροστά σε φωτογράφους ότι αποτελεί ένα κίνδυνο ασφαλείας για τους ιδίους καθότι κακόβουλοι χρήστες μπορούν εύκολα να ανακατασκευάσουν το αποτύπωμα τους [177]. Στην Εικόνα 17 φαίνονται τα πιθανά σημεία επίθεσης σε ένα σύστημα face verification.



Εικόνα 17: Σημεία επίθεσης σε ένα σύστημα face verification

4.3.3 Η ανθεκτικότητα των πολυτροπικών βιομετρικών συστημάτων ενάντια στις επιθέσεις spoof

Τα πολυτροπικά βιομετρικά συστήματα θεωρούνται ως ένας αμυντικός μηχανισμός ενάντια σε επιθέσεις πλαστογράφησης (επιθέσεις spoof). Έχουν προταθεί αρχικά προκειμένου να ξεπεράσουν τις αδυναμίες και ορισμένους εγγενείς περιορισμούς που έχουν τα μονοτροπικά συστήματα, όσον αφορά την αυθεντικοποίηση του χρήστη. Η αποτελεσματικότητα τους είναι αποδεδειγμένη από θεωρητικές και εμπειρικές αποδείξεις [178], [179]. Επιπλέον, έχει αποδειχθεί ότι είναι αρκετά ισχυρή μέθοδος υπό συνθήκες στρες ή κακής συνεργασίας του χρήστη (π.χ., φορώντας γυαλιά ή γενειάδα) [180]. Επίσης, τα πολυτροπικά συστήματα είναι εγγενώς πιο ανθεκτικά στις επιθέσεις πλαστογράφησης από ό, τι τα συστήματα που χρησιμοποιούν ένα μοναδικό βιομετρικό χαρακτηριστικό [181], [182], [51]. Η πεποίθηση αυτή βασίζεται στην παραδοχή ότι ένας εισβολέας πρέπει να εξαπατήσει όλα τα βιομετρικά στοιχεία ταυτόχρονα ώστε να προσπεράσει το πολυτροπικό σύστημα [182], [51], [160]. Μια τέτοια επίθεση θα απαιτούσε περισσότερη προσπάθεια και περισσότερο χρόνο και αυτός είναι ένας αποτρεπτικός παράγοντας για να επιχειρηθεί η επίθεση.

Ωστόσο, αυτή η υπόθεση δεν βασίζεται σε θεωρητικά συμπεράσματα ή εμπειρικές αποδείξεις, αλλά μόνο σε επιχειρήματα, τα οποία βασίζονται κυρίως στην υψηλότερη απόδοση των πολυτροπικών συστημάτων σε σχέση με των μονοτροπικών. Ωστόσο, ορισμένες πρόσφατες μελέτες, σε αντίθεση με την κοινή πεποίθηση, έδειξαν ότι η πλαστογράφηση ενός μόνο βιομετρικού χαρακτηριστικού

μπορεί να είναι επαρκής για να παρακαμφθεί το σύστημα, ακόμα και από όταν χρησιμοποιούνται περισσότερα από δύο βιομετρικά χαρακτηριστικά [183], [184], [185]. Τα συστήματα που δοκιμάστηκαν αποτελούνταν από δύο (πρόσωπο και το δακτυλικό αποτύπωμα) [183], [184] ή τρία βιομετρικά χαρακτηριστικά (πρόσωπο, δακτυλικό αποτύπωμα και την ίριδα) [185]. Πράγματι, παρατηρήθηκε μια ουσιώδης αύξηση του false acceptance rate (FAR) από τα συστήματα που δέχονταν επιθέσεις. Ωστόσο, τα περισσότερα από τα αποτελέσματα [183], [184], [185] προέκυψαν κάτω από τη μη ρεαλιστική και αυστηρή υπόθεση (γνωστό ως "worst- case" σενάριο) ότι ο εισβολέας είναι σε θέση να κατασκευάσει ένα τέλειο αντίγραφο του βιομετρικού χαρακτηριστικού του γνήσιου χρήστη του οποίου ο βαθμός ταύτισης είναι πανομοιότυπος με εκείνο του γνήσιου χαρακτηριστικού.

Αξίζει να σημειωθεί ότι [184] μερικά πειράματα έχουν πραγματοποιηθεί χρησιμοποιώντας κομμάτια από πραγματικά πλαστογραφημένα δακτυλικά αποτυπώματα από το Fingerprint Liveness Detection Competition (LivDet09) [186]. Το σκορ ταύτισης των πλαστών δακτυλικών αποτυπωμάτων που λήφθηκαν στη μελέτη ήταν σημαντικά διαφορετικό από αυτό των πραγματικών αποτυπωμάτων κάτι που αποδεικνύει ότι το "worst-case scenario" δεν είναι ρεαλιστικό για όλα τα βιομετρικά χαρακτηριστικά και τις τεχνικές πλαστογράφησης.

Έτσι, στα [183], [184], [185] και [187] εγείρεται το ζήτημα της περεταίρω διερεύνησης της ανθεκτικότητας των πολυτροπικών συστημάτων ενάντια στις αληθινές επιθέσεις spoof, κοινώς στην περίπτωση του "non-worst scenario" (όταν το ψεύτικα χαρακτηριστικά δεν είναι ακριβή αντίγραφα των γνησίων) και ανακάλυψης νέων μεθόδων στο σχεδιασμό πιο ανθεκτικών σε spoof επιθέσεις, πολυτροπικών βιομετρικών συστημάτων.

4.3.4 Ανοιχτά ζητήματα όσον αφορά την ανθεκτικότητα των πολυτροπικών βιομετρικών συστημάτων ενάντια στις επιθέσεις spoof

Μολονότι, τα πολυτροπικά βιομετρικά συστήματα προσφέρουν αρκετά πλεονεκτήματα όπως η μεγαλύτερη ακρίβεια αναγνώρισης, η αυξημένη πληθυσμιακή κάλυψη και η μεγαλύτερη ευελιξία, το πρόβλημα της αξιολόγησης της επίδοσης των πολυτροπικών βιομετρικών συστημάτων, τόσο από την άποψη της ικανότητας γενίκευσης όσο και της ανθεκτικότητας ενάντια σε επιθέσεις spoof, αποτελεί ένα ανοικτό ερευνητικό πρόβλημα. Τα κύρια προβλήματα που δεν έχουν ακόμη επιλυθεί για να διασφαλίσουμε ένα ασφαλές πολυτροπικό βιομετρικό σύστημα αναγνώρισης περιλαμβάνουν:

(α) μπορεί τα πολυτροπικά βιομετρικά συστήματα να παραβιαστούν επιτιθέμενα μόνο σε έναν αισθητήρα μέσω πραγματικών επιθέσεων;

Η ανθεκτικότητα των πολυτροπικών βιομετρικών συστημάτων έχει αμφισβητηθεί πρόσφατα στο [183], [184], [185], δείχνοντας ότι, σε ορισμένα σενάρια εφαρμογής, μπορούν να παραβιαστούν από spoofing ενός μόνο από τα απαιτούμενα βιομετρικά χαρακτηριστικά. Ωστόσο, το πεδίο εφαρμογής των αποτελεσμάτων αυτών είναι πολύ περιορισμένο, δεδομένου ότι αυτά αποκτήθηκαν κάτω από τη μη ρεαλιστική υπόθεση, γνωστή ως "worst-case scenario" όπου υποτίθεται ότι ο εισβολέας είναι σε θέση να κατασκευάσει ένα τέλειο αντίγραφο ενός βιομετρικού χαρακτηριστικού

του οποίου το σκορ ταύτισης είναι πανομοιότυπο με εκείνο του γνήσιου χαρακτηριστικού. Ωστόσο, εάν τα αποτελέσματα αυτά [183], [184], [185] πραγματοποιηθούν σε πιο ρεαλιστικά σενάρια εφαρμογής, αυτό συνεπάγεται ότι τα πολυτροπικά συστήματα είναι απλά ένας αποτρεπτικός παράγοντας και όχι μια πραγματική άμυνα ενάντια σε επιθέσεις spoof. Από την άλλη πλευρά, μια πιο ευρεία και ρεαλιστική αξιολόγηση θα μπορούσε να επισημάνει τις προϋποθέσεις υπό τις οποίες τα πολυτροπικά βιομετρικά συστήματα αποτελούν μια αποτελεσματική άμυνα. Με άλλα λόγια, είναι ακόμα σημαντικό να διερευνήσει κατά πόσον το συμπέρασμα που προέκυψε από τα αποτελέσματα [183], [184], [185] ότι δηλαδή, τα πολυτροπικά βιομετρικά συστήματα δεν είναι εγγενώς πιο ισχυρά ενάντια σε επιθέσεις spoof, αλλά μπορούν να σταθούν επίσης σε ρεαλιστικά σενάρια.

(β) είναι το "worst-case " σενάριο που τέθηκε στο [183], [184], [185] σχετικό με τις πραγματικές επιθέσεις spoof ;

Πρόσφατα έρευνες [183], [184], [185] έδειξαν ότι τα πολυτροπικά βιομετρικά συστήματα μπορεί να είναι ιδιαίτερα ευάλωτα σε spoof επιθέσεις, σύμφωνα με το σενάριο υπόθεσης "worst-case" . Ωστόσο, το σενάριο αυτό δεν μπορεί να γενικευθεί για όλα τα βιομετρικά χαρακτηριστικά, όπως γίνεται φανερό από το [184]. Πράγματι απαιτείται μια πιο συστηματική και ευρεία ανάλυση.

