Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Εξελίξεις στη Τεχνολογία Βιομετρικών , Μελέτη και Αξιολόγηση Ελέγχου Πρόσβασης με Χρήση Behavioral Biometrics, Μελέτη Περίπτωσης στα Keystroke Dynamics

Παναγιώτης Κυριακίδης

Επιβλέπουσα Καθηγήτρια
Δρ. Αδαμαντίνη Περατικού

Μάιος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Εξελίξεις στη Τεχνολογία Βιομετρικών , Μελέτη και Αξιολόγηση Ελέγχου Πρόσβασης με Χρήση Behavioral Biometrics, Μελέτη Περίπτωσης στα Keystroke Dynamics

Παναγιώτης Κυριακίδης

Επιβλέπουσα Καθηγήτρια
Δρ. Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2019

Λευκή σελίδα

Περίληψη

Στην παρούσα μεταπτυχιακή διατριβή εξετάσαμε τις βιομετρικές τεχνολογίες ως μέσα αύξησης της ασφάλειας των πληροφορικών συστημάτων και ειδικότερα το βιομετρικό συμπεριφοράς keystroke dynamics ή δυναμική του ρυθμού της πληκτρολόγησης. Είδαμε πως μπορεί να χρησιμοποιηθεί συμπληρωματικά με τα υπάρχοντα συστήματα αυθεντικοποίησης (username, password, token) ώστε να μπορέσει να μειώσει τις ευπάθειες που οφείλονται στον ανθρώπινό παράγοντα ή και να απομονώσει περιπτώσεις απειλών όπως τα brute force και dictionary attacks.

Πραγματοποιήθηκε μελέτη περίπτωσης πάνω σε έρευνες στο θέμα και σε υπάρχουσες βάσεις δεδομένων χρηστών, συμπληρώθηκε ερωτηματολόγιο με απαντήσεις 100 χρηστών ώστε να διαφανεί η γνώση τους πάνω στην ασφάλεια των υπολογιστών και των δικτύων, η αποδοχή τους στα βιομετρικά ως μέσο ελέγχου πρόσβασης αλλά και βέβαια κατά πόσο γνωρίζει τα keystroke dynamics ο μέσος χρήστης.

Τέλος πραγματοποιήθηκε πείραμα με εισαγωγή κωδικού σε εφαρμογή Python από 12 χρήστες ώστε να δούμε με ποσοτικά στοιχεία το βιομετρικό συμπεριφοράς keystroke dynamics του κάθε ενός χρήστη και ειδικότερα τα στοιχεία hold time και digraph. Σκοπός ήταν να αποδείξουμε εάν στην αρχική περίοδο χρήσης ενός κωδικού πρόσβασης υπάρχουν διακριτά αριθμητικά στοιχεία σχετικά με τον ρυθμό πληκτρολόγησης του κάθε ενός χρήστη που θα μπορούν να μας βοηθήσουν ώστε να προστεθεί ως μια πολύ γρήγορη και με μηδενικό κόστος μέθοδος διπλής αυθεντικοποίησης (two factor authentication) και τον αποκλεισμό των επιθέσεων τύπου brute force. Καταλήξαμε ότι με τη χρήση αλγόριθμων ταξινόμησης φάνηκε παρά το μικρό μέγεθος δείγματος και δοκιμών, ότι υπάρχει μετρήσιμη διαφορά μεταξύ των χρηστών, όταν χρησιμοποιούνται συνδυαστικά τα δυο στοιχεία ελέγχου των keystroke dynamics, το hold time και το digraph time.

Λέξεις κλειδιά: keystroke dynamics, biometrics authentication, authentication, biometrics, identity verification, behavioral biometrics.

Summary

In the present Master thesis we examined biometric technologies as means of enhancing the security of information systems, and in particular the behavioral biometric, keystroke dynamics.

We examined how it can be used in conjunction with existing well known authentication methods (username, password, token), and how it could help us to reduce security vulnerabilities caused by the human factor and increase protection by threats such as brute force or dictionary attacks.

A case study was performed on existing research papers and user databases. Additionally a questionnaire answered by 100 participants in order to demonstrate their knowledge on computer and network security and show the level of acceptance on biometrics as a means for access control, and at the same time if the behavioral biometric keystroke dynamics is actually known by an average user.

Finally an experiment was conducted by entering a code in a Python application from 12 users to examine based on quantitative data the keystroke dynamics biometric behavior of each user and especially the hold time and digraph. The purpose was to show whether in the initial period of a new password there are useful data about the user's typing rate which is the behavioral biometric keystroke dynamic, which can help us to add this to two- factor authentication, as a very fast and non-costing method of authentication and an additional defense to brute force attacks.

We concluded by using classification algorithms that despite the small sample size and number of tests, there was a significant difference between users when both keystroke dynamics attributes, hold time and digraph time were used together to check authentication.

Keywords: keystroke dynamics, biometrics authentication, authentication, biometrics, identity verification, behavioral biometrics.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την επιβλέπουσα της διατριβής, Καθηγήτρια Αδαμαντίνη Περατικού για την πολύτιμη βοήθεια και την επιστημονική καθοδήγηση της κατά τη διάρκεια σχεδιασμού και συγγραφής της παρούσας διατριβής. Επίσης θα ήθελα να ευχαριστήσω τους καθηγητές μου για τα εφόδια και την γνώση που μου προσέφεραν καθόλη τη διάρκεια των σπουδών μου στο μεταπτυχιακό πρόγραμμα ΑΥΔ. Τέλος θα ήθελα να ευχαριστήσω την οικογένεια μου για την υπομονή και την υποστήριξη και ιδιαίτερα τη σύζυγο μου Δώρα και τα παιδιά μου Μιχάλη και Σοφία.

Πίνακας Περιεχομένων

Εισαγωγή

Στην σημερινή εποχή στην οποία κυριαρχούν παγκοσμίως οι έξυπνες συσκευές, οι ΗΥ, οι διαδικτυακές υπηρεσίες όπως ηλεκτρονικό ταχυδρομείο, μέσα κοινωνικής δικτύωσης και ηλεκτρονική τραπεζική, και σε τεράστιους αριθμούς των δισεκατομμυρίων χρηστών και συσκευών, το κεφάλαιο της ασφάλειας των δεδομένων και των πληροφοριών αποτελεί ένα κρίσιμο τομέα και ταυτόχρονα μια συνεχή πρόκληση στην επιστήμη της Πληροφορικής.

Βασικές έννοιες στην ασφάλεια των υπολογιστικών συστημάτων είναι η απειλή (threat) δηλαδή μια πράξη που μπορεί να προξενήσει ζημιά σε τμήμα ή στο σύνολο του συστήματος, η επίθεση (attack) που είναι το αποτέλεσμα των ευπαθειών ή των αδυναμιών των συστημάτων μας που το εκμεταλλεύεται ο επιτιθέμενος και τέλος τα αντίμετρα που μπορούμε να πάρουμε ώστε να μειώσουμε όσο μπορούμε αυτή την απειλή και την επίθεση.

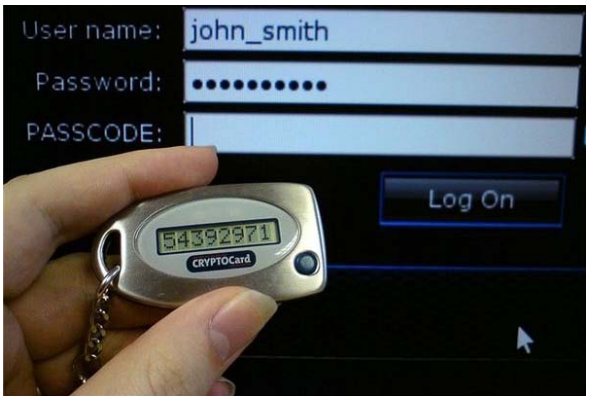
Πρέπει να λάβουμε υπόψη μας ότι η απόλυτη ή τέλεια ασφάλεια δεν μπορεί να υπάρξει άρα εμείς ως πρόληψη ή ως μέθοδο διόρθωσης και αντιμετώπισης προβλημάτων πρέπει να λαμβάνουμε όλα τα μέτρα ώστε να διασφαλίζουμε την αύξηση του επιπέδου ασφαλείας των συστημάτων μας και των χρηστών τους.

Ένας μεγάλος παράγοντας που επιδρά είτε αρνητικά είτε θετικά στο επίπεδο ασφαλείας ενός πληροφοριακού συστήματος είναι ο ανθρώπινος και ειδικά ο τελικός χρήστης. Ως απλός χρήστης θεωρούμε ότι δεν έχει την απαραίτητη εκπαίδευση ή εμπειρία να αντιληφθεί κινδύνους, επιθέσεις ή απειλές και για αυτό το λόγο πρέπει η επιστήμη της Πληροφορικής να τον προστατέψει με μέσα είτε λογισμικού είτε υλικού ώστε να μειώσει τους ενδεχόμενους κινδύνους (viruses, worms, phishing αλλά και πολλά άλλα).

Στην παρούσα μεταπτυχιακή διατριβή θα εξετάσουμε την τεχνολογία βιομετρικών στοιχείων, γνωστή στην διεθνή βιβλιογραφία ως keystroke dynamics, που στα ελληνικά θα μπορούσαμε να το μεταφράσουμε ως Δυναμική (του ρυθμού) της Πληκτρολόγησης.

Η Ασφάλεια των Πληροφοριακών Συστημάτων αποτελεί ένα κρίσιμο τομέα στην καθημερινότητα μας. Ειδικά τώρα που οι ηλεκτρονικές υπηρεσίες έχουν εισέλθει σχεδόν παντού, και μάλιστα σε κρίσιμους τομείς, όπως οι συναλλαγές με το δημόσιο, το ηλεκτρονικό εμπόριο και η ηλεκτρονική τραπεζική. Η προστασία λοιπόν των δεδομένων αποτελεί κύριο στόχο σε όλη τη διαδικασία πρόσβασης του χρήστη, αναγνώρισης, ταυτοποίησης και τελικά έγκριση ή απόρριψη της πρόσβασης στην υπηρεσία.

Με τη ραγδαία αύξηση του ποσοστού χρήσης αυτών των υπηρεσιών, αυξάνεται ραγδαία και η απαίτηση της προστασίας των χρηστών από κακόβουλες ενέργειες όπως πλαστοπροσωπία, κλοπή κωδικών και γενικά της μεθόδου υποκλοπής της ταυτότητας και της αυθεντικοποίησης του νόμιμου χρήστη. Ένας τρόπος πρόσβασης που είναι ουσιαστικά ασφαλέστερος από τα υπάρχοντα συστήματα, είναι με την χρήση της διπλής αυθεντικοποίησης γνωστότερης και ως *two factor authentication* στην οποία ο χρήστης πέρα από τον κλασικό συνδυασμό username / password πρέπει να επιβεβαιώσει και με ένα ακόμα τρόπο την ταυτότητα του, όπως μέσω εναλλακτικής διεύθυνσης email, αποστολή γραπτού μηνύματος SMS ή και με τη βοήθεια hardware υλοποίησης όπως με συσκευή παραγωγής κωδικών token, σύνηθες στην ηλεκτρονική τραπεζική, αφού με αυτή τη μέθοδο διασφαλίζεται και ο όρος περί μη αποποίησης της ευθύνης, το non-repudiation, όρος που ουσιαστικά διασφαλίζει και τα δυο μέρη, τον χρήστη και τον πάροχο της υπηρεσίας ότι αυτός που συνδέεται είναι όντως ο χρήστης και δεν μπορεί να αμφισβητηθεί από κανένα.

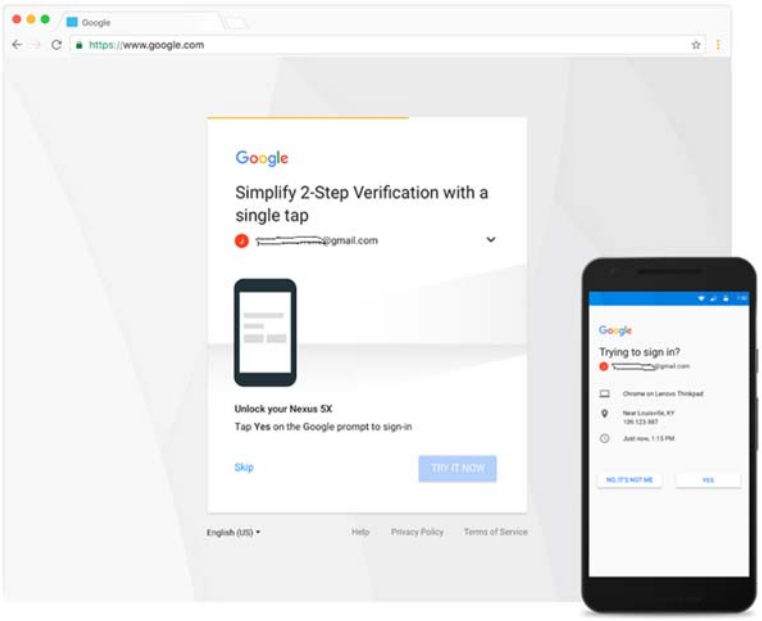


Εικόνα 1, two factor authentication με συσκευή token

Ένα παράδειγμα αποποίησης θα ήταν αν κάποιος χρήστης δεν δεχόταν ότι έκανε ο ίδιος μια τραπεζική κίνηση. Με τη χρήση του token διασφαλίζεται η ταυτότητα του χρήστη με προσθήκη hardware.