(γ) πώς μπορεί η ασφάλεια των πολυτροπικών συστημάτων να αξιολογηθεί υπό ρεαλιστικές επιθέσεις;

Μια εύκολη προσέγγιση για να αξιολογηθεί η ασφάλεια των πολυτροπικών βιομετρικών συστημάτων ενάντια στις ρεαλιστικές επιθέσεις spoof είναι να κατασκευαστούν πλαστά βιομετρικά χαρακτηριστικά και να τα υποβληθούν στο σύστημα για να ελεγχθεί πιθανή ευπάθεια. Ωστόσο, η κατασκευή ψεύτικων βιομετριών χαρακτηριστικών είναι μια χρονοβόρα και περίπλοκη διεργασία, επομένως και μη πρακτική για το σχεδιαστή του συστήματος [186]. Μια πιθανή εναλλακτική λύση είναι η ανάπτυξη μεθόδων που βασίζονται σε προσομοίωση των πλαστογραφημένων βιομετρικών χαρακτηριστικών. Ο στόχος της ανάπτυξης είναι διττός: πρέπει να (α) αξιολογηθεί η ανθεκτικότητα των πολυτροπικών συστημάτων και (β) να σχεδιαστούν νέοι πολυτροπικοί κανόνες, ισχυροί σε spoof επιθέσεις. Ειδικότερα, είναι ζωτικής σημασίας να αναπτυχθούν μέθοδοι αξιολόγησης που μπορεί να εφαρμοστούν σε οποιοδήποτε πολυτροπικό σύστημα. Επιπλέον, μπορεί να είναι χρήσιμο να συγκρίνεται η ανθεκτικότητα του σκορ διαφορετικών πολυτροπικών κανόνων που εφαρμόζονται σε ένα συγκεκριμένο πολυτροπικό σύστημα. Ωστόσο, μέχρι σήμερα καμία προσπάθεια δεν έχει διεξαχθεί προς αυτή την κατεύθυνση.

4.4 *Νεότερες επιθέσεις και πιθανές άμυνες σε συμπεριφορικά βιομετρικά*

Η [188] ασχολείται με επιθέσεις στο keystroke dynamics λαμβάνοντας κυρίως υπόψη την πλευρά του επιτιθέμενου. Αναλύονται δύο μέθοδοι, το Targeted K-means++ το οποίο είναι πιο ακριβό αλλά πάρα πολύ αποτελεσματικό από την πλευρά του επιτιθέμενου και το Indiscriminate K-means++ το οποίο δεν είναι τόσο ισχυρό αλλά δεν απαιτείται καμία έξτρα ενέργεια από τον επιτιθέμενο (δεν απαιτείται να συλλεχθούν δείγματα) και δεν προσθέτει έξτρα κόστος σε αυτόν. Με το Targeted K-means++ κατάφεραν να ξεγελάσουν το κινητό τηλέφωνο σε ποσοστό 40-70% των

χρηστών μέσα σε πολύ 10 προσπάθειες. Από την άλλη με το Indiscriminate K-means++ η ασφάλεια του κινητού παρακάμφθηκε σε ποσοστό 30-50%.

Στο [189] χρησιμοποιούν ένα νέο εκπαιδευτικό υποσύστημα που το αποκαλούν Mimesis για το Keystroke dynamics. Το Mimesis παρέχει τόσο θετικό όσο και αρνητικό feedback στις διαφορές μεταξύ του υποβληθέντος δείγματος και του δείγματος αναφοράς. Αυτό επιτρέπει σε ένα άτομο να μιμηθεί ένα άλλο προσαρμόζοντας σταδιακά τον τρόπο πληκτρολόγησης του. Ακόμη και σε περιπτώσεις που ο τρόπος γραφής του χρήστη ήταν μόνο μερικώς γνωστός, με βοήθεια και εκπαίδευση από το Mimesis ο επιτιθέμενος κατάφερνε να ξεγελάσει το σύστημα. Οι συγκεκριμένοι κάνανε μια έρευνα όπου 84 συμμετέχοντες έπαιξαν τον ρόλο του επιτιθέμενου για δύο 8ψήφιους κωδικούς και ανάλογα με την ευκολία ή μη του κωδικού πέτυχαν FAR από 0.24 έως 0.20 (πριν την εκπαίδευση με το Mimesis) και από 0.63 έως 0.42 μετά την εκπαίδευση με το Mimesis με μερικές πληροφορίες σχετικά με το θύμα. Με πλήρης πληροφορίες για ο θύμα το FAR αυξάνεται σε 0,99 για τους καλύτερους 14 επιτιθέμενους. Άλλα ενδιαφέροντα ευρήματα ήταν ότι όσο ευκολότερος είναι ο κωδικός τόσο ευκολότερη είναι η μίμηση. Επίσης οι άνδρες ήταν καλύτεροι στη μίμηση από τις γυναίκες.

Στο [190] παρουσιάζονται δύο ειδών ρομποτικές επιθέσεις με στόχο την αυθεντικοποίηση με βάσει την αφή: μια τυχαία στατιστική επίθεση γενικού πληθυσμού και μια προσαρμοσμένη πάνω σε συγκεκριμένο χρήστη. Η στατιστική επίθεση βασίζεται σε πρότυπα που έχουν εξαχθεί από μεγάλους πληθυσμούς ενώ η προσαρμοσμένη στο χρήστη σε δείγματα που έχουν υποκλαπεί από τον χρήστη. Όλες οι επιθέσεις γίνονται από ένα ρομπότ που είναι εκπαιδευμένο στο πώς να κινείται πάνω σε μία οθόνη αφής κινητού τηλεφώνου. Πέτυχαν FAR από 0.17 έως 0.32 . Επειδή η συγκεκριμένη επίθεση απαιτεί βασικές μόνο προγραμματιστικές δεξιότητες και χρήση φτηνού εξοπλισμού αποτελεί ένα πολύ ρεαλιστικό σενάριο επίθεσης σε αυθεντικοποίηση μέσω αφής. Σαν πιθανές λύσεις από τους συγγραφείς παρουσιάζεται ο συνδυασμός (fusion) πολλαπλών βιομετρικών χαρακτηριστικών καθώς επίσης και η εισαγωγή αισθητήρων για αναγνώριση ζωτικότητας ώστε να ξεχωρίζει ένα ρομπότ από ένα άνθρωπο.

Στο [191] κάνανε μία επίθεση στη keystroke αυθεντικοποίηση. Για να πραγματοποιήσουν την συγκεκριμένη επίθεση έκαναν μια στατιστική ανάλυση σε δεδομένα πάνω από 3000 χρηστών που συλλέχθηκαν σε χρονική περίοδο 2 ετών και έτσι δημιούργησαν τις συγκεκριμένες επιθέσεις. Καταφέραν να πετύχουν EER μεταξύ 28,6% και 84.4%. Το θετικό αυτή της επίθεσης είναι ότι είναι ρεαλιστική και βασίζεται σε τρεις εφικτές υποθέσεις: τα keystroke dynamics (KD) δεδομένα που απαιτούνται για να σχεδιαστεί η επίθεση μπορούν εύκολα να συλλεχθούν από ένα επιτιθέμενο, τα απαιτούμενα προγράμματα για την επίθεση είναι εύκολα προσβάσιμα από κάποιο επιτιθέμενο και οι λύσεις έμπιστου λογισμικού που θα μπορούσαν να ματαιώσουν αυτές τις επιθέσεις μπορούν εύκολα να παρακαμφθούν.

Στο [192] παρουσιάζουν μια επίθεση στο Keystroke που την αποκαλούν snoop-forge-replay επίθεση. Η επίθεση πραγματοποιείται σε τρία βήματα: υποκλοπή δεδομένων πληκτρολογίου του χρήστη με την χρήση ενός keylogger, δημιουργία ενός πλαστού δείγματος με βάση όσα δεδομένα υποκλάπηκαν προηγουμένως και υποβολή του συγκεκριμένου δείγματος στο κινητό τηλέφωνο για να παρακαμφθεί η αυθεντικοποίηση. Η επίθεση αυτή δοκιμάστηκε σε 2640 άτομα και με υποκλεμμένα δεδομένα από 20 έως 1200 χαρακτήρες το EER ήταν μεταξύ 48.7% και 91.2%. Σαν πιθανά αντίμετρα σε αυτού του είδους τις επιθέσεις προτείνουν να εισαχθούν και γλωσσικά

χαρακτηριστικά στην αυθεντικοποίηση όπως πόσες φορές ο χρήστης επαναλαμβάνει συγκεκριμένα γράμματα ή γράφει λάθος κάποιες λέξεις, πως ο χρήστης επαναλαμβάνει κάποιο συγκεκριμένο κείμενο, σε ποιες λέξεις ο χρήστης δείχνει μια παραπάνω χρονική καθυστέρηση στο να την γράψει κλπ.

Στο [193] δείχνουν πως με την χρήση ενός απλού "lego" ρομπότ που χρησιμοποιεί δεδομένα από στατιστικές έρευνες γενικού πληθυσμού μπορεί να ξεγελάσει ένα σύστημα αυθεντικοποίησης βασιζόμενο στην αφή. Χρησιμοποιώντας τους καλύτερους αλγορίθμους ταξινόμησης κατάφεραν να αυξήσουν το EER από 339% έως 1004% όταν «πληκτρολογούσε» το ρομπότ. Υπάρχουν κάποια θέματα που απαιτούν περαιτέρω ανάλυση καθότι τα δεδομένα που χρησιμοποίησαν στη συγκεκριμένη έρευνα προέρχονταν μόνο από δύο συγκεκριμένες εφαρμογές. Επίσης χρησιμοποίησαν μόνο 28 συγκεκριμένα χαρακτηριστικά που αυτοί θεώρησαν πιο χρήσιμα για αυτή την επίθεση. Ωστόσο, λόγω του μικρού κόστους των συγκεκριμένων ρομπότ θεωρείται εφικτή η ρεαλιστική τους χρήση σε επιθέσεις τέτοιου είδους.

Στο [194] ερεύνησαν την ευκολία με την οποία κάποιος μπορεί να μιμηθεί το βάδισμα άλλου χρησιμοποιώντας στο πρότυπό τους αισθητήρες σε 3 άξονες και χρησιμοποιώντας Pearson συσχέτιση. Στο πείραμα αυτό συμμετείχαν 13 συμμετέχοντες και προσπαθούσαν να μιμηθούν 5 πρότυπα ενώ για το κάθε πρότυπο κίνησης προσπαθούσαν να το μιμηθούν 15 φορές. Τα αποτελέσματα έδειξαν ότι πράγματι είναι αρκετά εύκολο να μάθει κάποιος να περπατάει όπως κάποιος άλλος και να αυθεντικοποιηθεί λανθασμένα σε κάποιο κινητό τηλέφωνο. Μία λύση που προτείνουν οι συγγραφείς είναι να συνδυάζεται η βάδιση και με άλλα βιομετρικά π.χ. με αποτύπωμα (πολυτροπική αυθεντικοποίηση).

Μία άλλη μελέτη για μίμηση της βάδισης παρουσιάζεται στο [195]. Το πείραμα περιλάμβανε 50 συμμετέχοντες και πέτυχαν ένα EER 6.2 %. Η μίμηση της βάδισης ενός ατόμου κατέληξαν οι ερευνητές ότι είναι κάτι δύσκολο και ακόμη και η εκπαίδευση των χρηστών δεν προσέφερε μεγάλη βελτίωση. Οι ερευνητές έφτασαν στο συμπέρασμα ότι οι εισβολείς έχουν ένα φυσικό άνω όριο μίμησης βάδισης, στο οποίο έδωσαν το όνομα plateau, πάνω από το οποίο δεν μπορούσε ο εισβολέας να πάει την μίμηση της βάδισης.

Στο [196] οι ερευνητές δείχνουν πώς ένα σύστημα αυθεντικοποίησης μέσω βάδισης μπορεί εύκολα κάποιος να το παρακάμψει και να μιμηθεί τον πραγματικό χρήστη με την βοήθεια ενός διαδρόμου γυμναστικής. Δοκιμάζουν την συγκεκριμένη επίθεση σε δεδομένα 18 χρηστών και ουσιαστικά επιτίθενται στο gait based authentication system (GBAS). Έτσι χρησιμοποιώντας μόνο δύο μιμητές και με την χρήση ενός ψηφιακού διαδρόμου γυμναστικής με δυνατότητα ελέγχου ταχύτητας ο επιτιθέμενος αυξάνει το FAR από 5.8% σε 43.66% . Ειδικότερα το FAR σε 11 από 18 χρήστες αυξήθηκε στο 70 % ή και παραπάνω. Αν και χρησιμοποιούνται σε αρκετά συστήματα αυθεντικοποίησης με βάση την βάδιση αισθητήρες των κινητών όπως το επιταχυνσιόμετρο και το γυροσκόπιο υπάρχουν δύο βασικά χαρακτηριστικά που τα καθιστούν εύκολα σε μίμηση. Πρώτον τα χαρακτηριστικά βάδισης αλλάζουν με την διάρκεια του χρόνου και έτσι έχουμε υπερκαλύψεις μεταξύ μεγάλων πληθυσμών και δεύτερον αν έχουμε το δείγμα βάδισης ενός συγκεκριμένου χρήστη τότε η μίμηση της βάδισης είναι πιθανή. Για να πετύχουν την μίμηση που θέλουν δεν προσπαθούν, όπως οι περισσότεροι, να αντιγράψουν τον τρόπο βάδισης εμφανισιακά αλλά να μιμηθούν τα βασικά χαρακτηριστικά της βάδισης όπως το μήκος του βηματισμού, το πλάτος του βηματισμού, την ταχύτητα και το ύψωμα του μηρού κατά την διάρκεια της βάδισης. Με την χρήση

κυρίως αυτών των τεσσάρων χαρακτηριστικών βάδισης πέτυχαν πολύ υψηλά ποσοστά επιτυχίας κάτι που δηλώνει σαφώς ότι μόνο η χρήση δεδομένων από το επιταχυνσιόμετρο δεν αρκεί για να αποφευχθούν επιθέσεις μίμησης.

Στο [197] γίνεται μία έρευνα για επιθέσεις τύπου spoof σε αυθεντικοποίηση μέσω βάδισης. Στη συγκεκριμένη επίθεση δεν βιντεοσκοπούν το χρήστη αλλά συλλέγουν δεδομένα από ένα επιταχυνσιόμετρο που τοποθετούν πάνω στο χρήστη. Συλλέξαν 760 δείγματα βάδισης από 100 άτομα. Το πείραμα αποτελούνταν από δύο μέρη. Στο πρώτο κομμάτι οι χρήστες περπατούσαν με το κανονικό τους βάδισμα και πέτυχαν EER 13%. Στο δεύτερο οι χρήστες προσπαθούσαν να μιμηθούν το περπάτημα κάποιου άλλου. Τα άτομα που είχαν καλή γνώση του πώς βαδίζει κάποιος άλλος χρήστης μπορούσαν εύκολα να παρακάμψουν την αυθεντικοποίηση.

Στο [198] γίνεται μία έρευνα για spoof επιθέσεις σε αυθεντικοποίηση μέσω φωνής. Γίνεται μια έρευνα για τις υπάρχουσες μελέτες πάνω στο συγκεκριμένο αντικείμενο. Κατέληξαν ότι με βάση την ευκολία υλοποίησης τους χωρίζονται σε 3 κατηγορίες οι υπάρχουσες επιθέσεις: επιθέσεις μίμησης χαμηλή πιθανότητα, επιθέσεις replay υψηλή πιθανότητα, επιθέσεις speech synthesis (text-to-speech (TTS)) μέτρια προς υψηλή και επιθέσεις μετατροπής φωνής επίσης μέτρια προς υψηλή. Από άποψη αποτελεσματικότητας (αύξηση του FAR) κατέληξαν στην εξής κατηγοριοποίηση : επιθέσεις μίμησης χαμηλή αποτελεσματικότητα, επιθέσεις replay υψηλή αποτελεσματικότητα, επιθέσεις speech synthesis υψηλή αποτελεσματικότητα και επιθέσεις μετατροπής φωνής υψηλή αποτελεσματικότητα. Ως προς τα υπάρχουσα αντίμετρα κατέληξαν ότι γενικά είναι μικρής αποτελεσματικότητας και απαιτείται περισσότερη μελέτη στο κομμάτι αυτό.

4.5 *Σύνοψη*

Στα ανωτέρω αναφέραμε τα οκτώ σημεία των ευπαθειών που ο επιτιθέμενος μπορεί να εκμεταλλευτεί ώστε να παραπλανήσει ένα σύστημα βιομετρικής αναγνώρισης. Ανάμεσα σε όλες τις επιθέσεις, οι spoof επιθέσεις, δηλαδή η παρουσίαση ενός ψεύτικου βιομετρικού χαρακτηριστικού στον αισθητήρα, κέρδισαν την προσοχή μας και αναλύθηκαν περισσότερο. Πράγματι, παρουσιάστηκε μία αναλυτική επισκόπηση των καινοτόμων μεθόδων spoof για το πρόσωπο και το δακτυλικό αποτύπωμα. Στη συνέχεια έγινε μια επισκόπηση της βιβλιογραφίας σχετικά με την αξιολόγηση της ανθεκτικότητας των πολυτροπικών συστημάτων ενάντια σε επιθέσεις πλαστογράφησης. Διάφορες υπάρχουσες μελέτες κατέληξαν, αντίθετα προς την κοινή πεποίθηση, ότι τα πολυτροπικά βιομετρικά συστήματα είναι ευάλωτα σε spoof επιθέσεις, και μπορεί να παραβιαστούν ακόμη και από την πλαστογράφηση ενός μόνο χαρακτηριστικού.

Τέλος έγινε μια σύντομη ανάλυση νεότερων επιθέσεων και πιθανών αντίμετρων σε συμπεριφορικά βιομετρικά.

5

Συζήτηση – Συμπεράσματα και Προτάσεις για περαιτέρω έρευνα

5.1 *Εισαγωγή*

Ο αριθμός των προσωπικών και ευαίσθητων πληροφοριών που είναι αποθηκευμένες στα smartphones μας συνεχώς αυξάνεται. Έχει αποδειχθεί ότι το 92.8% των χρηστών Android smartphones αποθηκεύουν τέτοιου είδους πληροφορίες στα κινητά τους. Τα smartphones έχουν γίνει επιπλέον και προσωπικοί υπολογιστικές για τους χρήστες, οι οποίοι τα χρησιμοποιούν για την πρόσβαση τους σε υπηρεσίες τύπου cloud όπως π.χ. το e-banking και τα online κοινωνικά δίκτυα. Για τον λόγο αυτό, τα smartphones καθίστανται πολύ ελκυστικοί στόχοι για τους επιτιθέμενους, οι οποίοι προσπαθούν να αποκτήσουν πρόσβαση σε προσωπικές και πολύτιμες πληροφορίες. Η αυθεντικοποίηση του χρήστη είναι απαραίτητη για την προστασίας των προσωπικών μας δεδομένων, της εμπιστευτικότητας και της ακεραιότητας τα οποία μπορούν να πληγούν μέσω επιθέσεων στα smartphones.

Οι υπάρχοντες μηχανισμοί σύνδεσης στη συσκευή χρησιμοποιούν τη μέθοδο της ρητής αυθεντικοποίησης, η οποία απαιτεί την ενεργό συμμετοχή του χρήστη, π.χ., κωδικούς πρόσβασης και δακτυλικά αποτυπώματα. Η σάρωσης της ίριδας και η αναγνώριση του προσώπου μπορεί επίσης να χρησιμοποιηθούν για ρητή αυθεντικοποίηση. Ωστόσο, η επανάληψη της αυθεντικοποίησης για την πρόσβαση σε ευαίσθητες πληροφορίες μέσω αυτών των μηχανισμών δεν αποτελεί μία βολική μέθοδο για τους χρήστες smartphones. Λόγω αυτής της δυσκολίας, όταν ο χρήστης περάσει τον αρχικό έλεγχο ταυτότητας, το σύστημα δεν τον ελέγχει ξανά και αυτό είναι κάτι που αυξάνει τον κίνδυνο ένας επιτιθέμενος να αναλάβει τον έλεγχο του smartphone, σε αντικατάσταση του νόμιμου χρήστη. Έτσι οι κακόβουλοι χρήστες έχουν την δυνατότητα να αποκτήσουν πρόσβαση στα ευαίσθητα δεδομένα και στις υπηρεσίες, είτε αυτά αποθηκεύονται στο cloud είτε στην ίδια την κινητή συσκευή.

Για την προστασία των δεδομένων των smartphones και των cloud-based υπηρεσιών από κακόβουλους χρήστες που φέρονται ως νόμιμοι, προτείνεται ένα ασφαλές σύστημα επαν-αυθεντικοποίησης, το οποίο είναι έμμεσο και συνεχές. Μια έμμεση μέθοδος αυθεντικοποίησης δεν

βασίζεται στην άμεση συμμετοχή του χρήστη, αλλά είναι στενά συνδεδεμένη με την συμπεριφορά του, η οποία καταγράφεται από ενσωματωμένο στο smartphone υλικό όπως η οθόνη αφής, οι αισθητήρες και το GPS. Μια μέθοδος σιωπηρής συνεχούς αυθεντικοποίησης, η οποία πρέπει να επικυρώνει το χρήστη καθ' όλη τη διάρκεια χρήσης, πέρα από τον έλεγχο της αρχικής σύνδεσης, χωρίς να τον διακόπτει. Με αυτό τον τρόπο δύναται να ανιχνευθεί ο «αντίπαλος», όταν πάρει στον έλεγχο του το smartphone και έτσι να αποτραπεί η πρόσβαση του σε ευαίσθητα δεδομένα ή υπηρεσίες που εκτελούνται μέσω των smartphones, ή υπάρχουν μέσα σε αυτά.