Αυτοί οι δυο τρόποι που μόλις αναφέρθηκαν ουσιαστικά περιγράφουν την φιλοσοφία διαχείρισης των πιστοποιητικών εισόδου σε μια διαδικτυακή υπηρεσία, γνωστά και ως *credentials*.

Αυτό προϋποθέτει ότι ο νόμιμος χρήστης γνωρίζει τους κωδικούς πρόσβασης στο πρώτο στάδιο και να έχει ένα κινητό τηλέφωνο για λήψη του SMS ή μια συσκευή παραγωγής κωδικών token για τη δεύτερη φάση της ταυτοποίησης.



Εικόνα 2, two factor authentication με αποστολή επιβεβαιωτικού email

Αυτά τα δυο είναι τα δυο βασικά στοιχεία της αυθεντικοποίησης χρήστη που βασίζεται πολύ απλά σε **κάτι που γνωρίζει** και σε **κάτι που έχει** μόνο αυτός ώστε να διασφαλιστεί η ταυτότητα του.

Στα προηγούμενα επίπεδα ασφάλειας της πρόσβασης, μπορούμε να προσθέσουμε και ένα τρίτο χαρακτηριστικό ασφαλείας **[18]** με τίτλο *keystroke dynamics* που είναι ένα βιομετρικό μοναδικό χαρακτηριστικό και ουσιαστικά προσθέτει **αυτό που είναι** ο χρήστης με τον ίδιο τρόπο όπως ένα βιολογικό βιομετρικό φυσιολογίας όπως είναι τα δακτυλικά αποτυπώματα ή η ίριδα του

ματιού ή ένα βιομετρικό στοιχείο συμπεριφοράς όπως είναι ο ρυθμός ή η δυναμική πληκτρολόγησης, τα keystroke dynamics.

Αυτό ακριβώς το βιομετρικό στοιχείο συμπεριφοράς είναι και το αντικείμενο αυτής της διατριβής η οποία έχει τελικό στόχο να συμβάλει στην αύξηση της ενημέρωσης άρα και της ασφάλειας των δεδομένων του χρήστη από υποκλοπή, διαρροή ή ακόμα και από ενδεχόμενη κακή χρήση ή αμέλεια, όπως για παράδειγμα η είσοδος από δημόσιο δίκτυο ή ΗΥ σε προσωπικό λογαριασμό ταχυδρομείου, τραπεζικής , κοινωνικής δικτύωσης ή άλλου και η μη επιτυχής αποσύνδεση του χρήστη με συνέπεια την έκθεση των προσωπικών στοιχείων του σε κίνδυνο.

Όπως αναφέρει και το U.S. Department of Homeland Security **[14]** τα βιομετρικά δεδομένα είναι τα "*unique physical characteristics, such as fingerprints, that can be used for automated recognition*" και αυτό ακριβώς θα μας απασχολήσει, το πώς συνεισφέρουν στην ασφαλή, αυτοματοποιημένη και γρήγορη πρόσβαση του νόμιμου χρήστη.

Περιγραφή κεφαλαίων

Στην παρούσα διατριβή θα εξετάσουμε τα βιομετρικά, και ειδικότερα το βιομετρικό συμπεριφοράς keystroke dynamics.

Η διατριβή ξεκινάει με την **Εισαγωγή** που όπως είδαμε περιγράφονται οι κύριες παράμετροι της ασφάλειας των υπολογιστών όπως οι κίνδυνοι και τα κυριότερα μέσα που έχουν στη διάθεση τους οι χρήστες.

Στο **Κεφάλαιο 1** έχουμε τις πληροφορίες σχετικά με την έρευνα όπως την συνεισφορά της πάνω στο θέμα, τα βασικά ερευνητικά ερωτήματα και την βιβλιογραφική ανασκόπηση.

Στο **Κεφάλαιο 2** γίνεται η εισαγωγή στις τεχνολογίες βιομετρικών στοιχείων με τις εισαγωγικές πληροφορίες, την ιστορική αναδρομή των βιομετρικών, τους βασικούς ορισμούς ώστε να υπάρξει κατανόηση της ορολογίας, οι μέθοδοι ελέγχου πρόσβασης με χρήση βιομετρικών στοιχείων, η αναφορά στα πλεονεκτήματα και τα μειονεκτήματα των πιο διαδεδομένων και γνωστών βιομετρικών τεχνολογιών, η εισαγωγή στα βιομετρικά συμπεριφοράς και τέλος τις μεθόδους επίθεσης σε βιομετρικά στοιχεία και συστήματα.

Στο **Κεφάλαιο 3** έχουμε την περιγραφή και την ανάλυση των Keystroke Dynamics, τους τρόπους και τις τεχνικές ελέγχου πρόσβασης και αυθεντικοποίησης με την χρήση αυτού του τύπου βιομετρικού συμπεριφοράς, και τους αλγόριθμους που χρησιμοποιούνται με αναφορά σε συγκεκριμένες μελέτες και έρευνες.

Το **Κεφάλαιο 4** ασχολείται με την Ερευνητική διαδικασία και συγκεκριμένα τον κύκλο της έρευνας, περιγράφεται ο σκοπός της έρευνας καθώς και τα βασικά ερευνητικά ερωτήματα με τη μεθοδολογία που ακολουθήθηκε και τη διαδικασία συλλογής των στοιχείων από το ερωτηματολόγιο και το πείραμα. Ακολουθεί το **Κεφάλαιο 5** με τα ευρήματα από την έρευνα, την ανάλυση και την ερμηνεία των αποτελεσμάτων.

Το **Κεφάλαιο 6**, ασχολείται με τα ηθικά αλλά και νομικά ζητήματα των βιομετρικών και ειδικά από την αρχή εφαρμογής του κανονισμού GDPR και τις επιδράσεις θετικές και αρνητικές που υπάρχουν πάνω στα δικαιώματα των χρηστών.

Ακολουθεί το **Κεφάλαιο 7** ως επίλογος με τα συμπεράσματα και την αποτίμηση της τεχνολογίας των keystroke dynamics, αλλά και τα ανοικτά ερευνητικά ερωτήματα πάνω σε αυτά.

Στο τέλος έχουμε τη **βιβλιογραφία** και τα **παραρτήματα**.

Κεφάλαιο 1

Συνεισφορά της έρευνας, ερευνητικά ερωτήματα και βιβλιογραφία

1.1 Σχετικά με την παρούσα έρευνα

Σε αυτή την έρευνα θα προσπαθήσουμε να αναδείξουμε τη χρησιμότητα των βιομετρικών συμπεριφοράς keystroke dynamics. Για να γίνει αυτό πρέπει να ακολουθηθούν σημαντικά βήματα της ερευνητικής διαδικασίας όπως τα ερευνητικά ερωτήματα, η ανασκόπηση της βιβλιογραφίας και βέβαια το τι πρόσθεσε στη γνώση πάνω στο πεδίο η εργασία μας. Σε αυτό το κεφάλαιο αναλύονται αυτά τα θέματα ως εισαγωγή για το υπόλοιπο περιεχόμενο.

1.2 Συνεισφορά της έρευνας

Από τον Ιούνιο του 2015 με την επιβολή των capital control στην Ελλάδα υπήρξε σημαντική αύξηση στο ποσοστό των πολιτών που χρησιμοποιούν πιστωτικές και χρεωστικές κάρτες και βέβαια εφαρμογές ηλεκτρονικής τραπεζικής. Σε αυτό το ποσοστό προσθέτουμε και τα εκατομμύρια αυτών που χρησιμοποιούν το ηλεκτρονικό εμπόριο, ηλεκτρονικό ταχυδρομείο και λογαριασμούς κοινωνικής δικτύωσης. Οι κίνδυνοι στην ασφάλεια αυτής της μεθόδου οδηγεί στην αύξηση του επιπέδου ασφαλείας κατά την πρόσβαση με χρήση επιπλέον επιβεβαίωση της ταυτότητας με αποστολή συνήθως sms στο κινητό τηλέφωνο του πολίτη που εκτελεί για παράδειγμα την τραπεζική κίνηση. Δηλαδή εφαρμόζεται το *two*

factor authentication κάνοντας χρήση το κάτι που γνωρίζει (το username και password του web-banking) και κάτι που έχει στη κατοχή του, το κινητό του τηλέφωνο. Με την χρήση των βιομετρικών στοιχείων, όμως εισέρχεται και μια τρίτη μέθοδος αυθεντικοποίησης (factor of authentication), η επιβεβαίωση του κάτι που είναι, όπως τα δαχτυλικά αποτυπώματα, η αναγνώριση προσώπου, φωνής και βέβαια τα βιομετρικά στοιχεία τύπου keystroke dynamics.

Τα keystroke dynamics προσφέρουν μια πρόσθετη ασφάλεια αφού έχουν τα στοιχεία της μοναδικότητας του ρυθμού πληκτρολόγησης του κάθε ανθρώπου αναλογικά όπως ο κάθε άνθρωπος έχει διαφορετικό και μοναδικό γραφικό χαρακτήρα. Αυτή η εργασία ερευνά τις εξελίξεις στη τεχνολογία των βιομετρικών , και θα προχωρήσει σε μελέτη και αξιολόγηση ελέγχου πρόσβασης κάνοντας χρήση των behavioral biometrics keystroke dynamics. Θα δείξει πιο συγκεκριμένα πόσο μπορεί να χρησιμοποιηθεί στο αρχικό διάστημα χρήσης ενός νέου κωδικού χρησιμοποιώντας ένα κωδικό που έχει χρησιμοποιηθεί και σε άλλες έρευνες ώστε να προσθέσουμε πάνω στην έρευνα **[23]** με περισσότερα στοιχεία όπως την αποτελεσματικότητα των μέσων όρων των χρόνων των hold times αλλά και των digraphs. Επίσης θα συνοψίσουμε τα ανοικτά ερευνητικά θέματα αλλά και τις προοπτικές που έχει το μη επεμβατικό στη προσωπικότητα αλλά και πιο φιλικό στη χρήση, βιομετρικό συμπεριφοράς keystroke dynamics.

1.3 Βασικά ερευνητικά ερωτήματα

Τα βασικά ερευνητικά ερωτήματα που αναδείχθηκαν κατά την έρευνα στην βιβλιογραφία και που θα προσπαθήσουμε να απαντήσουμε ή έστω να πλησιάσουμε στην απάντηση ή ακόμα και να τα θέσουμε ως ανοικτά ερευνητικά ερωτήματα για μελλοντικές εργασίες είναι:

- Ποιες είναι οι παρούσες τεχνολογίες συλλογής βιομετρικών στοιχείων και ποιες βρίσκονται υπό εξέλιξη;
- Είναι αξιόπιστος τρόπος τα keystroke dynamics για ταυτοποίηση της ταυτότητας του χρήστη;

- Προσθέτει Ιδιαίτερη ασφάλεια αυτή η μέθοδος και ακυρώνει τις επιθέσεις dictionary, rainbow αφού πρέπει το password να συνοδεύεται από το σωστό keystroke dynamics;
- Τι επίδραση έχει η ηλικία, η εκπαίδευση, η αλλαγή διάθεσης και ο χρόνος στη αξιοπιστία των keystroke dynamics;
- Τι επίδραση έχει η χρησιμοποίηση άλλων μεθόδων εισαγωγής credential από άλλο ΗΥ, φορητό ή κινητό τηλέφωνο στη αξιοπιστία των keystroke dynamics;
- Ποιες είναι οι ενδεχόμενες απειλές στη χρήση των βιομετρικών στοιχείων keystroke dynamics ;
- Είναι η μελλοντική τάση ασφαλούς πρόσβασης το two factor authentication με χρήση behavioral biometrics;
- Τι γίνεται σε περίπτωση διαρροής των δεδομένων των keystroke dynamics βιομετρικών στοιχείων του πολίτη;
- Ποια είναι η στάση των ανθρώπων απέναντι στη χρήση των βιομετρικών και ειδικότερα στα keystroke dynamics;

Θα προσπαθήσουμε σε αυτή την έρευνα να απαντήσουμε σε αυτά αλλά και σε άλλα όπως το τι γίνεται αν διαρρεύσουν τα βιομετρικά μας στοιχεία όπως τα δακτυλικά αποτυπώματα μας, λαμβάνοντας υπόψη ότι δεν μπορούμε να τα αλλάξουμε όπως ένα password ή ακυρώνοντας απλά μια χρεωστική κάρτα αλλά χρειάζονται πολυσύνθετες διαδικασίες. Άλλα θα ξεκαθαριστούν μέσω του ερωτηματολογίου, της μελέτης των ευρημάτων από έρευνες που έχουν διεξαχθεί και του πειράματος.