Με τους χρήστες να έχουν συνεχώς πρόσβαση στα smartphones, υπάρχει η ανάγκη για ένα μηχανισμό συνεχούς αυθεντικοποίησης (CA) προκειμένου να μειωθεί η συχνότητα της εισαγωγή PIN ή κωδικού. Το CA μπορεί να βασίζεται σε δύο τύπους συμπεριφορικών βιομετρικών στοιχείων: την χρήση των εφαρμογών και στο τρόπο αφής (touch) του κινητού. Η ευρεία χρήση των εφαρμογών (ο αριθμός των downloads για κινητά έφτασε τα 175 δις το 2017) που λειτουργούν σε οθόνες αφής και χρησιμοποιούν και τους δύο τρόπους για αυθεντικοποίηση είναι κάτι φυσιολογικό.

Έχουν προταθεί πολλοί μέθοδοι συμπεριφορικής βιομετρικής αυθεντικοποίησης του χρήστη. Υπάρχει ένας σεβαστός αριθμός δημοσιευμένων εργασιών που αφορούν συμπεριφορικά χαρακτηριστικά είτε μόνα τους είτε σε συνδυασμό, με ποικίλους βαθμούς επιτυχίας. Η συνεχής αυθεντικοποίηση που βασίζεται στο μοτίβο χρήσης εφαρμογών είναι ένα ανοιχτό θέμα προς διερεύνηση. Μελλοντικές εργασίες πρέπει να εστιάσουν προς την κατεύθυνση ενίσχυσης της ιδιωτικότητας του χρήστη, ώστε οι ευαίσθητες πληροφορίες να μη στέλνονται σε online υπηρεσίες. Η αξιολόγηση των μεθόδων πρέπει να λάβει υπόψιν τα ποσοστά false-positive / false-negative, τον αντίκτυπο στην ιδιωτικότητα, την αποδοχή του χρήστη και το κόστος ανάπτυξης και λειτουργείας.

5.2 *Συζητήσεις Και Μελλοντικές Κατευθύνσεις*

Σε αυτή την εργασία παρουσιάστηκε μια επισκόπηση των τελευταίων εξελίξεων στο θέμα της συνεχούς αυθεντικοποίησης που περιλαμβάνει κυρίως τα συμπεριφορικά χαρακτηριστικά, οι πολυτροπικές βιομετρικές μεθόδους καθώς και μία σύντομη αναφορά στις επιθέσεις εναντίον αυτών των μεθόδων. Ελπίζω ότι η εργασία αυτή θα βοηθήσει και θα καθοδηγήσει ένα αναγνώστη που ενδιαφέρεται για αυτή την εκτενή βιβλιογραφία, αλλά προφανώς δεν μπορεί να καλύψει όλη την βιβλιογραφία και γι' αυτό επέλεξα ένα αντιπροσωπευτικό υποσύνολο. Η συνεχής αυθεντικοποίηση σε κινητά τηλέφωνα είναι ένας ενεργός τομέας της έρευνας, καθότι ολοένα και περισσότεροι αισθητήρες προστίθενται στις συσκευές smartphones και η υπολογιστική ισχύς τους έχει αυξηθεί δραματικά. Ωστόσο, υπάρχουν πολλές προκλήσεις που πρέπει να ξεπεραστούν πριν σχεδιαστεί με επιτυχία ένα σύστημα που να βασίζεται σε βιομετρικά χαρακτηριστικά για συνεχή αυθεντικοποίηση. Παρακάτω αναφέρω μερικά:

1. Τα βιομετρικά στοιχεία τη στιγμή της εγγραφής (enrollment) ενδέχεται να έχουν διαφορετικά χαρακτηριστικά από ό, τι εκείνα που παρουσιάζονται κατά τη διάρκεια της αυθεντικοποίησης. Για παράδειγμα στην περίπτωση των βιομετρικών χαρακτηριστικών προσώπου, τα εγγεγραμμένα πρόσωπα είναι συνήθως τραβηγμένα μετωπικά και σε ένα καλά φωτιζόμενο περιβάλλον. Ωστόσο, κατά τη διάρκεια της αυθεντικοποίησης πρέπει το σύστημα να επεξεργαστεί πρόσωπα που μπορεί να έχουν ληφθεί σε πολύ κακό φωτισμό, με παραλλαγές στάσεως ή από κομμάτι του προσώπου. Αυτό το ζήτημα όπου η εκπαίδευση του συστήματος (εγγραφή) και τα δεδομένα που χρησιμοποιούνται έχουν διαφορετική κατανομή από τα δεδομένα στα οποία εφαρμόζεται το μοντέλο είναι συχνά γνωστό ως προσαρμογή τομέα (domain adaptation) [199]. Μία τέτοια μέθοδος

που βασίζεται σε αναγνώριση προσώπου και στις χειρονομίες αφής για συνεχή αυθεντικοποίηση χρησιμοποιώντας προσαρμογή τομέα προτάθηκε πρόσφατα στο [200].

2. Καθώς όλο και περισσότερο συστήματα συνεχούς αυθεντικοποίησης γίνονται διαθέσιμα, οι επιχειρήσεις έχουν αρχίσει να ενσωματώνουν αυτές τις τεχνολογίες στα προϊόντα τους. Οι τεχνολογίες συνεχούς αυθεντικοποίησης συχνά ανατίθενται σε εταιρείες (outsourcing) που παρέχουν τέτοιες υπηρεσίες ως μια υπηρεσία αυθεντικοποίησης, επειδή η ανάπτυξη και η διατήρηση αυτών των τεχνολογιών απαιτεί εξειδικευμένη τεχνογνωσία και υποδομή. Αυτό εγείρει ανησυχίες προστασίας προσωπικών δεδομένων επειδή βιομετρικές πληροφορίες αποκαλύπτονται σε τρίτους. Προκειμένου να αντιμετωπιστεί αυτό το ζήτημα, μέθοδοι για την ανάθεση με ασφάλεια συστημάτων συνεχούς αυθεντικοποίησης είναι απαραίτητοι [201].
3. Ένας μεγάλος αριθμός μεθόδων συνεχούς αυθεντικοποίησης έχει προταθεί στη βιβλιογραφία αλλά η κάθε μέθοδος αξιολογεί την απόδοση της στηριζόμενη σε ένα δικό της dataset [202]. Ωστόσο, στη βιβλιογραφία δεν υπάρχει κανένα σαφές πρότυπο για την αξιολόγηση της επίδοσης των διαφορετικών μεθόδων. Απαιτούνται κατευθυντήριες γραμμές σχετικά με ένα αποδεκτό σημείο αναφοράς.
4. Όπως αναφέρθηκε ένας μεγάλος αριθμός μεθόδων συνεχούς αυθεντικοποίησης αγνοεί το ζήτημα της χρηστικότητας (usability) και της αποδοχής (acceptability). Παρότι μερικές πρόσφατες εργασίες έχουν προσπαθήσει να αντιμετωπίσουν αυτά τα ζητήματα, απαιτείται περισσότερη δουλειά.
5. Ορισμένες από τις συμπεριφορικές μεθόδους συνεχούς αυθεντικοποίησης εξετάζονται βασίζονται σε πολύ απλές λειτουργίες. Για παράδειγμα, οι περισσότεροι μέθοδοι με αναγνώριση χειρονομιών αφής βασίζονται στις x, y συντεταγμένες και σε πληροφορίες ώρας. Ωστόσο, συνήθως δεν κάνουν χρήση της δυναμικής που υπάρχει στις χειρονομίες αφής. Θεωρούμε ότι η ενσωμάτωση γεωμετρίας καθώς και της δυναμικής των κινήσεων αφής σε έναν αλγόριθμο εξόρυξης χαρακτηριστικών θα μπορούσε να ενισχύσει σημαντικά την απόδοση ενός συστήματος για συνεχή αυθεντικοποίηση βασισμένο σε χειρονομίες αφής. Η επιλογή των κατάλληλων χαρακτηριστικών γνωρισμάτων είναι ένα άλλο σημαντικό πρόβλημα που πρέπει να αντιμετωπιστεί στις μεθόδους συνεχούς αυθεντικοποίησης.
6. Ορισμένες από τις μεθόδους των φυσιολογικών, καθώς και των συμπεριφορικών βιομετρικών χαρακτηριστικών συνεχούς αυθεντικοποίησης βασίζονται σε μεθόδους που είναι ευάλωτες σε spoof, mimic, statistic ή digital replay attacks [203], [204]. Για παράδειγμα, κάποιος μπορεί να πλαστογραφήσει (spoof) συστήματα ελέγχου αυθεντικοποίησης ομιλητή χρησιμοποιώντας τεχνικές morphing φωνής. Έχουν γίνει κάποιες προσπάθειες στη βιβλιογραφία για την αντιμετώπιση αυτών των ζητημάτων της συνεχούς αυθεντικοποίησης. Ωστόσο, απαιτείται περισσότερη έρευνα. Για παράδειγμα, στην περίπτωση βιομετρικών στοιχείων προσώπου πρέπει να γίνεται χρήση πρόσθετων αισθητήρων για την ανίχνευση ζωτικότητας (liveness) ώστε να αντιμετωπιστούν προβλήματα spoof attacks.
7. Σε αντίθεση με τις πιστωτικές κάρτες και τους κωδικούς πρόσβασης, οι οποίοι μπορεί να ανακληθούν και να επανεκδοθούν όταν παραβιαστούν, τα βιομετρικά στοιχεία συνδέονται μόνιμα με ένα χρήστη και δεν μπορούν να αντικατασταθούν. Προκειμένου να αποτραπεί η κλοπή των βιομετρικών χαρακτηριστικών των χρηστών κινητών συσκευών, βιομετρικά πρότυπα προστασίας όπως τα ακυρώσιμα βιομετρικά [205], [206] πρέπει να ενσωματωθούν στο πλαίσιο της συνεχούς αυθεντικοποίησης.
8. Οι περισσότερες μέθοδοι συνεχούς αυθεντικοποίησης που εξετάζονται στη παρούσα εργασία έχουν αξιολογηθεί σε μικρού και μεσαίου μεγέθους σύνολα δεδομένων που αποτελούνται από εκατοντάδες δείγματα το πολύ. Ωστόσο, προκειμένου να δούμε πραγματικά τη σημασία και την επίδραση των μεθόδων συνεχούς αυθεντικοποίησης όσον αφορά την χρηστικότητα και την

ασφάλεια, πρέπει να αξιολογηθούν σε μεγάλης κλίμακας σύνολα δεδομένων που να περιέχουν χιλιάδες ή και εκατομμύρια δείγματα.