1.4 Βιβλιογραφική ανασκόπηση

Το θέμα μας είναι η χρήση βιομετρικών στοιχείων keystroke dynamics για έλεγχο πρόσβασης για την ασφαλή πρόσβαση σε υπηρεσίες πληροφορικής μέσω πειράματος, για αυτό τον λόγο θα ακολουθήσουμε την χρήση βιβλιογραφίας από άρθρα επιστημονικών περιοδικών και συνεδρίων ώστε να έχουμε όσο το

δυνατό πιο περιεκτική εικόνα της τρέχουσας ερευνητικής κατάστασης, των ερευνητικών ερωτημάτων και προβλημάτων. Θα δούμε τη θεωρία και την τεχνολογία πάνω στα βιομετρικά ειδικά στα βιομετρικά συμπεριφοράς keystroke dynamics, τις μεθοδολογίες που χρησιμοποιούνται, τα εργαλεία, τα συμπεράσματα και τα ανοικτά ή νέα ερευνητικά ερωτήματα και προοπτικές.
Για αυτό τον λόγο έγινε έρευνα από την βιβλιοθήκη του ΑΠΚΥ σε δύο βάσεις δεδομένων, την IEEExplore και την Science Direct, χρησιμοποιώντας λέξεις κλειδιά με λογικούς τελεστές όπως biometrics AND keystroke dynamics AND OR access control, και συνδυασμούς αυτών.
Βρέθηκε αντιπροσωπευτική λίστα από 51 πηγές και μελέτες πάνω στα βιομετρικά και στο θέμα του βιομετρικού keystroke dynamics. Αυτή η λίστα εμπλουτίστηκε με θέματα βιβλιογραφίας όπως οι επιθέσεις και η ασφάλεια των βιομετρικών, τα *multimodal biometrics*, τις βάσεις δεδομένων από έρευνες πάνω στα keystroke dynamics και η εξέλιξη των ερευνών πάνω σε αυτά.
Ακολουθεί η ανασκόπηση της βιβλιογραφίας, όπου η αρίθμηση αντιστοιχεί στον τίτλο της εργασίας που αναφέρεται.

Αρχίζουμε με το paper των Ahmad et al **[1]**, στο οποίο αφού γίνεται μια εισαγωγή στα keystroke dynamics, μελετάται με στοιχεία πάνω σε διαθέσιμες βάσεις δεδομένων η χρησιμότητα τους ως πρόσθετο μέτρο ασφάλειας με έλεγχο μέσω στατιστικών εργαλείων αλλά και νευρωνικών δικτύων αλλά και fuzzy logic για την ταυτοποίηση του νόμιμου χρήστη φτάνοντας αθροιστικά τα ποσοστά επιτυχίας το 99%.
Στο επόμενο paper **[2]**, βλέπουμε μια μελέτη πάνω στα συστήματα ελέγχου πρόσβασης που βασίζονται στα φυσιολογικά βιομετρικά στοιχεία του ανθρώπου, και αναφέρονται τα πλεονεκτήματα, τα μειονεκτήματα τους αλλά και η μελλοντικές προοπτικές που έχουν με τη βελτίωση των τεχνολογικών μεθόδων και των αλγορίθμων.
Στο **[3]**, προτείνεται το πρώτο (κατά δήλωση του ερευνητή) σύστημα συνεχόμενης αναγνώρισης μέσω keystroke dynamics χωρίς να απαιτείται προγενέστερη εγγραφή του χρήστη στο σύστημα αναπτύσσοντας και δυο νέες τεχνικές μέτρησης των χρηστών τα Stroke to False Reject (SFR) και Stroke to

False Accept (SFA). Με αυτή τη μελέτη βλέπουμε και τον τρόπο της δυναμικής αναγνώρισης του ρυθμού πληκτρολόγησης.

Στο paper αυτό **[4]** εξετάζεται η επίδραση των keystroke dynamics μέσω οθόνης αφής στην απόδοση ταυτοποίησης και επαλήθευσης μέσω του συνόλου δεδομένων των 42 χρηστών. Τα αποτελέσματα δείχνουν ότι αυτά τα πρόσθετα χαρακτηριστικά ενισχύουν την ακρίβεια και των δύο διαδικασιών.

Βλέπουμε στο επόμενο paper **[5]** να αναφέρει ότι από τα πιο τρωτά σημεία ασφαλείας είναι ο αδύναμος κωδικός πρόσβασης. Επειδή η χρήση μόνο κωδικών πρόσβασης για έλεγχο ταυτότητας ενδέχεται να μην είναι αρκετός, γιατί οι κωδικοί πρόσβασης μπορούν να καταγραφούν ή να εκτεθούν εύκολα σε άλλους. Επομένως, αρκετοί ερευνητές επιλύουν αυτό το πρόβλημα προσθέτοντας τα keystroke dynamics σε ένα όνομα χρήστη ή έναν κωδικό πρόσβασης για την ενίσχυση της διαδικασίας ελέγχου ταυτότητας. Σε αυτή την εργασία, εφαρμόζονται τρεις τεχνικές δυναμικής πληκτρολόγησης, δηλαδή στατιστικές που χρησιμοποιούν confidence interval, k-means clustering, και trajectory dissimilarity, και συγκρίνονται με το ίδιο σύνολο δεδομένων. Η μέτρηση της απόδοσης είναι η ακρίβεια. Από το πείραμα, η τεχνική trajectory dissimilarity δίνει την καλύτερη ακρίβεια στο 96% μεταξύ άλλων.

Σε αυτή τη μελέτη **[6]**, γίνεται έρευνα πάνω στα multimodal biometrics και συγκεκριμένα πάνω στα keystroke dynamics σε συνδυασμό με την κίνηση του mouse και την αλληλεπίδραση με το γραφικό περιβάλλον επιτυγχάνοντας σύμφωνα με τους ερευνητές False Acceptance Rate (FAR) 2.10% και False Rejection Rate (FRR) 2.24%.

Στο επόμενο paper **[7]**, έχουμε μια μελέτη πάνω στη συμβολή των βιομετρικών στην ασφάλεια των πληροφοριών, στις τεχνολογίες, στα διεθνή πρότυπα, στα πλεονεκτήματα και τα μειονεκτήματα τους. Στο επόμενο πολύ ενδιαφέρον paper των Banerjee και Woodard **[8]**, βλέπουμε μια εκτεταμένη μελέτη πάνω στα keystroke dynamics ως μέθοδο βιομετρικής αυθεντικοποίησης και ταυτοποίησης του χρήστη. Γίνεται αναφορά στα διαθέσιμα datasets από βάσεις δεδομένων και οι αλγόριθμοι που χρησιμοποιούνται με έμφαση στην δυναμική μάθηση του συστήματος, τις εφαρμογές πάνω σε αυτά και τις εμπορικές λύσεις που υπάρχουν.

Συνεχίζουμε με το επόμενο άρθρο **[9]** στο οποίο γίνεται αναφορά στους συνδυασμούς μεθόδων βιομετρικής αναγνώρισης με χρήση πολλαπλών βιομετρικών και ειδικού υλικού ώστε να μειωθούν τα μειονεκτήματα τους.

Σε αυτή την μελέτη **[10]** βλέπουμε την εξέλιξη των πατεντών πάνω στα keystroke dynamics, του τύπους μετρήσεων των βιομετρικών χαρακτηριστικών όπως τις στατιστικές μεθόδους, τα νευρωνικά δίκτυα και τη fuzzy logic και την επέκταση του στα κινητά τηλέφωνα.

Στην έρευνα των Bhattacharyya et al **[11]** έχουμε μια πολύ ενδιαφέρουσα παράθεση των φυσιολογικών και μια αναφορά πάνω στα συμπεριφορικά βιομετρικά, τις εφαρμογές τους και τα κριτήρια μετρήσεων πάνω σε αυτά από τις εφαρμογές.

Το paper **[12]** αναφέρει ότι τα παραδοσιακά συστήματα ταυτοποίησης ή ταυτοποίησης χρηστών ενδιαφέρονται για κάτι που έχετε (όπως ένα κλειδί, μια κάρτα ταυτότητας κ.λπ.) ή κάτι που ήδη γνωρίζετε (όπως ένας κωδικός πρόσβασης ή ένας κωδικός PIN). Με το βιομετρικό στοιχείο, αυτό το ενδιαφέρον μετατοπίστηκε προς μια διαφορετική προσέγγιση: κάτι που είναι μέρος σας (δακτυλικά αποτυπώματα ή πρόσωπο) ή κάτι που κάνετε (π.χ. χειρόγραφη υπογραφή ή φωνή). Το σύστημα αναγνώρισης λειτουργεί με τέτοιο τρόπο ώστε το σύστημα να αποκτά ένα δείγμα και να συγκρίνεται με κάθε εγγραφή στη βάση δεδομένων. Αυτή η μέθοδος είναι μια σύγκριση που ονομάζεται "one-to-many". Οι συμπεριφορές και οι ρυθμοί των χαρακτήρων πληκτρολόγησης χρησιμοποιούνται ως ένα βιομετρικό σύστημα ελέγχου ταυτότητας που ονομάζεται Keystroke Dynamics. Σε αντίθεση με τα περισσότερα συστήματα αναγνώρισης που απαιτούν συγκεκριμένο υλικό, η δυναμική πληκτρολόγησης απαιτεί μόνο ένα πληκτρολόγιο. Στην προτεινόμενη προσέγγιση, το μικρό σταθερό κείμενο χρησιμοποιείται όπως στη διαδικασία του κλασικού login . Οι αλγόριθμοι d-variate Gaussian, kNN και decision tree ελέγχονται σε βάση δεδομένων CMU keystroke.

Η επόμενη πηγή **[13]** είναι το βιβλίο του Creswell που αναφέρεται πάνω στην μέθοδο της επιστημονικής έρευνας. Στην επόμενη πηγή **[14]** έχουμε τον ορισμό των βιομετρικών από ένα κυβερνητικό οργανισμό των ΗΠΑ. Σε αυτή τη μελέτη **[15]** παρέχεται μια ανασκόπηση της βιβλιογραφίας σχετικά με τα υπάρχοντα datasets αναφοράς των keystroke dynamics, παρουσιάζουν διάφορα κριτήρια

και δοκιμές για να τα χαρακτηρίσουν, και να εφαρμόσει αυτά τα κριτήρια σε αυτά τα διαθέσιμα datasets δείκτη αναφοράς. Η ανάλυση ανασκόπησης δείχνει ότι υπάρχει σχετική διαφορά 76% μεταξύ του EER στα χειρότερα και καλύτερα αποτελέσματα σύνολα δεδομένων με την ίδια μέθοδο επαλήθευσης ταυτότητας.

Στον 2ο τόμο της εγκυκλοπαίδειας των βιομετρικών **[16]** μαθαίνουμε τη θεωρία σχετικά με την αναγνώριση της υπογραφής. Σε αυτή την εργασία **[17]** μαθαίνουμε για την τεχνολογία εξόρυξης πληροφορίας από τα δακτυλικά αποτυπώματα. Ο στόχος αυτού του paper **[18]** είναι να συνοψίσουμε τις γνωστές προσεγγίσεις που χρησιμοποιούνται στα keystroke dynamics τις τελευταίες δύο δεκαετίες. Εδώ έχουμε ένα πολύ γνωστό βιβλίο **[19]**, και ένα κλασικό εγχειρίδιο σε πανεπιστήμια, που έχει ως θέμα την ασφάλεια των Ασφάλεια πληροφοριακών συστημάτων.

Στην εργασία των Killourhy et al **[20]** έχουμε μια έρευνα με πείραμα ώστε να εξαχθούν συμπεράσματα πάνω στα keystroke dynamics με διάφορους αλγόριθμους ταξινόμησης.

Σε αυτή την εργασία **[21]** ο ερευνητής ασχολείται με το κύριο πρόβλημα στα συστήματα επαλήθευσης που βασίζονται στα στοιχεία σύνδεσης και που είναι το γεγονός ότι δεν μπορούν να πιστοποιήσουν τους χρήστες μετά την πρόσβαση στην πρόσβαση. Για να εξασφαλιστεί η συνεχής επαλήθευση του χρήστη, χρησιμοποιήθηκε το keystroke dynamics που συλλέχθηκε από ελεύθερα πληκτρολογημένο κείμενο κατά τη διάρκεια της περιόδου σύνδεσης. Ωστόσο, η απόδοση αυθεντικότητας δεν ήταν ικανοποιητική. Για να βελτιωθεί η απόδοση του ελέγχου ταυτότητας χρήστη βασισμένου σε ελεύθερα πληκτρολογούμενα πληκτρολόγια, προτείνεται μια μέθοδο εξαγωγής χαρακτηριστικών προσαρμοσμένη στο χρήστη, η οποία συλλαμβάνει τις ξεχωριστές συμπεριφορές δακτυλογράφησης των μεμονωμένων χρηστών που ενσωματώνονται σε σχετικές ταχύτητες δακτυλογράφησης για διαφορετικές ψηφιακές συσκευές.

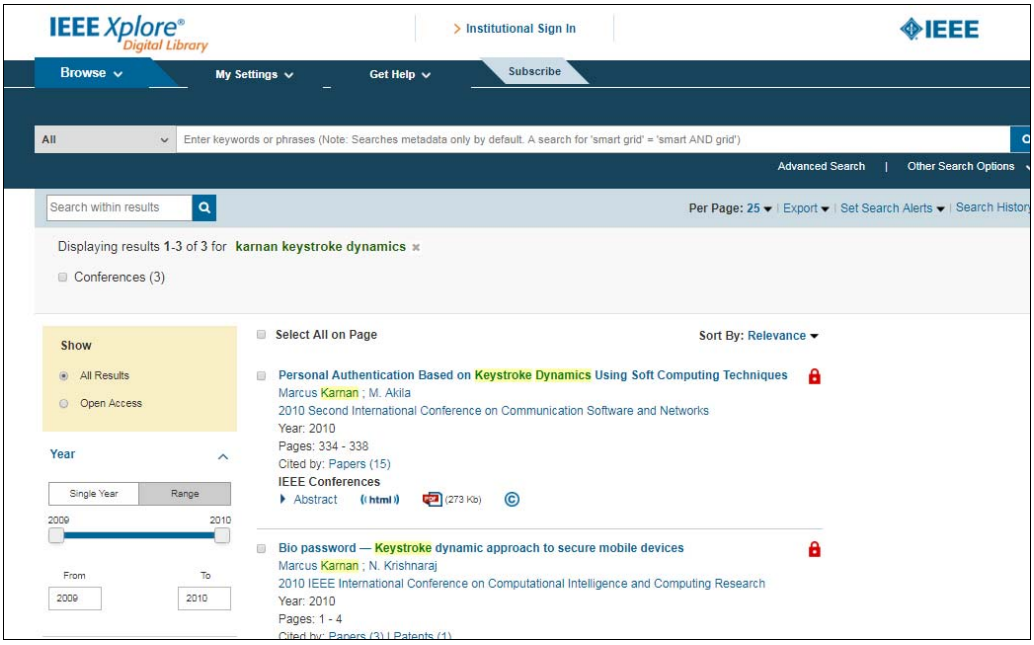
Στο **[22]** των Kochegurova et al έχουμε τη δημιουργία εφαρμογής και αλγόριθμου αναγνώρισης και ταυτοποίησης ατόμων με χρήση keystroke dynamics. Με συμμετοχή 10 ατόμων είχαν αποτελέσματα ακρίβεια αναγνώρισης 87.5%.

Στη μελέτη του Loy **[23]** έχουμε τη χρήση keystroke dynamics σε συνδυασμό με σύλληψη και ενός δεύτερου βιομετρικού χαρακτηριστικού την πίεση που

ασκείται από τον χρήστη σε ειδικό πληκτρολόγιο. Ο κωδικός try4-mbs που χρησιμοποιείται σε αυτό το πείραμα και γίνεται αναφορά σε κατοπινές έρευνες χρησιμοποιείται και από εμάς σε αυτή τη διατριβή.

Στην επόμενη έρευνα **[24]** βλέπουμε σχετικά με την ευχρηστία των βιομετρικών συστημάτων αναγνώρισης ταυτόχρονα με την βελτίωση της ασφάλειας με παρουσίαση μιας μεθόδου στρωματοποίησης της διαδικασίας αυτής και γίνεται και εδώ αναφορά στα πλεονεκτήματα και μειονεκτήματα των βιομετρικών ως μέθοδο αναγνώρισης. Σε αυτό το paper **[25]** εξετάζεται η βιομετρική τεχνική των keystroke dynamics που στοχεύει στον εντοπισμό των χρηστών με βάση την ανάλυση του συνήθη ρυθμού αλλά και με τον τρόπο που γράφουν.

Σε αυτό την εργασία **[26]** γίνεται έρευνα μέσω πειράματος του πως επηρεάζει το keystroke dynamics την απόδοση της επαλήθευσης αφού κάθε ακολουθία συμβόλων προκαλεί ένα ρυθμικό προφίλ . Η σταθεροποίηση αυτού του ρυθμού φαίνεται να είναι μια διαδικασία μάθησης. Τα ρυθμικά πρότυπα στους κωδικούς πρόσβασης αντιμετωπίζονται μέσω βιομετρικών δοκιμών επαλήθευσης. Τα πειραματικά αποτελέσματα αποκτώνται μέσω τριών διαθέσιμων στο κοινό βάσεων δεδομένων, ενώ τα πειράματα καθοδηγούνται από δυο συγκεκριμένα ερευνητικά ερωτήματα.



Εικόνα 3, Βάση δεδομένων επιστημονικών πηγών IEEE Xplore.

Στην επόμενη εργασία **[27]** γίνεται έρευνα για να διαφανεί η χρησιμότητα του ρυθμού πληκτρολόγησης για να ανιχνευτούν στοιχεία όπως η ψυχική διάθεση των χρηστών. Στην εργασία του O'Gorman **[28]** γίνεται μια πολύ ενδιαφέρουσα σύγκριση μεταξύ των βιομετρικών, των κωδικών και των token ως τρόποι αυθεντικοποίησης και την άμυνα τους απέναντι σε τύπους επιθέσεων. Στην εργασία των Peacock et al **[29]** , έχουμε την μελέτη της αναγνώρισης μέσω κοινών αλληλουχιών κειμένου (text patterns) δηλαδή μέσω δυναμικής αναγνώρισης με τα keystroke dynamics. Επίσης θίγεται το θέμα της ιδιωτικότητας και της ασφάλειας των προσωπικών δεδομένων.

Στο επόμενο paper **[30]** ειδικός από τη *BioPassword* εξηγεί την επιστήμη πίσω από τα keystroke dynamics και εξετάζει πώς μπορεί να εφαρμοστεί η τεχνολογία για την ενίσχυση της ασφάλειας και της ευκολίας του χρήστη. Το paper αυτό **[31]** επικεντρώνεται στα keystroke dynamics σε ένα σενάριο με σκοπό να αποδειχτεί ότι η σωστή κατανόηση δεδομένων και προ επεξεργασία των δεδομένων μπορεί να είναι κρίσιμη σε αυτό το σενάριο. Δείγματα από τον ίδιο χρήστη παρουσιάζουν ομοιότητες σε αυτό που ονομάζουμε υπογραφή δακτυλογράφησης μέσα από τα keystroke dynamics. Μετατροπή της κατάταξης μπορεί να επωφεληθεί για να βελτιώσει την απόδοση ταξινόμησης. Γίνεται εκτέλεση ορισμένων immune αλγορίθμων.

Συνεχίζουμε με την εργασία του Qinghan Xiao **[32]** που γίνεται μελέτη πάνω στα θέματα ασφαλείας των βιομετρικών και τους τύπους επιθέσεων που δέχονται ή που είναι δυνατό να δεχτούν. Γίνεται αναφορά στους συνδυαστικούς τρόπους βιομετρικών (multimodal biometrics) και στη συνεχή δυναμική αναγνώριση του χρήστη.

Αμέσως μετά έχουμε μια μελέτη **[33]** σχετικά με τα περιστατικά εξαπάτησης των βιομετρικών συστημάτων, από πολύ απλά όπως την αντιγραφή των δακτυλικών αποτυπωμάτων έως πολύ σύνθετα. Γίνεται και αποτίμηση των ρίσκων από τη χρήση βιομετρικών και αναφέρονται τα πιθανά αντίμετρα και άμυνες. Στην επόμενη μελέτη **[34]** γίνεται μια πρωτότυπη υλοποίηση χρήσης του ρυθμού πληκτρολόγησης για αυθεντικοποίηση του χρήστη με νευρωνικά δίκτυα.

Στην εργασία της Saini et al **[35]**, γίνεται σύγκριση μεθόδων βιομετρικής αναγνώρισης με αναφορά στα πλεονεκτήματα και μειονεκτήματα αρκετών

βιομετρικών στοιχείων φυσιολογικών αλλά και συμπεριφορικών. Στην μελέτη του Senk et al **[36]**, έχουμε την προσέγγιση του ελέγχου πρόσβασης με τα βιομετρικά ως ξεχωριστή υπηρεσία με την εισαγωγή του ως όρο το BioAaaS (Biometric Authentication as a Service) με ιδιαίτερη έμφαση στα ελαττώματα των κλασικών προσεγγίσεων όπως το SaaS στην προστασία των ευαίσθητων προσωπικών και ιδιωτικών δεδομένων. Γίνεται πρωτότυπη σχεδίαση σε επίπεδο εμπορικής χρήσης για επιχειρησιακό μέγεθος με χρήση των keystroke dynamics. Στην εργασία των Shanmugapriya et al **[37]** έχουμε μελέτη πάνω στα keystroke dynamics και ειδικά στις τεχνολογίες, τις προσεγγίσεις και τις προκλήσεις που αντιμετωπίζουν αυτού του είδους τα βιομετρικά συστήματα ελέγχου πρόσβασης. Γίνεται λεπτομερής αναφορά στις μετρικές και τις μεθόδους τέτοιων συστημάτων και τα στοιχεία τους και περιγράφονται οι τύποι των επιθέσεων.

Στην εργασία των Sidlauskas et al **[38]** βλέπουμε τις τεχνικές βιομετρικής αναγνώρισης με βάση τα χαρακτηριστικά της γεωμετρίας του ανθρώπινου χεριού. Πέρα από τα δακτυλικά αποτυπώματα και το περίγραμμα περιέχει βιομετρικές πληροφορίες. Το επόμενο **[39]** είναι ένα άρθρο ιστοσελίδας σχετικά με την τεχνολογία αναγνώρισης προσώπου μέσα σε πλήθος για λόγους ασφαλείας.

Το paper **[40]** που παρουσιάζει μια νέα προσέγγιση προφίλ των ατόμων βασισμένη στα keystroke dynamics που είναι και soft biometrics. Τα soft biometrics χαρακτηριστικά είναι μοναδικά σε κάθε άτομο, το οποίο μπορεί να έχει μια μορφή σωματικών, συμπεριφορικών ή βιολογικών ανθρωπίνων χαρακτηριστικών που διαφοροποιούν τον άνθρωπο σε ομάδα (π.χ. φύλο, ηλικία, ύψος, χρώμα, φυλή κλπ.). Τα keystroke dynamics όπως είδαμε είναι ένα βιομετρικό συμπεριφοράς που αναγνωρίζει τον τρόπο με τον οποίο ένα άτομο πληκτρολογεί σε ένα πληκτρολόγιο. Σε αυτή την εργασία, εξετάζουμε τα παρακάτω soft χαρακτηριστικά: την κατηγορία χεριών (δηλαδή αν ο χρήστης πληκτρολογεί με ένα ή δύο χέρια), την κατηγορία φύλου, την ηλικιακή κατηγορία και την κατηγορία χεριών. Για το σκοπό αυτό, συλλέξαμε μια νέα βάση δεδομένων. Μελετώνται δύο περιπτώσεις: οι στατικοί κωδικοί πρόσβασης και το ελεύθερο κείμενο. Συνδυάζοντας τη διαδικασία της μηχανικής μάθησης και της σύντηξης, τα αποτελέσματα είναι ελπιδοφόρα.

Συνεχίζουμε με το paper **[41]** που περιγράφει μια καινοτόμο τεχνική για την ενίσχυση του συστήματος ελέγχου ταυτότητας με την ενσωμάτωση πολλαπλών δυναμικών πληροφοριών πληκτρολόγησης κάτω από ένα πλαίσιο σύντηξης. Στοχεύει σε τέσσερις τύπους καθυστέρησης ως χαρακτηριστικό πληκτρολόγησης και δύο μεθόδους για τον υπολογισμό των ομοιόμορφων αποτελεσμάτων μεταξύ των δύο δοσμένων λανθανόντων χρόνων. Προτείνεται μια προσέγγιση σύντηξης δύο επιπέδων για τη βελτίωση της συνολικής απόδοσης του συστήματος ώστε να επιτευχθεί σχεδόν 1,401% ίσος ρυθμός σφάλματος (EER). Εισάγονται δύο πρόσθετες ενότητες για την αύξηση της ευελιξίας του προτεινόμενου συστήματος. Αυτές οι ενότητες αποσκοπούν στην αντιμετώπιση εξαιρετικών περιπτώσεων, για παράδειγμα, όταν ένας νόμιμος χρήστης δεν είναι σε θέση να παράσχει την κανονική του μορφή τυποποίησης λόγω αιτιών όπως ο τραυματισμός των χεριών. Η επόμενη πηγή **[42]** είναι εγκυκλοπαίδεια σχετικά με την ασφάλεια και την κρυπτογραφία που μας δίνει χρήσιμες πληροφορίες σχετικά τις τεχνολογίες και τους όρους που χρησιμοποιούνται.