9. Άλλα θέματα που απαιτείται να λυθούν αφορούν την βελτίωση της ακρίβειας ορθής αυθεντικοποίησης με την χρήση συνδυασμού μεθόδων, να γίνουν εργασίες όχι μόνο για Android αλλά και για IOS και Windows και να ληφθεί σοβαρά υπόψη η κατανάλωση ενέργειας (μπαταρίας) κατά την χρήση αυτών των μεθόδων.

6

Αναφορές - Βιβλιογραφία

[1] M. Panzarino, "More iphones are sold than babies are born each day," 2012. [Online]. Available: https://thenextweb.com/apple/2012/01/25/there-are-now-more-iphones-sold-than-babies-born-in-the-world-every-day/.

[2] "How smartphones are on the verge of taking over the world," 2013. [Online]. Available: http://www.nydailynews.com/life-style/smartphones-world-article-1.1295927.

[3] Khaley, "Introducing the symantec smartphone honey stick project," 2012. [Online]. Available: http://www.symantec.com/connect/blogs/introducing-symantec-smartphone-honey-stick-project.

[4] H. Spray, "Top 100 leaked nude celeb photos of all time," 2016. [Online]. Available: http://www.hecklerspray.com/nude-celebrities.

[5] M. Raza, M. Iqbal, M. Sharif and W. Haider, "A survey of password attacks and comparative analysis on methods for secure authentication," *World Applied Sciences Journal*, vol. IV, p. 439–444, 2012.

[6] H. M. Wood, "The use of passwords for controlled access to computer resources," US Department of Commerce, National Bureau of Standards, 1977.

[7] C. Theriault, "Survey says 70% don't password-protect mobiles: download free Mobile Toolkit," 2014. [Online]. Available: https://nakedsecurity.sophos.com/2011/08/09/free-sophos-mobile-security-toolkit/.

[8] M. Jakobsson, E. Shi, P. Golle and R. Chow, "Implicit authentication for mobile devices," in *Proceedings of the 4th USENIX conference on Hot topics in security , USENIX Association*, 2009.

[9] McAfee, "Mobile Security Report 2009," 2009. [Online]. Available: http://www.telecoms.com/files/2009/05/mobile_secur_report_ph7_b.pdf.

[10] Android, "Google: Ice cream sandwich," 2011. [Online]. Available: http://developer.android.com/about/ versions/android-4.0-highlights.html.

[11] Android, "Introducing: Smart lock," 2018. [Online]. Available: https://get.google.com/smartlock/.

[12] C. Velazco, "Apple touch id is a 500ppi fingerprint sensor built into the iphone 5s home button," Techcrunch, 2013. [Online]. Available: https://techcrunch.com/2013/09/10/apples-touch-id-a-500ppi-fingerprint-sensor-built-into-iphone-5s-home-button/.

[13] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor and M. Savvides, "Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption," in *Proc. USEC*, 2015.

[14] Z. Akhtar, Security of multimodal biometric systems against spoof attacks, Cagliari: Department of Electrical and Electronic Engineering, University of Cagliari, 2012.

[15] F. Bergadano, D. Gunetti and C. Picardi, "User authentication through keystroke dynamics," *ACM Transactions on Information and System Security (TISSEC),* vol. 5, no. 4, p. 367–397, 2002.

[16] "Sensors Overview (Android)," Developer.android.com, 2018. [Online]. Available: https://developer.android.com/guide/topics/sensors/sensors_overview.

[17] V. M. Patel, R. Chellappa and D. Chandra, "Continuous User Authentication on Mobile Devices:Recent progress and remaining challenges," *IEEE Signal Processing Magazine,* vol. 33, no. 4, pp. 49-61, 2016.

[18] M. Smith, M. Mann and G. Urbas, Biometrics, Crime and Security, London: Taylor and Francis Group, 2018.

[19] I. Biperis, "Information Systems Security," 2015. [Online]. Available: http://goo.gl/qsd0M1.

[20] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," in *IEEE Transactions on Circuits and Systems for Video Technology* , 2014.

[21] R. Yampolskiy and V. Govindaraju, "Behavioural biometrics: A survey and classification," *International Journal of Biometrics,* 2008.

[22] T. Sloane, "Behavioral Biometrics: The Restructuring of the Authentication Landscape," 2017. [Online]. Available: https://bit.ly/2CFuMe4.

[23] K. Delac and M. Grgic, "A survey of biometric recognition methods," in *Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine* , Zadar, Croatia, 2004 .

[24] M. A. El-Sayed, M. Hassaballah and M. A. Abdel-Latif, " Identity Verification of Individuals Based on Retinal Features Using Gabor Filters and SVM," *Journal of Signal and Information Processing,* vol. 22, pp. 11-14, 2007.

[25] R. Newman, Security and Access Control Using Biometric Technologies, Course Technology - Cengage Learning, 2009.

[26] J. Campbell, "Speaker recognition: a tutorial," in *Proceedings of the IEEE,* 1997.

[27] L. Friedrichsen, "Barclays Uses Nuance Voice Biometrics to Identify Customers by the Sound of their Voice," Businesswire, 2013. [Online]. Available: https://tinyurl.com/y84j99ld.

[28] H. V. Halteren, "Linguistic profiling for author recognition and verification," in *ACL '04 Proceedings of the 42nd Annual Meeting on Association for Computational Linguistics* , Barcelona, Spain, 2004.

[29] R. Zheng, J. Li, H. Chen and Z. Huang, "A framework for authorship identification of online messages: Writing-style features and classification techniques," *Wiley Online Library,* 2005.

[30] P. Bours and R. Shrestha, "Eigensteps: A giant leap for gait recognition," in *2nd International Workshop on Security and Communication Networks (IWSCN)* , Karlstad, Sweden, 2010.

[31] C. S. Hasan, S. I. Ahamed and M. Tanviruzzaman, "A Privacy Enhancing Approach for Identity Inference Protection in Location-Based Services," in *33rd Annual IEEE International Computer Software and Applications Conference* , Seattle, WA, USA, 2009.

[32] H. Saevanee, N. Clarke, S. Furnell and V. Biscione, "Continuous user authentication using multi-modal biometrics," *Computers & Security,* vol. 53, pp. 234-246, 2015.

[33] P. S. Teh, N. Zhang, A. B. J. Teoh and K. Chen, "A survey on touch dynamics authentication in mobile devices," *Computers & Security by Science Direct,* vol. 59, pp. 210-235, 2016.

[34] Z. Akhtar, A. Hadid, M. Nixon and a. et, "Biometrics: In search of identity and security (q a)," *IEEE MultiMedia,* pp. 1-10, 2017.

[35] A. Jain, R. Bolle and S. Pankanti, Personal Identification in Networked Society, New York: Springer, 2006.

[36] Techtarget, "Definition of authentication," 2018. [Online]. Available: https://searchsecurity.techtarget.com/definition/authentication.

[37] A. Buriro, Behavioral Biometrics for Smartphone User Authentication, Trento, Italy, 2017.

[38] A. Buriro, B. Crispo and 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)* , New Delhi, India , 2017.

[39] K. Olmstead and A. Smith, "Password management and mobile security," Pew Research Center, 2017. [Online]. Available: http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/.

[40] "Lock pattern, PIN, or password: What is the most reliable way to lock a phone?," Secure Group, 2017. [Online]. Available: https://bit.ly/2x1Xqkp.

[41] G. Ye, Z. Tang, D. Fang and a. et, "Cracking Android Pattern Lock in Five Attempts," in *Proceedings of the Network and Distributed System Security Symposium*, San Diego, CA, USA, 2017.

[42] McAfee, "McAfee Threats Report: First Quarter 2013," 2013. [Online]. Available: https://www.cert.uy/wps/wcm/connect/certuy/df8b1a3f-72e4-44b9-82d2-bc7f9c43f810/McAfee+Threats+Report+-+First+Quarter+2013.pdf?MOD=AJPERES.

[43] N. Clarke and S. Furnell, "Authentication of users on mobile telephones - A survey of attitudes and practices," *Computers and Security,* vol. 24, no. 7, pp. 519-527, 2005.

[44] S. Kurkovsky and E. Syta, "Digital natives and mobile phones: A survey of practices and attitudes about privacy and security," in *Technology and Society (ISTAS), IEEE International Symposium,* Wollongong, NSW, Australia , 2010.

[45] P. Rodwell, S. Furnell and P. Reynolds, "A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head," *Computers & Security*, vol. 26, no. 7-8, pp. 468-478, 2007.

[46] N. L. Clarke and S. M. Furnell, "Advanced user authentication for mobile devices," *Computers and Security*, vol. 26, no. 2, pp. 109-119, 2007.

[47] A. E. A. Ahmed and I. Traoré, Continuous Authentication Using Biometrics: Data, Models, and Metrics, Hershey, PA, USA: IGI Global, 2011.

[48] I. Stylios and S. Kokolakis, "Privacy Enhancing on Mobile Devices: Continuous Authentication with Biometrics and Behavioral Modalities," 2016. [Online]. Available: http://bit.ly/2OlsD94.

[49] D. Crouse, H. Han, D. Chandra and et al, "Continuous authentication of mobile user: Fusion of face image and inertial Measurement Unit data," in *International Conference on Biometrics (ICB)* , Phuket, Thailand, 2015.

[50] A. Jain, M. Bolle and S. Pankanti, Biometrics Personal Identification in Networked Society, Springer, 2006.

[51] A. A. Ross, K. Nandakumar and A. Jain, Handbook of Multibiometrics, New York: Springer-Verlag , 2006.

[52] N. Clarke, "Transparent User Authentication: Biometrics, RFID and Behavioural Profiling," *Springer Science & Business Media*, 2011.

[53] M. d. Pawar and R. D. Kokate, "A Review of Multimodal Fusion Techniques: Applications and Research Area," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 6, no. 1, 2017.

[54] A. Perala, "Galaxy S9's 'Intelligent Scan' Feature to Combine Face, Iris Authentication: Report," 2018. [Online]. Available: https://mobileidworld.com/galaxy-s9-intelligent-scan-502053/.

[55] T. G. Staff, "Set Up Intelligent Scan on the Galaxy S9," Tom'S Guide, 2018. [Online]. Available: https://www.tomsguide.com/us/samsung-galaxy-s9-guide,review-5253-2.html.

[56] "All Three New iPhones Feature Face ID Biometric Authentication," 2018. [Online]. Available: https://bit.ly/2NBJaIO.

[57] "System Usability Scale (SUS)," 2017. [Online]. Available: https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.

[58] M. O. Derawi, D. Gafurov and P. Bours, "Towards Continuous Authentication Based on Gait Using Wearable Motion Recording Sensors," in *Continuous Authentication Using Biometrics: Data, Models, and Metrics*, IGI Global, 2012, p. 23.

[59] J. Mantyjarvi, M. Lindholm and E. Vildjiounaite, "Identifying users of portable devices from gait pattern with accelerometers," in *ICASSP '05 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Philadelphia, PA, USA , 2005.

[60] F. Juefei-Xu, C. Bhagavatula, A. Jaech, U. Prasad and M. Savvides, "Gait-ID on the move: Pace independent human identification using cell phone accelerometer dynamics," in *IEEE Fifth*

International Conference on Biometrics: Theory, Applications and Systems (BTAS) , Arlington, VA, USA , 2012.

[61] C. Nickel, C. Busch, S. Rangarajan and M. Möbius, "Using Hidden Markov Models for accelerometer-based biometric gait recognition," in *IEEE 7th International Colloquium on Signal Processing and its Applications* , Penang, Malaysia , 2011.

[62] H. M. Thang, V. Q. Viet, N. D. Thuc and D. Choi, "Gait identification using accelerometer on mobile phone," in *International Conference on Control, Automation and Information Sciences (ICCAIS)* , Ho Chi Minh City, Vietnam , 2012.

[63] M. Muaaz and R. Mayrhofer, "An Analysis of Different Approaches to Gait Recognition Using Cell Phone Based Accelerometers," in *Proceedings of International Conference on Advances in Mobile Computing & Multimedia*, Vienna, Austria, 2013.

[64] Y. Zhong, Y. Deng and G. Meltzner, "Pace independent mobile gait biometrics," in *IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)* , Arlington, VA, USA , 2015.

[65] M. Muaaz and R. Mayrhofer, "Smartphone-Based Gait Recognition: From Authentication to Imitation," *IEEE Transactions on Mobile Computing*, vol. 16, no. 11, pp. 3209 - 3221, 2017.

[66] B. Abdelkader, R. Cutler and L. Davis, "Person Identification Using Automatic Height and Stride Estimation," in *IEEE International Conference on Automatic Face and Gesture Recognition - FGR*, Quebec, Canada, 2002.

[67] D. Gafurov, K. Helkala and T. Søndrol, "Biometric Gait Authentication Using Accelerometer Sensor," *Journal of Computers*, vol. 1, no. 7, pp. 51-59, 2006.

[68] J. R. Kwapisz, G. M. Weiss and S. A. Moore, "Cell phone-based biometric identification," in *IEEE Fourth International Conference on Biometrics: Theory, Applications and Systems (BTAS 10)*, Washington DC, USA, 2010.

[69] T. Feng, X. Zhao and 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)* , Arlington, VA, USA, 2013.

[70] T. Feng, Z. Liu, K.-A. Kwon and et al, "Continuous mobile authentication using touchscreen gestures," in *IEEE Conference on Technologies for Homeland Security (HST)* , Waltham, MA, USA, 2012.

[71] H. Saevanee and P. Bhatarakosol, "User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device," in *International Conference on Computer and Electrical Engineering* , Phuket, Thailand , 2008.

[72] M. Frank, R. Biedert and E. Ma, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," in *IEEE Transactions on Information Forensics and Security*, 2012.

[73] L. Li, X. Zhao and G. Xue, "Unobservable Re-authentication for Smartphones," in *NDSS Symposium* , San Diego, CA United States, 2013.

[74] X. Zhao, T. Feng and W. Shi, "Continuous mobile authentication using a novel Graphic Touch Gesture Feature," in *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)* , Arlington, VA, USA , 2013.

[75] C. Bo, L. Zhang, T. Jung and et al, "Continuous user identification via touch and movement behavioral biometrics," in *IEEE 33rd International Performance Computing and Communications Conference (IPCCC)* , Austin, TX, USA , 2014.

[76] H. Xu, Y. Zhou and M. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *Symposium On UsablePrivacy and Security (SOUPS)*, 2014.

[77] Z. Sitová, J. Šeděnka, Q. Yang and et al, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877 - 892, 2016.

[78] A. Buriro, B. Crispo, F. Delfrari and K. Wrona, "Hold and Sign: A Novel Behavioral Biometrics for Smartphone User Authentication," in *IEEE Security and Privacy Workshops (SPW)*, San Jose, CA, USA, 2016.

[79] H. Seo, E. Kim and H. K. Kim, "A Novel Biometric Identification Based on a User's Input Pattern Analysis for Intelligent Mobile Devices," *International Journal of Advanced Robotic Systems (IJARS)*, vol. 9, no. 2, 2012.

[80] C. Shen, T. Yu, S. Yuan, Y. Li and X. Guan, "Performance Analysis of Motion-Sensor Behavior for User Authentication on Smartphones," *Sensors 2016*, 2016.

[81] A. D. Luca, A. Hang, F. Brudy and H. Hussmann, "Touch me once and i know it's you! Implicit authentication based on touch screen patterns," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* , Austin, Texas, USA, 2012.

[82] P. Gosset, "Aspect: Fraud detection concepts: Final report," 1998.

[83] Y. Moreau, H. Verrelst and J. Vandewalle, "Detection of mobile phone fraud using supervised neural networks: A first prototype," *International Conference on Artificial Neural Networks* , pp. 1065-1070, 1997.

[84] J. Hall, M. Barbeau and E. Kranakis, "Anomaly-based intrusion detection using mobility profiles of public transportation users," in *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications*, Montreal, Que., Canada , 2005.

[85] F. Li, N. Clarke, M. Papadaki and P. Dowland, "Behaviour profiling for transparent authentication for mobile devices," in *10th European Conference on Information Warfare and Security*, Tallinn, Estonia, 2011.

[86] F. Li, N. L. Clarke, M. Papadaki and P. S. Haskell-Dowland, "Active authentication for mobile devices utilising behaviour profiling," *International Journal of Information Security* , vol. 13, no. 3, pp. 229-244, 2014.

[87] D. Bassu, M. Cochinwala and A. Jain, "A new mobile biometric based upon usage context," in *IEEE International Conference on Technologies for Homeland Security (HST)* , Waltham, MA, USA , 2013.

[88] N. Eagle and A. Pentland, "Reality mining: sensing complex social systems," *Personal and Ubiquitous Computing*, vol. 10, no. 4, pp. 255-268, 2006.

[89] H. G. Kayacik, M. Just, L. Baillie, D. Aspinall and N. Micallef, "Data Driven Authentication: On the Effectiveness of User Behaviour Modelling with Mobile Device Sensors," in *In Proceedings of the Third Workshop on Mobile Security Technologies (MoST)*, 2014.

[90] T. J. Neal, D. L. Woodard and A. D. Striegel, "Mobile device application, Bluetooth, and Wi-Fi usage data as behavioral biometric traits," in *IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)* , Arlington, VA, USA , 2015.

[91] T. C. Mendenhall, "The characteristic curves of composition," vol. 11, no. 11, 1887.

[92] F. Mosteller and D. Wallace, Inference and Disputed Authorship: The Federalist, Series in Behaviour Science: Quantitative Methods ed. Addison-Wesley, 1964.

[93] O. D. Vel, A. Anderson, M. Corney and G. Mohay, "Mining E-mail Content for Author Identification Forensics," *ACM Sigmod Record*, vol. 30, no. 4, p. 55–64, 2001.

[94] M. Koppel and J. Schler, "Exploiting Stylistic Idiosyncrasies for Authorship Attribution," in *Proceeding of IJCAI'03 Workshop on Computational Approaches to Style Analysis and Synthesis*, 2003.

[95] M. Gamon, "Linguistic correlates of style: authorship classification with deep linguistic analysis features," in *Proceeding of the 20th international conference on Computational Linguistics (COLING'04)*, 2004.

[96] A. Mohan, M. Baggili and M. K. Rogers, "Authorship attribution of SMS messages using an N-grams approach," 2010.

[97] R. Goodman, M. Hahn, M. Marella and et al, "The use of stylometry for email author identification: a feasibility study," in *Proceedings of Student/Faculty Research Day, CSIS, Pace University*, 2007.

[98] A. Castro, O. Sotoye and e. al, "A Stylometry System for Authenticating Students Taking Online Tests," in *Proceedings of CSIS Research Day*, 2011.

[99] F. Iqbal, M. Debbabi and et al, "E-mail authorship verification for forensic investigation," in *Proceedings of the 25th ACM SIGAPP Symposium on Applied Computing (SAC)*, 2010.

[100] S. Ouamour and H. Sayoud, "Authorship attribution of ancient texts written by ten arabic travelers using a SMO-SVM classifier," in *International Conference on Communications and Information Technology (ICCIT)*, 2012.

[101] A. Boukerche and A. Nitare, "Behavior-Based Intrusion Detection in Mobile Phone Systems," *Journal of Parallel and Distributed Computing*, vol. 62, pp. 1476-1490, 2002.

[102] B. Sun, F. Yu, K. Wu and V. Leung, "Mobility-based anomaly detection in cellular mobile networks," in *Proceedings of the 3rd ACM workshop on Wireless security*, Philadelphia, PA, USA, 2004.

[103] M. Sultana, P. P. Paul and M. L. Gavrilova, "Social Behavioral Information Fusion in Multimodal Biometrics," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, no. 99, pp. 1 - 12 , 2017.

[104] W.-H. Lee and R. B. Lee, "Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning," in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2017.

[105] A. Gupta, M. Miettinen and N. Asokan, "Intuitive Security Policy Configuration in Mobile Devices Using Context Profiling," in *International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing* , Amsterdam, Netherlands , 2012.