Αυτή η εργασία **[43]** επιχειρεί να αναγνωρίσει το φύλο ενός άγνωστου χρήστη με δεδομένα που προέρχονται μόνο από τα keystroke dynamics. Τα keystroke dynamics, που μπορεί να περιγραφούν ως ο τρόπος πληκτρολόγησης ενός χρήστη, συνήθως ανέρχεται σε δεκάδες χιλιάδες χαρακτηριστικά, καθένα από τα οποία περικλείει κάποιες πληροφορίες. Το ερώτημα που τίθεται είναι ποια από τα χαρακτηριστικά αυτά είναι τα πλέον κατάλληλα για την ταξινόμηση των φύλων. Για να απαντηθεί αυτή η ερώτηση, δημιουργήθηκε ένα νέο σύνολο δεδομένων καταγράφοντας τους χρήστες κατά την καθημερινή χρήση του υπολογιστή τους, υπολογίστηκε το κέρδος πληροφοριών για κάθε δυναμική πληκτρολόγησης και χρησιμοποιήθηκαν πέντε πολύ γνωστά μοντέλα ταξινόμησης για να δοκιμαστούν τα σύνολα χαρακτηριστικών. Τα αποτελέσματα δείχνουν ότι το φύλο ενός άγνωστου χρήστη μπορεί να αναγνωριστεί με ακρίβεια άνω του 95% με μόνο μερικές εκατοντάδες χαρακτηριστικά. Αυτό το ποσοστό, το οποίο είναι το υψηλότερο που υπάρχει στη βιβλιογραφία, είναι αρκετά ελπιδοφόρο για την ανάπτυξη αξιόπιστων συστημάτων που μπορούν να προειδοποιήσουν έναν ανυποψίαστο χρήστη να πέσει θύμα εξαπάτησης. Επιπλέον, η κατοχή της ικανότητας προσδιορισμού του

φύλου ενός χρήστη που πληκτρολογεί ένα συγκεκριμένο κείμενο είναι σημαντικής σημασίας για την ψηφιακή εγκληματολογία.

Συνεχίζουμε με βιβλίο **[44]** πάνω στα βιομετρικά συμπεριφοράς, το οποίο είναι συλλογή 19 μελετών πάνω στο τομέα από το οποίο αντλούμε σημαντικές πληροφορίες για την θεωρία των βιομετρικών όπως τα multimodal biometrics.

Το **[45]** και το **[46]** είναι άρθρα από την Wikipedia σχετικά με τα βιομετρικά και τα δακτυλικά αποτυπώματα και από τα οποία αντλούμε χρήσιμες πληροφορίες, βιβλιογραφικές αναφορές και ορισμούς. Η επόμενη εργασία **[47]** ασχολείται με τις επιθέσεις μίμησης στα βιομετρικά και δείχνει τις μεθόδους και τις τεχνολογίες που χρησιμοποιούνται και τους τρόπους αντιμετώπισης. Η μελέτη **[48]** είναι και αυτή πάνω στα βιομετρικά συμπεριφοράς και ουσιαστικά κάνει χρήση των βιομετρικών για να διακρίνει κακόβουλα λογισμικά όπως bots αλλά και να ταυτοποιεί τους χρήστες για εφαρμογές όπως την ασφάλεια των πληροφοριών μέσω της αυθεντικοποίησης του νόμιμου χρήστη με μεγάλη λεπτομέρεια και σε ευρεία έκταση όπως τον τρόπο συγγραφής των email ή τον τρόπο που μεταχειρίζεται την γλώσσα και τις λέξεις με εφαρμογή ακόμα και στην εγκληματολογία (forensics). Από τη πηγή **[49]** χρησιμοποιήσαμε κομμάτια κώδικα για το πείραμα. Στην επόμενη **[50]** μελέτη διερευνώνται οι επιπτώσεις αλλά και οι περιορισμοί που υπάρχουν πάνω στη χρήση των βιομετρικών σε σχέση με τον νέο κανονισμό GDPR. Στην τελευταία μελέτη **[51]** βλέπουμε την προσπάθεια συνεργασίας soft και hard βιομετρικών για την βελτίωση του επιπέδου ασφαλείας που είναι μια μορφή multimodal. Ένα παράδειγμα είναι ο συνδυασμός του δακτυλικού αποτυπώματος και της φωνής για την ταυτοποίηση του χρήστη.

Κεφάλαιο 2

Οι τεχνολογίες βιομετρικής αναγνώρισης

2.1 Εισαγωγή στις τεχνολογίες βιομετρικών

Σε αυτό το κεφάλαιο θα κάνουμε την εισαγωγή και μια ιστορική αναδρομή στα βιομετρικά, στους διαφορετικούς τύπους και κατηγορίες που αυτά διακρίνονται, στις τεχνολογίες και στα ζητήματα ασφάλειας που αντιμετωπίζουμε κατά τη χρήση τους. Θα συνεχίσουμε στον έλεγχο πρόσβασης με τη χρήση των βιομετρικών φυσιολογικών αλλά και της συμπεριφοράς, τα πλεονεκτήματα και τα μειονεκτήματα τους και τους κινδύνους που αντιμετωπίζουν.

2.2 Ιστορική αναδρομή βιομετρικών

Η βιομετρική τεχνολογία λειτουργεί όπως έχουμε δει μέχρι τώρα αναγνωρίζοντας και ταυτοποιώντας τα μοναδικά σωματικά χαρακτηριστικά ή τα χαρακτηριστικά συμπεριφοράς ή και του ρυθμού κίνησης των ανθρώπων ώστε να προσδιοριστεί η ταυτότητα ενός ατόμου. Από την αρχή της ανθρωπότητας έχουμε ενδείξεις ότι ο άνθρωπος διαισθητικά αξιοποίησε αυτά τα χαρακτηριστικά αφού έχουν βρεθεί αρχαίες τοιχογραφίες με δείγματα παλαμών που θεωρούμε ότι έγιναν ως υπογραφή των δημιουργών τους **[38]** και βέβαια η προσπάθεια αξιοποίησης συνεχίστηκε σε κάθε μεγάλο πολιτισμό της αρχαιότητας, όπως τους Βαβυλώνιους, τους Έλληνες και τους Αιγύπτιους οι οποίοι περιέγραφαν με λεπτομέρειες σε κείμενα τον άγνωστο συνομιλητή ή εκπρόσωπο ώστε να υπάρξει ένας τρόπος απόδειξης του αν είναι αυτός που λέει πράγματι ή είναι κάποιος απατεώνας που υποδύεται το πραγματικό άτομο.

Αυτά τα μοναδικά χαρακτηριστικά είχαν αρχίσει να εντοπίζονται και μελετηθεί ήδη από τον μεσαίωνα και ειδικά τα δακτυλικά αποτυπώματα είχαν από το 1788 αρχίσει να αναγνωρίζονται ως μοναδικά για κάθε άνθρωπο από τον Γερμανό Johann Christoph Andreas Mayer και άρχισαν να υπάρχουν σκέψεις και προσπάθειες αξιοποίησης για την απόδειξη της ταυτότητας **[46].**

Ο Alphonse Bertillon ένας Γάλλος αστυνομικός εισήγαγε στα τέλη του 19ου αιώνα και την μέθοδο της μέτρησης των ανθρώπινων άκρων ως μέθοδο ταυτοποίησης ατόμων **[47].**

Έτσι φτάσαμε στο 1858 όπου ο Sir William James Herschel ένας Βρετανός κρατικός υπάλληλος που υπηρετούσε στην Ινδία ξεκίνησε να χρησιμοποιεί τα δακτυλικά αποτυπώματα ως μέθοδο ταυτοποίησης των ανθρώπων σε συμβόλαια, αποδείξεις πληρωμών αλλά και ως αναγνώριση καταδίκων.

Εικόνα 4, δακτυλικά αποτυπώματα σε έγγραφο του Sir Herschel, 1859-60 [46].

Συνεχίζοντας την έρευνα της ιστορίας των βιομετρικών βλέπουμε ότι στη συνέχεια το 1892 ένας Βρετανός επιστήμονας, ο Francis Galton, με τη μελέτη του πάνω στα δακτυλικά αποτυπώματα δείχνει τη μοναδικότητα τους, πράγμα που ο Juan Vucetich Αργεντινός αστυνομικός χρησιμοποίησε και ταυτοποίησε τον ένοχο μιας δολοφονίας, μια γυναίκα που σκότωσε τα παιδιά της και προσπάθησε να καλύψει τα ίχνη της. Ο Vucetich αξιοποίησε τα αποτυπώματα από τον τόπο του εγκλήματος και μπόρεσε να αποδείξει την ενοχή της κάνοντας την αρχή της αστυνομικής επιστημονικής έρευνας ή forensics science. Στα

επόμενα χρόνια υπήρξε ραγδαία εξέλιξη σε αυτό τον τομέα όπως με την ίδρυση στο FBI ειδικού τμήματος με αρχεία δακτυλικών αποτυπωμάτων το 1924 και τελικά τα δακτυλικά αποτυπώματα επικράτησαν ως η βασική μέθοδος της εγκληματολογικής έρευνας και ταυτοποίησης των ανθρώπων.

Στη συνέχεια και λαμβάνοντας υπόψη τις επιτυχίες διαλεύκανσης αστυνομικών υποθέσεων υπήρξε η δημιουργία βιβλιοθηκών με εκατομμύρια δείγματα σε παγκόσμιο επίπεδο μέσω της Interpol για την εξιχνίαση νέων. Σε προληπτικό επίπεδο έγιναν προσπάθειες, ειδικά στις ΗΠΑ μετά την 11η Σεπτεμβρίου του 2001 και την επίθεση στους δίδυμους πύργους, της μαζικής αναγνώρισης προσώπων (*face recognition*) ώστε να εντοπίζονται άμεσα οι ύποπτοι. Ένα παράδειγμα ήταν στον τελικό του Αμερικάνικου ποδοσφαίρου στην Τάμπα της Φλόριδα το 2001 όπου ένα τέτοιο σύστημα σκάναρε σε πραγματικό χρόνο τα πρόσωπα περίπου 100.000 θεατών για να εντοπίσει υπόπτους τρομοκρατίας **[39].**

Αν και τα αποτελέσματα ήταν απογοητευτικά λόγω των δεκάδων παραμέτρων και της έλλειψης τεχνολογίας οδηγώντας το πανάκριβο σύστημα σε αχρηστία, θεωρείται το πρώτο μεγάλης κλίμακας σύστημα βιομετρικού εντοπισμού.

Αυτό το σύστημα έφερε στην επιφάνεια και τα πρώτα ηθικά διλήμματα και ερωτήματα στην επιφάνεια και άνοιξε ουσιαστικά την συζήτηση για την ορθή χρήση των βιομετρικών σε προληπτικό βαθμό και την ενδεχόμενη καταπάτηση θεμελιωδών δικαιωμάτων του ανθρώπου, θέματα που θα τα θίξουμε σε επόμενο ξεχωριστό κεφάλαιο.

Φεύγοντας από τα φυσιολογικά μοναδικά χαρακτηριστικά όπως τα δακτυλικά αποτυπώματα και την αναγνώριση προσώπων βλέπουμε ότι από την αρχή της τηλεγραφίας τον 19ο αιώνα, οι χειριστές των τηλεγραφικών συσκευών μπορούσαν με τον καιρό να αντιλαμβάνονται την ταυτότητα του απομακρυσμένου χειριστή που έστελνε τον **κώδικα Morse** από τον τρόπο και τον ρυθμό της εκπομπής και μόνο. Αυτό μπορούμε να πούμε ότι ήταν και το πρώτο παράδειγμα παρατήρησης των βιομετρικών της συμπεριφοράς και ένας πρόγονος των σημερινών keystroke dynamics. Από εκεί ουσιαστικά διαφάνηκε ότι μπορούμε να διακρίνουμε τους διαφορετικούς χρήστες από τα

χαρακτηριστικά της συμπεριφοράς αλλά πέρασαν αρκετά χρόνια μέχρι να μελετηθεί και να αξιοποιηθεί αυτό το πεδίο.
Συνεχίζοντας την ιστορική αναδρομή των βιομετρικών βλέπουμε ότι οι επιστήμονες και ερευνητές αναγνώρισαν ότι δεν περιορίζονται σε αυτά που είδαμε αλλά επεκτείνονται σε αρκετά ακόμα κάνοντας ουσιαστικά δυο μεγάλες κατηγορίες, τα φυσιολογικά βιομετρικά και τα βιομετρικά συμπεριφοράς τα οποία πλέον έχουν και τους τίτλους soft και hard biometrics, με τα οποία διαχωρίστηκαν ώστε να μπορούν να χρησιμοποιηθούν κατάλληλα είτε μόνα τους είτε σε συνδυασμό με όνομα χρήστη και κωδικό αλλά και μεταξύ τους (περίπτωση multimodal biometrics).