[106] H. Saevanee, N. Clarke and S. Furnell, "SMS linguistic profiling authentication on mobile device," in *5th International Conference on Network and System Security* , Milan, Italy , 2011.

[107] H. Feng, K. Fawaz and K. G. Shin, "Continuous Authentication for Voice Assistants," in *MobiCom '17 Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, Snowbird, Utah, USA, 2017.

[108] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," *International Journal of Information Security,* vol. 6, no. 1, pp. 1-14, 2006.

[109] S. Karatzouni, S. M. Furnell, N. L. Clarke and R. A. Botha, "Perceptions of User Authentication on Mobile Devices," in *Proceedings of the 6th Annual ISOnEworld*, Las Vegas, USA, 2007.

[110] E. Maiorana, P. Campisi, N. Gonzalez-Carballo and A. Neri, "Keystroke dynamics authentication for mobile phones," in *Proceedings of the 2011 ACM Symposium on Applied Computing*, New York, NY, USA, 2011.

[111] T. Chang, C. Tsai and J. Lin, "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices," *Journal of Systems and Software,* vol. 85, no. 5, pp. 1157-1165, 2012.

[112] A. Buriro, S. Gupta and B. Crispo, "Evaluation of motionbased touch-typing biometrics in online financial environments," in *16th International Conference of the Biometrics Special Interest Group*, Darmstadt, Germany, 2017.

[113] A. Serwadda, V. V. Phoha and 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, USA, 2013.

[114] H. Zhang, V. M. Patel, M. Fathy and R. Chellappa, "Touch Gesture-Based Active User Authentication Using Dictionaries," in *IEEE Winter Conference on Applications of Computer Vision* , Waikoloa, HI, USA , 2015.

[115] M. Sherman, G. D. Clark, Y. Yang and et al, "User-generated free-form gestures for authentication: security and memorability," in *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*, New Hampshire, USA, 2014.

[116] X. Zhao, T. Feng, W. Shi and I. A. Kakadiaris, "Mobile user authentication using statistical touch dynamics images," *IEEE Transactions on Information Forensics and Security,* vol. 9, no. 11, pp. 1780 - 1789 , 2014.

[117] A. Primo, V. V. Phoha, R. Kumar and A. Serwadda, "Context-Aware Active Authentication Using Smartphone Accelerometer Measurements," in *IEEE Conference on Computer Vision and Pattern Recognition Workshops* , Columbus, OH, USA , 2014.

[118] E. Hayashi, S. Das, S. Amini, J. Hong and I. Oakley, "CASA: context-aware scalable authentication," in *Proceedings of the Ninth Symposium on Usable Privacy and Security* , Newcastle, United Kingdom, 2013.

[119] T. Feng, J. Yang, E. M. Tapia and W. Shi, "TIPS: context-aware implicit user identification using touch screen in uncontrolled environments," in *Workshop on Mobile Computing Systems and Applications*, 2014.

[120] N. Aljohani, J. Shelton and K. Roy, "Continuous Authentication on Smartphones Using An Artificial Immune System," *MAICS*, 2017.

[121] A. Shye, B. Scholbrock and G. Memik, "Into the wild: Studying real user activity patterns to guide power optimizations for mobile architectures," in *42nd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)* , New York, NY, USA , 2009.

[122] R. Murmuria, J. Medsger, A. Stavrou and J. M. Voas, "Mobile Application and Device Power Usage Measurements," in *Proceedings of the 2012 IEEE Sixth International Conference on Software Security and Reliability* , Washington, DC, USA, 2012.

[123] R. Murmuria, A. Stavrou, D. C. Barbará and D. Fleck, "Continuous Authentication on Mobile Devices Using Power Consumption, Touch Gestures and Physical Movement of Users," in *Proceedings of the 18th International Symposium on Research in Attacks, Intrusions, and Defenses*, Kyoto, Japan , 2015.

[124] A. Ross, A. Jain and J.-Z. Qian, "Information Fusion in Biometrics," in *Proc. of 3rd Int'l Conference on Audio- and Video-Based Person Authentication (AVBPA)*, Halmstad, Sweden, 2001.

[125] D.-J. Kim, K.-W. Chung and K.-S. Hong, "Person authentication using face, teeth and voice modalities for mobile device security," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, pp. 2678 - 2685 , 2010.

[126] H. Saevanee, N. L. Clarke and S. M. Furnell, "Multi-modal Behavioural Biometric Authentication for Mobile Devices," *International Information Security Conference of the series IFIP Advances in Information and Communication Technology*, vol. 376, pp. 465-474, 2011.

[127] E. Shi, Y. Niu, M. Jakobsson and R. Chow, "Implicit authentication through learning user behavior," in *Proceedings of the 13th international conference on Information security*, Boca Raton, FL, USA , 2010.

[128] O. Riva, C. Qin, K. Strauss and D. Lymberopoulos, "Progressive Authentication: Deciding When to Authenticate on Mobile Phones," in *Proceedings of the 21st USENIX conference on Security symposium*, Berkeley, CA, USA, 2012.

[129] H. Crawford, K. V. Renaud and T. Storer, "A framework for continuous, transparent mobile device authentication," *Computers & Security*, vol. 39, p. 127–136, 2013.

[130] M. Wolff, "Behavioral Biometric Identification on Mobile Devices," in *Foundations of Augmented Cognition: 7th International Conference, AC 2013, Held as Part of HCI International* , Las Vegas, NV, USA, 2013, pp. 783-791.

[131] N. Zheng, K. Bai, H. Huang and H. Wang, "You Are How You Touch: User Verification on Smartphones via Tapping Behaviors," in *IEEE 22nd International Conference on Network Protocols* , Raleigh, NC, USA , 2014.

[132] C. Bo, L. Zhang and X.-Y. Li, "SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics," Cornell University Library, 2013.

[133] A. Buriro, B. Crispo, F. D. Frari, J. Klardie and K. Wrona, "ITSME: Multi-modal and Unobtrusive Behavioural User Authentication for Smartphones," *International Conference on Passwords . Lecture Notes in Computer Science,* vol. 9551, no. Springer, p. 45 – 61, 2015.

[134] H. Zhang, V. M. Patel and R. Chellappa, "Robust multimodal recognition via multitask multivariate low-rank representations," in *11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)* , Ljubljana, Slovenia , 2015.

[135] L. Fridman, S. Weber, R. Greenstadt and M. Kam, "Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location," *IEEE Systems Journal*, 2015.

[136] S. Weidong, J. Yang and e. al, "Senguard: Passive user identification on smartphones using multiple," in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2011.

[137] C. McCool, S. Marcel and et al, "Bi-modal person recognition on a mobile phone: Using mobile phone data," in *IEEE International Conference on Multimedia and Expo Workshops*, 2012.

[138] H. Saevanee, N. Clarke, S. Furnell and V. Biscione, "Text-Based Active Authentication for Mobile Devices," *IFIP International Information Security Conference* , pp. 99-112, 2014.

[139] Z. Akhtar, B. Attaullah, B. Crispo and T. H. Falk, "Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns," in *5th IEEE Global Conference on Signal and Information Processing (GlobalSIP 2017)*, Montreal, Quebec, Canada, 2017.

[140] M. Khamis, M. Hassib and a. et, "GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication," in *19th ACM International Conference on Multimodal Interaction*, Glasgow, UK , 2017.

[141] Y. Abdelrahman, M. Khamis and F. Alt, "Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication," in *CHI Conference on Human Factors in Computing Systems*, Denver, Colorado, USA, 2017.

[142] X. Zhang, H. Kulkarni and M. R. Morris, "Smartphone-Based Gaze Gesture Communication for People with Motor Disabilities," in *the 2017 CHI Conference*, 2017.

[143] M. Eiband, M. Khamis and a. et, "Understanding Shoulder Surfing in the Wild: Stories from Users and Observers," in *CHI Conference on Human Factors in Computing Systems*, Denver, Colorado, USA, 2017.

[144] V. Rajanna, S. Polsley and a. et, "A Gaze Gesture-Based User Authentication System to Counter Shoulder-Surfing Attacks," in *CHI Conference Extended Abstracts on Human Factors in Computing Systems*, Denver, Colorado, USA, 2017.

[145] I. Brosso, A. L. Neve, G. Bressan and W. V. Ruggiero, "A Continuous Authentication System Based on User Behavior Analysis," in *International Conference on Availability, Reliability and Security*, Krakow, Poland, 2010.

[146] H. Ketabdar, M. Roshandel and D. Skripko, "Towards implicit enhancement of security and user authentication in mobile devices based on movement and audio analysis," in *The Fourth International Conference on Advances in Computer-Human*, 2011.

[147] I. C. Stylios, S. Chatzis, O. Thanou and S. Kokolakis, "Mobile Phones & Behavioral Modalities: Surveying users' practices," in *TELFOR 2015 International IEEE Conference*, SAVA Center, Belgrade, Serbia, November 24-26, 2015.

[148] I. Stylios, O. Thanou, I. Androulidakis and E. Zaitseva, "A Review of Continuous Authentication Using Behavioral Biometrics," in *ACM SEEDA-CECNSM 2016*, Kastoria, Greece, 2016.

[149] J. Sametinger and R. Schloglhofer, "Secure and usable authentication on mobile devices," in *The 10th International Conference on Advances in Mobile Computing & Multimedia (MoMM2012)*, Bali, Indonesia, 2012.

[150] "Verizon Data Breach Investigations: How long since you took a hard look at your cybersecurity?," Verizon Enterprise, 2018. [Online]. Available: https://www.verizonenterprise.com/verizon-insights-lab/dbir/.

[151] "Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," The National Institute of Standards and Technology (NIST), 2018. [Online]. Available: https://www.nist.gov/publications/systems-security-engineering-considerations-multidisciplinary-approach-engineering-1.

[152] I. Agadakos, C. Chen and a. et, "Jumping the Air Gap: Modeling Cyber-Physical Attack Paths in the Internet-of-Things," in *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*, Dallas, Texas, USA, 2017.

[153] T. Zink and M. Waldvogel, "X.509 User Certificate-based Two-Factor Authentication For Web Applications," in *DFN-Forum Kommunikationstechnologien* , Berlin, Germany, 2017.

[154] A. Roy, D. Dasgupta and A. K. Nag, "An Adaptive Approach Towards the Selection of Multi-Factor Authentication," in *2015 IEEE Symposium Series on Computational Intelligence*, Cape Town, South Africa, 2015.