2.3 Βασικοί ορισμοί

Ξεκινώντας την εργασία μας είναι απαραίτητη μια υποενότητα στην οποία θα αναφερθεί η βασική ορολογία της βιομετρικής τεχνολογίας καθώς και ορισμοί της ασφάλειας υπολογιστών ώστε να μπορούμε με σαφήνεια να καθορίσουμε το τι ακριβώς είναι το κάθε τι, και να μπορούμε να παρακολουθήσουμε πιο εύκολα και με ακρίβεια σε ποιο τομέα η κάθε μια επιδρά αλλά και από τι επηρεάζεται. Έτσι έχουμε τους κάτωθι βασικούς όρους **[19],**

***Έλεγχος προσπέλασης (Access Control)*.** Στο πεδίο της ασφάλειας πληροφοριών ο έλεγχος προσπέλασης είναι ο περιορισμός ή η απαγόρευση της πρόσβασης σε δεδομένα, πόρους ή πληροφορίες. Χωρίζεται σε φυσικό (physical) που πραγματοποιείται με τη βοήθεια βιομετρικών τεχνολογιών όπου η επιτυχής είσοδος και εξουσιοδότηση γίνεται μετά από εισαγωγή και σύγκριση των βιομετρικών στοιχείων του χρήστη που μπορεί να είναι τα δακτυλικά αποτυπώματα, η αναγνώριση του προσώπου ή της ίριδας του ματιού, και σε λογικό έλεγχο πρόσβασης (logical), στον οποίο η πρόσβαση του χρήστη επιτρέπεται με την εισαγωγή του ορθού κωδικού ή token που είναι κάτι που ξέρει και κάτι που έχει αλλά και βιομετρικών στοιχείων που είναι κάτι που είναι ή και με συνδυασμό τους. Με αυτές τις μεθόδους πρόσβασης ο διαχειριστής δημιουργεί μια access control list (*ACL*) που ορίζει σε τι ακριβώς θα έχει

πρόσβαση ο κάθε χρήστης που εξουσιοδοτείται επιτυχώς. ***Εμπιστευτικότητα (Confidentiality).*** Όρος που σημαίνει τη βεβαιότητα ή τους μηχανισμούς ότι τα δεδομένα δεν θα γίνουν γνωστά σε μη εξουσιοδοτημένα άτομα ή σε άλλα συστήματα και πρόληψη μη εξουσιοδοτημένης πρόσβασης σε αυτά.

Ακεραιότητα (Integrity). Όρος που αφορά τη μη τροποποίηση των δεδομένων από μη εξουσιοδοτημένους χρήστες ή προγράμματα.

Διαθεσιμότητα (Availability). Είναι η ιδιότητα της διαθεσιμότητας των δεδομένων ή των πόρων όταν απαιτηθούν από τον εξουσιοδοτημένο χρήστη ή σύστημα. Αυτό σημαίνει ότι πρέπει να έχει εξασφαλιστεί ότι γίνεται ασφαλώς η αποθήκευση της πληροφορίας και η μέθοδος πρόσβασης σε αυτή να λειτουργεί απρόσκοπτα. Συνήθως περιγράφεται είτε αριθμητικά σε ποσοστό, πχ διαθεσιμότητα 99.5% ή με περιγραφή όπως 'υψηλή διαθεσιμότητα υπηρεσίας'. Σε αυτό το σημείο αξίζει να αναφερθεί ότι οι τελευταίο τρεις όροι *confidentiality*, *integrity*, και *availability* διαμορφώνουν τη πολύ γνωστή τριάδα και τον πυρήνα ουσιαστικά της ασφάλειας πληροφοριών, που τη βλέπουμε σε όλα τα σχετικά εγχειρίδια με το αρκτικόλεξο CIA. Αυτά βέβαια πολλές φορές συμπληρώνονται με πρόσθετα χαρακτηριστικά ασφαλείας όπως την πιστοποίηση ταυτότητας (Authentication), την Εξουσιοδότηση (Authorization) και την Μη – Αποποίηση (non – repudiation) και διαμορφώνουν το αρκτικόλεξο τελικά και ως CIAAAN.

Εικόνα 5, CIA triad, [19].

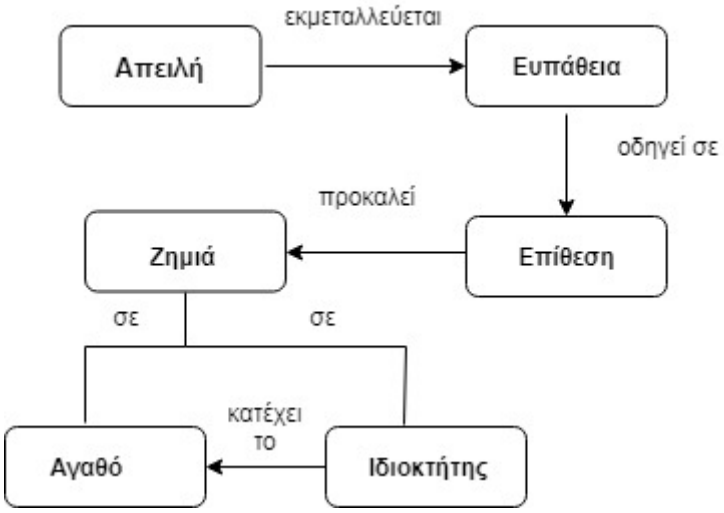
Πιστοποίηση Ταυτότητας (Authentication), είναι ο όρος που επικυρώνει με ψηφιακό τρόπο την ταυτότητα του χρήστη δηλαδή ότι όντως υπάρχει στις λίστες πρόσβασης ως νόμιμος χρήστης ή ακόμα και υποσύστημα.

Εξουσιοδότηση (Authorization), όρος ο οποίος είναι το επόμενο στάδιο της πιστοποίησης της ταυτότητας, κατά το οποίο αποδίδονται τα καθορισμένα από τον διαχειριστή δικαιώματα χρήστη στους πόρους και στις εφαρμογές του συστήματος.

Μη- αποποίηση ευθύνης (Non-repudiation), είναι η διαβεβαίωση ότι δεν μπορεί κάποιος να αρνηθεί ότι έγινε από αυτόν αποστολή μηνύματος ή αιτήματος ή διεργασίας και αντίστοιχα ότι δεν μπορεί να αρνηθεί ότι παρέλαβε το αντίστοιχο μήνυμα ή αίτημα.

Ευπάθεια (Vulnerability), είναι μια πιθανή αδυναμία στα συστήματα ασφάλειας η οποία προκαλεί κίνδυνο και φανερώνει ευάλωτα σημείο σε τυχόν κακόβουλες ενέργειες. Οι ευπάθειες μπορεί να οφείλονται στον ανθρώπινο παράγοντα, ο οποίος είναι και ο κρισιμότερος στην ασφάλεια των πληροφοριών, αλλά και σε ευπάθειες του υλικού και του λογισμικού και των επικοινωνιών και είναι κρίσιμο να εντοπίζονται με τακτικούς ελέγχους και να διορθώνονται.

Απειλή (Threat), είναι το αποτέλεσμα των ευπαθειών στο σύστημα η οποία μπορεί να προξενήσει απώλειες ή ζημιές στο σύστημα και στους χρήστες όπως υποκλοπή, απώλεια ή μεταβολή. Οι απειλές μπορεί να είναι φυσικές που προκύπτουν από το φυσικό περιβάλλον, τις εκούσιες που είναι αποτέλεσμα κακόβουλων ενεργειών και ακούσιες που οφείλονται σε ελλιπείς ή εσφαλμένες ενέργειες των χρηστών του συστήματος και βέβαια τεχνικής φύσης.



Εικόνα 6, σχέση μεταξύ των βασικών εννοιών στην ασφάλεια των πληροφοριών

Πολιτική ασφάλειας (Security Policy), είναι το σύνολο των μεθόδων και των οδηγιών ώστε να δημιουργείται ασφαλές περιβάλλον στο σύστημα και στους χρήστες με όλα τα κατάλληλα μέσα που παρέχονται από τον διαχειριστή του συστήματος και την διοίκηση.

Επίθεση (Attack), είναι η εκμετάλλευση μιας ευπάθειας από ένα κακόβουλο άτομο ή πρόγραμμα για την πραγματοποίηση απειλής με την κατάλληλη μέθοδο και με συγκεκριμένο κίνητρο.

Βιομετρικά (Biometrics), είναι ο όρος που περικλείει το σύνολο των βιολογικών και συμπεριφορικών χαρακτηριστικών του ανθρώπου τα οποία με κατάλληλη συλλογή, αποθήκευση, ανάλυση και επεξεργασία μπορούν να χρησιμοποιηθούν από τομείς όπως η εγκληματολογία (*forensics*) μέχρι την αυθεντικοποίηση του ατόμου ως νόμιμος εξουσιοδοτημένος χρήστης μιας υπηρεσίας ή όχι.

Φυσιολογικά βιομετρικά (Physical biometrics), είναι το σύνολο των βιολογικών μοναδικών χαρακτηριστικών του ανθρώπου όπως τα δακτυλικά αποτυπώματα, η ίριδα του ματιού, το φλεβικό σύστημα της παλάμης, η γεωμετρία του χεριού και βέβαια το DNA. Ουσιαστικά είναι τα μόνιμα και μη μεταβαλλόμενα φυσιολογικά χαρακτηριστικά.

Βιομετρικά συμπεριφοράς (behavioral biometrics), είναι τα χαρακτηριστικά του τρόπου που ξεχωρίζει ένας άνθρωπος από άλλον, όπως ο τρόπος περπατήματος, ο γραφικός χαρακτήρας, η φωνή και ο ρυθμός πληκτρολόγησης.

Δυναμική ή Ρυθμός πληκτρολόγησης (keystroke dynamics), είναι βιομετρικό συμπεριφοράς το οποίο χρησιμοποιείται για να χαρακτηρίσει τον μοναδικό τρόπο που ένας άνθρωπος πληκτρολογεί ένα κείμενο ως μέθοδο ταυτοποίησης. Αυτός ο συγκεκριμένος ρυθμός πληκτρολόγησης εξάγεται και αναλύεται μέσω του πληκτρολογίου αλλά ουσιαστικά μπορεί να συλλεχθεί και μέσα από άλλες πηγές εισόδου όπως τις οθόνες αφής.

Αναγνώριση προσώπου (Face recognition), είναι η διαδικασία αναγνώρισης του συγκεκριμένου ανθρώπου μέσω των μοναδικών γεωμετρικών χαρακτηριστικών του προσώπου. Ουσιαστικά συγκρίνονται κάποια προεπιλεγμένα σημεία του προσώπου προς εξέταση με αυτά από την ήδη αποθηκευμένη εικόνα στο σύστημα πρόσβασης.

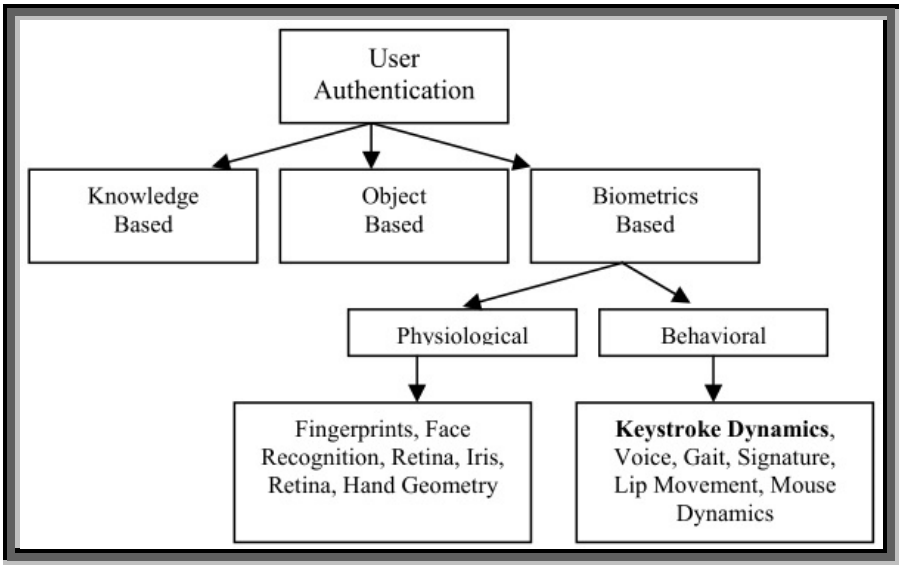
Αναγνώριση δακτυλικών αποτυπωμάτων (Fingerprint recognition), είναι ίσως η πιο παλαιά επιστημονική μέθοδος αναγνώρισης των ανθρώπων πολύ πριν τα ψηφιακά μέσα, και στηρίζεται στη μοναδικότητα των αυλακιών στην επιφάνεια των δακτύλων και της λιπαρότητας του ανθρωπίνου σώματος που ουσιαστικά αφήνει το ίχνος των αποτυπωμάτων σε μεγάλο εύρος επιφανειών.

Αναγνώριση φωνής (Voice recognition), είναι το βιομετρικό συμπεριφοράς το οποίο χρησιμοποιεί τα χαρακτηριστικά της ομιλίας ενός ανθρώπου για πρόσβαση σε υπηρεσίες. Συνηθίζεται λόγω του μεγάλου ποσοστού σφαλμάτων να μη χρησιμοποιείται σε ευαίσθητες εφαρμογές πιστοποίησης αλλά σε αυτοματοποιημένα μενού που παίζει ρόλο το τι λέω και όχι το ποιος το λέει.

2.4 Πρόσβαση με χρήση βιομετρικών ελέγχων

Σε αυτή την υποενότητα θα εξετάσουμε ποια είναι η λογική πάνω στην οποία στηρίζεται η πρόσβαση με τη χρήση των βιομετρικών στοιχείων του χρήστη. Να θυμηθούμε ότι το πρώτο που απαιτείται κατά τη διαδικασία ελέγχου πρόσβασης είναι η αυθεντικοποίηση του χρήστη. Η διαδικασία που ουσιαστικά επικυρώνει την ταυτότητα του νόμιμου ατόμου που αιτείται την πρόσβαση. Αυτό επιτυγχάνεται μέσω της σύγκρισης και του ελέγχου ταύτισης του ήδη αποθηκευμένου δείγματος που υπέβαλε κατά την εγγραφή του ο χρήστης, με αυτό που εκείνη τη δεδομένη στιγμή εκείνος υποβάλει **[37].**

Αυτή η διαδικασία ελέγχου εισόδου της ταυτότητας του χρήστη χωρίζεται σε τρεις κατηγορίες, την ***knowledge – based***, δηλαδή κάτι που γνωρίζει μόνο ο χρήστης, ***token – based***, κάτι που μόνο ο χρήστης έχει και τέλος το ***biometric – based***, δηλαδή κάτι που χαρακτηρίζει μοναδικά τον χρήστη.



Εικόνα 7, Οι μέθοδοι ταυτοποίησης του χρήστη, [37]

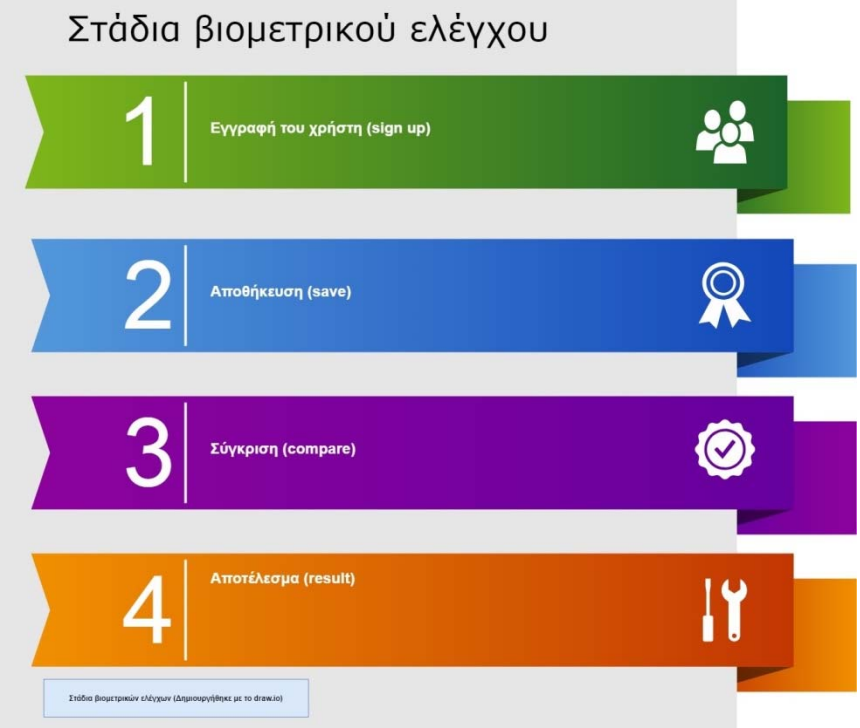
Εμείς θα μελετήσουμε την **biometric – based**, αυτό που χαρακτηρίζει μοναδικά τον χρήστη και γίνεται με τη βοήθεια των βιομετρικών του χαρακτηριστικών. Αυτό επιτυγχάνεται ακολουθώντας κάποια λογικά βήματα και κάνοντας χρήση του αντίστοιχου εξοπλισμού ώστε να μπορέσουμε να συλλάβουμε τα βιομετρικά χαρακτηριστικά. Με τη βοήθεια κάμερας μπορούμε να κάνουμε λήψη του προσώπου ή της ίριδας και αυτό αποθηκεύεται σε μορφή αρχείου εικόνας ώστε να αναλυθεί και να συγκριθούν τα ορισμένα γεωμετρικά στοιχεία του προσώπου, ενώ αντίθετα αν κάνουμε σύλληψη της φωνής του χρήστη χρειαζόμαστε μικρόφωνο ως συσκευή εισόδου και το αρχείο αυτό αποθηκεύεται σε μορφή αρχείου ήχου ώστε να αναλυθεί το φάσμα των συχνοτήτων των κυματομορφών της.

Τα βασικά στάδια που ακολουθούνται σε ένα σύστημα βιομετρικού ελέγχου είναι τα εξής: Η αρχική εισαγωγή με την **εγγραφή** του χρήστη (φάση *signing up*, *enrolment*) που γίνεται η εισαγωγή των βιομετρικών στοιχείων του με χρήση κατάλληλης κάθε φοράς συσκευής εισόδου. Αυτή η διαδικασία μπορεί να

απαιτήσει επαναλήψεις ώστε να μπορέσει να δημιουργηθεί ένα κατάλληλο και αξιόπιστο δείγμα αρχικής ταυτοποίησης ώστε να μειωθούν τα περιστατικά εσφαλμένης έγκρισης (*false accept rate,* ***FAR***) ή εσφαλμένης απόρριψης (*false reject rate,* ***FRR***). Αυτά τα δυο στοιχεία είναι πολύ σημαντικά στην ουσιαστική αξιοπιστία του συστήματος μας, αφού θεωρητικά το σύστημα βιομετρικού ελέγχου απαιτεί να παρέχει ανάλογα με την εφαρμογή υψηλούς δείκτες σε ένα από τα δυο τουλάχιστον.

Ακολουθεί η **αποθήκευση** (*store*) η οποία είναι ένα κομμάτι με ιδιαίτερο χαρακτήρα αφού σε αυτό υπάρχουν μοναδικά και μόνιμα βιομετρικά χαρακτηριστικά του ανθρώπου, άρα πρέπει να διασφαλίζεται σε απόλυτο βαθμό η ασφάλεια του. Καταλαβαίνουμε ότι σε περίπτωση διαρροής κωδικών μιας υπηρεσίας πέρα από τα αρχικά προβλήματα ασφαλείας το άμεσο μέτρο είναι η αλλαγή των κωδικών με νέους. Τι γίνεται όμως όταν διαρρέονται βιομετρικά στοιχεία που δεν είναι δυνατό να αλλάξουν και το χειρότερο αν χρησιμοποιούνται και σε άλλες κρίσιμες υπηρεσίες; Εδώ λοιπόν πρέπει να έχει προβλεφθεί η κατάλληλη κρυπτογράφηση των δεδομένων με ισχυρούς αλγόριθμους και τεχνικές ώστε να μη μπορεί να υποκλαπούν όπως θα δούμε.

Επόμενη φάση είναι αυτή της **σύγκρισης** (*compare*) του δείγματος με αυτό που υποβάλει ο χρήστης κάθε φορά για είσοδο στο σύστημα. Εδώ πρέπει να δούμε ότι ανάλογα με την εφαρμογή όπως είδαμε παραπάνω να είναι πολύ αυστηρή ή όχι.
Τέλος έχουμε το **αποτέλεσμα** (*result*) στο οποίο αποφασίζεται αν θα γίνει ή όχι δεκτός από το σύστημα ανάλογα με τον αλγόριθμο που ακολουθείται.



Εικόνα 8, στάδια βιομετρικού ελέγχου

Αυτή η προσέγγιση στον έλεγχο πρόσβασης ανοίγει ένα νέο τομέα στην τεχνολογία που τείνει να πάρει την ονομασία Biometric Authentication as a Service (*BioAaaS*) **[36].** Αυτές οι προσεγγίσεις έχουν ανοικτά ερωτήματα ως προς την ιδιωτικότητα και ως προς την προστασία των δεδομένων και τους κινδύνους που μπορεί να ανακύψουν. Όπως θα δείξουμε παρακάτω ο συνδυασμός της γνωστής διαδικασίας εισόδου με κωδικό μαζί με τα keystroke dynamics δημιουργεί ένα πολύ βολικό, γρήγορο, αξιόπιστο και νόμιμο τρόπο για τον έλεγχο της πρόσβασης. Γενικά όμως τα βιομετρικά χαρακτηριστικά μας δίνουν τα εξής **ποιοτικά στοιχεία** ως ιδιότητες που τα κάνουν ιδανικά για την πρόσβαση και τον έλεγχο της, όπως τα:

- Καθολικότητα (*Universality*), δηλαδή τη βεβαιότητα ότι κάθε άνθρωπος εκτός ελαχίστων περιπτώσεων θα κατέχει το συγκεκριμένο βιομετρικό χαρακτηριστικό.

- Διακριτικότητα (*Distinctive*) δηλαδή το χαρακτηριστικό της μοναδικότητας, ότι μόνος ένας άνθρωπος μπορεί να έχει αυτό το στοιχείο.

- Μονιμότητα (*Permanence*), η ιδιότητα της σταθερότητας και της μη μεταβολής στο χρόνο του βιομετρικού χαρακτηριστικού.

- Συλλογή (*Collectability*), η δυνατότητα της σύλληψης των βιομετρικών στοιχείων μέσα από υπάρχουσες τεχνολογίες και η ανάλυση τους με αξιόπιστα ποσοτικά μεγέθη.

Πέρα από αυτά τα σημαντικά ποιοτικά στοιχεία που χαρακτηρίζουν τα βιομετρικά συστήματα πρόσβασης, πολύ σημαντικά θέματα που πρέπει να λαμβάνουμε υπόψη στον σχεδιασμό τους, είναι η **επίδοση** του συστήματος που ουσιαστικά είναι το μέγεθος της ακρίβειας και της ταχύτητας με την οποία εκτελεί όλα τα στάδια του βιομετρικού ελέγχου που είδαμε παραπάνω καθώς και οι περιβαλλοντικοί παράγοντες που τα επηρεάζουν. Η **δεκτικότητα** του συστήματος, που είναι η ανοχή αλλά και η αποδοχή των ατόμων που θα υποβάλουν τα βιομετρικά τους στοιχεία σε καθημερινή βάση και τέλος η δυνατότητα **παραβίασης** τους που δείχνει σε τι επίπεδο το σύστημα θα μπορούσε να ξεγελαστεί από ένα κακόβουλο ή μη εξουσιοδοτημένο χρήστη.

Συνεχίζοντας θα θέλαμε να προσθέσουμε το ότι υπάρχει μια ακόμα κατηγοριοποίηση των βιομετρικών συστημάτων ελέγχου πρόσβασης και την οποία την βρίσκουμε στην βιβλιογραφία ως διαχωρισμό μεταξύ **μονοτροπικών** (*unimodal*) και **πολυτροπικών** (*multimodal*) συστημάτων. Τα unimodal συστήματα περιλαμβάνουν τον έλεγχο μέσω ενός μόνο βιομετρικού στοιχείου του χρήστη σαν τα δακτυλικά αποτυπώματα, ενώ τα multimodal, χρησιμοποιούν περισσότερα από ένα για αύξηση της ακρίβειας και μείωση των false accept ή reject rates, για την εξακρίβωση της ταυτότητας του νόμιμου χρήστη. Ένα παράδειγμα είναι ο συνδυασμός fingerprint reader και keystroke dynamics.