[155] Statista, "Number of smartphone users in the United States from 2010 to 2022 (in millions)*," 2011. [Online]. Available: https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us.

[156] S. Bhable, "A Survey of Security of Multimodal Biometric Systems," *Engineering Research and Applications* , vol. 5, no. 12, pp. 67-75, 2015.

[157] B. Geller, J. Almog, P. Margot and E. Springer, "A chronological review of fingerprint forgery," *Journal of Forensic Sciences*, vol. 44, no. 5, p. 963–968, 1999.

[158] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of artificial "gummy" fingers on fingerprint systems," in *Op. Security and Counterfeit Deterrence Tech (SPIE)*, 2002.

[159] X. Tan, Y. Li, J. Liu and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in *The 11th European conference on Computer vision: Part VI*, Heraklion, Crete, Greece, 2010.

[160] P. Devakumar and R. Sarala, "An Intelligent Approach for Anti-Spoofing in a Multimodal Biometric System," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no. 3, 2017.

[161] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli and S. Schuckers, "LivDet2011 - fingerprint liveness detection competition 2011," in *In International Conference on Biometrics (ICB 2012)*, 2012.

[162] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: a public database and a baseline.," in *International Joint Conference on Biometrics (IJCB 2011)*, Washington, USA, 2011.

[163] G. Fadda, M. Pili, N. Sirena, G. Murgia, Z. Zhang, S. Z. Li, W. R. Schwartz, A. Rocha, H. Pedrini and e. al, "Competition on counter measures to 2-D facial spoofing attacks," in *International Joint Conference on Biometrics (IJCB 2011)*, Washington, USA, 2011.

[164] M. Joshi, B. Mazumdar and S. Dey, "Security Vulnerabilities Against Fingerprint Biometric System," *Cryptography and Security*, 2018.

[165] V. Mura, G. Orrù, R. Casula and a. et, "LivDet 2017 Fingerprint Liveness Detection Competition 2017," *Computer Vision and Pattern Recognition*, 2017.

[166] M. Killioğlu, M. Taşkiran and N. Kahraman, "Anti-spoofing in face recognition with liveness detection using pupil tracking," in *IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)* , Herl'any, Slovakia , 2017.

[167] M. Devi, D. C. Kant and a. et, "A Novel Approach to Improve Biometric Security using Multi-Modal Biometrics and Liveness Detection," *International Journal of Engineering, Science and Mathematics* , vol. 7, no. 4, pp. 421-428, 2018.

[168] T. Putte and J. Keuning, "Biometrical fingerprint recognition: Don't get your fingers burned," in *4th Working Conf. on Smart Card Research and Advanced Applications*, 2000.

[169] J. Galbally-Herrero, J. Fierrez-Aguilar, J. D. Rodriguez-Gonzalez and e. al, "On the vulnerability of fingerprint verification systems to fake fingerprint attacks.," in *Proc. IEEE Intl. Carnahan Conf. on Security Technology*, 2006.

[170] A. Godil, Y. Ressler and P. Grother, "Face recognition using 3d facial shape and color map information: comparison and combination," in *The International Society for Optical Engineering (SPIE)*, Philadelphia, PA, United States, 2005.

[171] Z. Zhang, D. Yi, Z. Lei and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in *IEEE International Conference on Automatic Face and Gesture Recognition*, Santa Barbara, USA, 2011.

[172] R. Raghavendra and C. Busch, "Presentation Attack Detection Methods for Face Recognition Systems - A Comprehensive Survey," *ACM Computing Surveys (ACM COMPUT SURV)*, vol. 50, no. 1, pp. 1-37, 2017.

[173] L. Souza, M. Pamplona, L. Oliveira and J. P. Papa, "How far did we get in face spoofing detection?," *Engineering Applications of Artificial Intelligence*, 2017.

[174] J. Titcomb, "Hackers claim to beat iPhone X's Face ID in one week with £115 mask," Technology Intelligence, 2017. [Online]. Available: https://bit.ly/2xcV2Hx.

[175] S. Kovach, "Samsung's Galaxy S8 facial recognition feature can be fooled with a photo," Business Insider, 2017. [Online]. Available: https://www.businessinsider.com/samsung-galaxy-s8-facial-recognition-tricked-with-a-photo-2017-3?IR=T.

[176] "Samsung Galaxy S8 iris scanner fooled by German hackers," The Guardian, 2017. [Online]. Available: https://bit.ly/2rPlhPX.

[177] C. McGoogan and D. Demetriou, "Peace sign selfies could let hackers copy your fingerprints," Technology Intelligence, 2017. [Online]. Available: https://bit.ly/2NBJaIO.

[178] G. L. Marcialis, F. Roli and L. Didaci, "Personal identity verification by serial fusion of fingerprint and face matchers," *Pattern Recognition*, vol. 42, no. 11, pp. 2807-2817, 2009.

[179] K. Nandakumar, Y. Chen, S. C. Dass and A. K. Jain, "Likelihood ratiobased biometric score fusion," *IEEE Transactions on Pattern Analysis and Machine Intelligence* , vol. 30, no. 2, p. 342–347, 2008.

[180] G. L. Marcialis and F. Roli, "Score-level fusion of fingerprint and face matchers for personal verification under "stress" conditions," in *Proceedings of the 14th International Conference on Image Analysis and Processing*, Modena, Italy , 2007.

[181] X. He, Y. Lu and P. Shi., "A fake iris detection method based on FFT and quality assessment," in *Chinese Conference on pattern recognition* , 2008.

[182] L. Hong, A. Jain and S. Pankanti, "Can multibiometrics improve performance," in *IEEE Workshop on Identification Advanced Technologies Proceedings AutoID*, 1999.

[183] R. N. Rodrigues, L. L. Ling and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks.," *Journal of Visual Languages and Computing*, vol. 20, p. 169–179, 2009.

[184] R. N. Rodrigues, N. Kamat and V. Govindaraju, "Evaluation of biometric spoofing in a multimodal system," in *In 4th IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS)*, Istanbul, Turkey , 2010.

[185] P. A. Johnson, B. Tan and S. Schuckers, "Multimodal fusion vulnerability to non-zero effort (spoof) imposters," in *IEEE Workshop on Information Forensics and Security (WIFS)*, Seattle, WA, USA, 2010.

[186] G. L. Marcialis, A. Lewicke, B. Tan and et al, "First international fingerprint liveness detection competition - LivDet 2009," in *International Conference on Image Analysis and Processing (ICIAP)*, Vietri sul Mare, Italy, 2009.

[187] P. Sharma and K. Singh, "Multimodal Biometric System Fusion Using Fingerprint and Face with Fuzzy Logic," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no. 5, 2017.

[188] P. Negi, P. Sharma, V. S. Jain and B. Bahmani, "K-means++ vs. Behavioral Biometrics: One Loop to Rule Them All," in *Network and Distributed System Security Symposium*, 2018.

[189] C. M. TEY, P. GUPTA and D. GAO, "I Can Be You: Questioning the Use of Keystroke Dynamics as Biometrics," in *Annual Network and Distributed System Security Symposium 20th NDSS 2013*, San Diego, CA, 2013.

[190] A. Serwadda, V. V. Phoha and a. et, "Toward Robotic Robbery on the Touch Screen," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 4, 2016.

[191] A. Serwadda and V. V. Phoha, "Examining a Large Keystroke Biometrics Dataset for Statistical-Attack Openings," *ACM Transactions on Information and System Security (TISSEC)*, vol. 16, no. 2, 2013.

[192] K. A. Rahman, K. S. Balagani and V. V. Phoha, "Snoop-Forge-Replay Attacks on Continuous Verification With Keystrokes," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 528-541, 2013.

[193] A. Serwadda and V. V. Phoha, "When kids' toys breach mobile phone security," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, Berlin, Germany, 2013.

[194] O. Stang, "Gait analysis: Is it easy to learn to walk like someone else?," Gjøvik University College , Norway, 2007.

[195] B. B. Mjaaland, P. Bours and D. Gligoroski, "Walk the Walk: Attacking Gait Biometrics by Imitation," *International Conference on Information Security*, pp. 361-380, 2010.

[196] R. Kumar, V. V. Phoha and A. Jain, "Treadmill attack on gait-based authentication systems," in *IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, Arlington, VA, USA , 2015.

[197] D. Gafurov, E. Snekkenes and P. Bours, "Spoof Attacks on Gait Authentication System," *IEEE Transactions on Information Forensics and Security* , vol. 2, no. 3, 2007.

[198] Z. Wu, N. Evans, T. Kinnunen and a. et, "Spoofing and countermeasures for speaker verification: A survey," *Speech Communication*, vol. 66, pp. 130-153, 2015.

[199] V. M. Patel, R. Gopalan and R. Li, "Visual Domain Adaptation: A survey of recent advances," *IEEE Signal Processing Magazine* , vol. 32, no. 3, 2015.

[200] H. Zhang, V. M. Patel, S. Shekhar and R. Chellappa, "Domain adaptive sparse representation-based classification," in *11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)* , Ljubljana, Slovenia , 2015.

[201] J. Šeděnka and S. Govindarajan, "Secure Outsourced Biometric Authentication With Performance Evaluation on Smartphones," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 2, pp. 384 - 396 , 2015.

[202] "Face Recognition Databases," Face Recognition, 2018. [Online]. Available: http://www.face-rec.org/databases/.

[203] D. F. Smith, A. Wiliem and B. C. Lovell, "Binary watermarks: a practical method to address face recognition replay attacks on consumer mobile devices," in *IEEE International Conference on Identity, Security and Behavior Analysis (ISBA 2015)* , Hong Kong, China , 2015.

[204] D. F. Smith, A. Wiliem and B. C. Lovell, "Face Recognition on Consumer Devices: Reflections on Replay Attacks," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 4, pp. 736 - 745 , 2015.

[205] V. M. Patel, N. K. Ratha and R. Chellappa, "Cancelable Biometrics: A review," *IEEE Signal Processing Magazine,* vol. 32, no. 5, pp. 54 - 65 , 2015.

[206] R. ParkaviK, R. C. Babu, T. Neelambika and P. Shilpa, "Cancelable Biometrics Using Geometric Transformations and Bio Hashing," *Computational Vision and Bio Inspired Computing,* pp. 652-662, 2018.