Τα τελευταία χρόνια έχει αναδειχτεί ένα νέο ζήτημα που έχει φέρει στην επιφάνεια την συμβατότητα των αλγορίθμων αναγνώρισης των βιομετρικών που παρέχονται από διαφορετικές εταιρίες ή οργανισμούς ώστε να συγκρίνονται τα δείγματα με τα πρότυπα και έχουν εξελιχθεί με το πέρασμα του χρόνου ώστε να μειώνουν τα σφάλματα. Το πρόβλημα είναι ότι κάθε πάροχος υπηρεσίας έχει εξελίξει με τη δική του τεχνική και με δοκιμές πάνω σε συγκεκριμένες ομάδες δεδομένων (data sets) και πρέπει να εξασφαλιστεί το

ενδιάμεσο λογισμικό (middleware) που θα μπορεί να ταιριάξει υλικό και λογισμικό διαφορετικών εταιρειών. Μια προσέγγιση είναι να λειτουργούν διαφορετικά συστήματα παράλληλα ώστε να εκπαιδεύεται το σύστημα και με διαφορετικό εξοπλισμό και λογισμικό αλλά και εμμέσως με περισσότερες ομάδες δεδομένων ώστε να βελτιωθεί δραματικά η συνολική απόδοση του συστήματος. Αυτή η τεχνική έχει την ονομασία **intramodal fusion** of algorithms **[9].**

2.5 Μειονεκτήματα και πλεονεκτήματα βιομετρικών τεχνολογιών

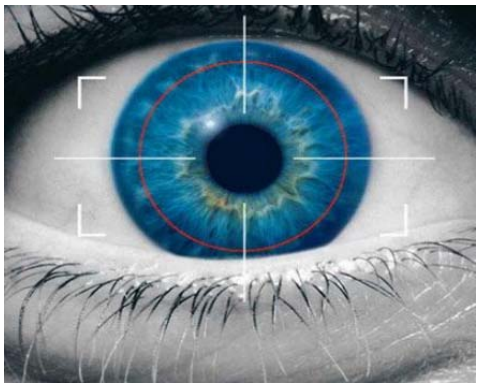
Σε αυτή την υποενότητα θα προσπαθήσουμε να συνοψίσουμε τα μειονεκτήματα και τα πλεονεκτήματα των βιομετρικών τεχνολογιών μέσα από τις μελέτες και τα συμπεράσματα που έχουν εξαχθεί και σύμφωνα με την βιβλιογραφία. Η συνεχώς αυξανόμενη χρήση τους από τα συστήματα ελέγχου ασφαλείας και πρόσβασης τα καθιστά πλέον μέρος της καθημερινής μας ζωής. Κλασικό παράδειγμα οι αυτοματοποιημένες οδηγίες των τηλεφωνικών τραπεζικών υπηρεσιών που χρησιμοποιούν την αναγνώριση της φωνής ώστε να περιηγηθούμε στο μενού και να επιλέξουμε την υπηρεσία που θέλουμε, υποβάλλοντας μέσω της ομιλίας μας ακόμα και ευαίσθητα δεδομένα όπως αριθμούς πιστωτικών καρτών και αυτό χωρίς να μεσολαβεί άνθρωπος διασφαλίζοντας με αυτό το τρόπο την προστασία των δεδομένων μας.

Αυτά βέβαια προϋποθέτουν τη βεβαιότητα ότι έχουμε λάβει υπόψη τα δομικά μειονεκτήματα της κάθε τεχνολογίας που δυνητικά μπορεί να δημιουργήσουν με τη σειρά τους προβλήματα εγκυρότητας, ακρίβειας και αξιοπιστίας, πράγματα που καθορίζονται, αναφέρονται ξεκάθαρα ή και λύνονται στην πολιτική ασφάλειας του κάθε συστήματος. Υπάρχουν όπως είδαμε και παραπάνω οι δυο ουσιαστικές κατηγορίες των βιομετρικών στην βάση της λειτουργικότητας (*functionality*) τους. **[7]** Αυτές είναι οι **ταυτοποίηση** (*identification*), στην οποία γίνεται η αναζήτηση όπως είδαμε σε βάση δεδομένων των βιομετρικών στοιχείων του χρήστη για ανεύρεση του ώστε να απαντήσουμε στην ερώτηση: Ποιο είναι αυτό το άτομο; και η **επικύρωση** (*verification*) στην οποία γίνεται η επικύρωση ότι όντως είναι αυτό το άτομο που ισχυρίζεται και γίνεται με

εμπεριστατωμένη σύγκριση της αποθηκευμένης ταυτότητας με αυτή που υποβάλει ο χρήστης. Το βασικό πλεονέκτημα των βιομετρικών για τον χρήστη είναι ουσιαστικά η ευκολία ότι **δεν χρειάζεται να θυμάσαι ή να κατέχεις** κάποιο συνθηματικό μια που το φέρεις συνέχεια πάνω σου και είναι είτε φυσιολογικό είτε συμπεριφοράς. Αυτά δεν μπορούν ούτε να απολεστούν ούτε να κλαπούν (μπορούν όμως να υποκλαπούν) αλλά ούτε και να ξεχαστούν. Ας εξετάσουμε όμως συγκεκριμένα κάποια από αυτά ώστε να δούμε ποιες είναι όλες οι όψεις της χρηστικότητας τους.
Θα δούμε λοιπόν τις βασικές τεχνολογίες ξεκινώντας από την αναγνώριση της ***ίριδας του ματιού*** η οποία αποτελεί ένα από τους πιο ασφαλείς και ακριβείς τρόπους αναγνώρισης με πολύ μικρά ποσοστά False accept Rate (FAR) και False Reject Rate (FRR) **[35].**

Τα συγκριτικά **πλεονεκτήματα της αναγνώρισης της ίριδας του ματιού** λοιπόν είναι,

- το γεγονός ότι τα μοναδικά της χαρακτηριστικά διαμορφώνονται πλήρως από την ηλικία των 10 ετών και παραμένουν τα ίδια για όλη τη ζωή του ατόμου.
- Η μορφολογία της ίριδας είναι τόσο διακριτή και μοναδική που ακόμα και σε γενετικά όμοιους ανθρώπους όπως τους διδύμους είναι εντελώς διαφορετική.
- Είναι δυνατό να σκαναριστεί με ακρίβεια από την κάμερα από τα 10 εκατοστά μέχρι και μερικά μέτρα απόσταση.



Εικόνα 9, Δείγμα εικόνας ίριδας, [35].

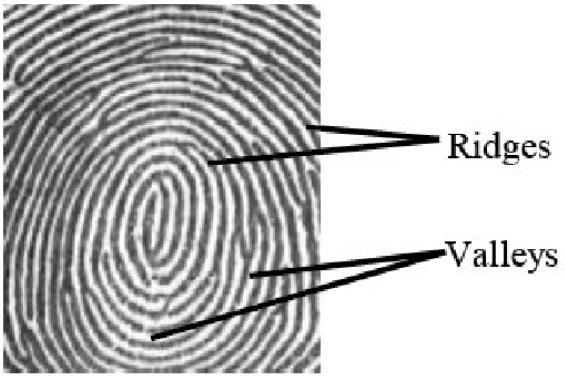
- Μπορεί να εξαχθεί το δείγμα της ίριδας ακόμη και αν το άτομο φοράει φακούς επαφής ή γυαλιά διόρθωσης όρασης. Εξαίρεση εδώ είναι οι χρωματιστοί φακοί επαφής και βέβαια τα γυαλιά ηλίου.
- Έχει επιδείξει υψηλά ποσοστά ακρίβειας και ταχύτητας αναγνώρισης με 2 δευτερόλεπτα για χρόνο επεξεργασίας του δείγματος.
- Δεν απαιτεί φυσική επαφή για το σκανάρισμα της συμβάλλοντας στην μείωση του αισθήματος της ενόχλησης.
- Έχει αποδειχτεί μέσα από την χρήσης ως ένας αξιόπιστος τρόπος αναγνώρισης ατόμου.

Τα **μειονεκτήματα της αναγνώρισης της ίριδας του ματιού** είναι,

- Τα σκάνερ της ίριδας μπορούν να ξεγελαστούν με μια υψηλής ποιότητας φωτογραφίας αντί της πραγματικής.
- Τα μηχανήματα είναι δύσκολο να ρυθμιστούν και μπορεί να είναι άβολα ή δύσχρηστα για κάποιους ανθρώπους πχ λόγω ύψους.
- Η ακρίβεια τους μπορεί να επηρεαστεί λόγω εξωτερικών συνθηκών όπως έντονο φως ή ανακλάσεις.
- Ο εξοπλισμός δειγματοληψίας της ίριδας είναι συνήθως πιο ακριβός και εξεζητημένος και απαιτεί ρυθμίσεις όπως καλιμπράρισμα και συντήρηση.
- Έχει όρια στην απόσταση ελέγχου τα μερικά μέτρα.
- Η αξιοπιστία και η ακρίβεια του δείγματος μπορεί να επηρεαστεί από ανθρώπινες παθήσεις όπως ο Διαβήτης.

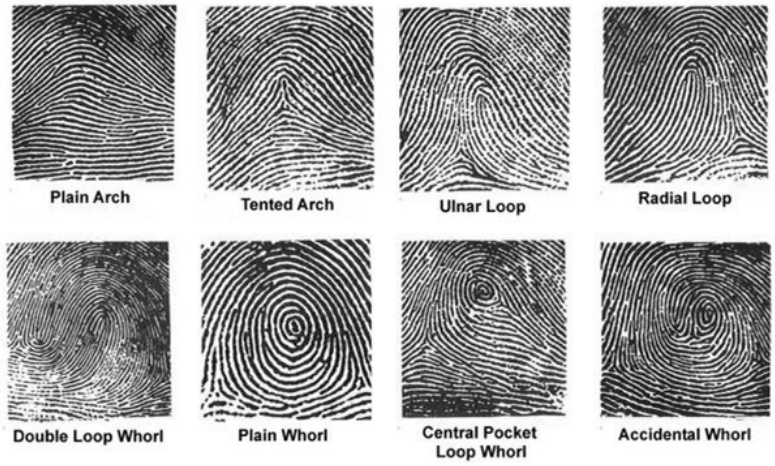
Συνεχίζοντας τις βασικές τεχνολογίες θα δούμε τα πολύ γνώριμα σε όλους μας **δακτυλικά αποτυπώματα** (*finger prints*) τα οποία είναι μοναδικά σε κάθε άνθρωπο και όπως είδαμε το πιο παλαιό βιομετρικό που έχει χρησιμοποιηθεί μαζικά και με επιτυχία ήδη από τον 19ο αιώνα και στο οποίο αξίζει να σταθούμε λίγο. Έχει τα χαρακτηριστικά όπως είδαμε πιο πάνω που πρέπει να κατέχει κάθε αξιόπιστο βιομετρικό δηλαδή την μοναδικότητα που μόλις είπαμε, αλλά και την καθολικότητα δηλαδή ότι το συναντούμε σε κάθε άνθρωπο. Επίσης έχει την ιδιότητα της μονιμότητας δηλαδή παραμένει αμετάβλητο (σε κανονικές συνθήκες) καθόλη την διάρκεια ζωής του ανθρώπου και μπορεί να συλλεχθεί με κατάλληλες ποσοτικές μεθόδους με μεγάλη ακρίβεια. Τα βασικά μοναδικά

χαρακτηριστικά που του δίνουν την μοναδικότητα τους είναι το διακριτό σχήμα και η γεωμετρία τους που ουσιαστικά είναι οι **κοιλάδες** και οι **παρυφές** που σχηματίζονται επιφανειακά στο ανθρώπινο δέρμα των χεριών. Αυτά τα δυο τα συναντούμε με τα ονόματα valley και ridge αντίστοιχα. Μπορούμε να τις ξεχωρίσουμε αφού με έντονο και πιο σκούρο χρωματισμό φαίνονται οι παρυφές που είναι τα εξογκωμένα κομμάτια, ενώ οι κοιλάδες είναι πιο ανοικτός ο χρωματισμός και σε πιο χαμηλό επίπεδο με τις αποστάσεις μεταξύ τους να κυμαίνονται από 100 έως και 300 μικρόμετρα. Αυτά σχηματίζουν μοναδικές γεωμετρικές καμπυλότητες ώστε επιλέγοντας συγκεκριμένα σημεία να μπορούμε να ταυτοποιήσουμε με ακρίβεια τον άνθρωπο με κατάλληλη τεχνική όπως σκάνερ.



Εικόνα 10, παρυφές και κοιλάδες των δακτυλικών αποτυπωμάτων, [17]

Οι παρυφές και οι κοιλάδες μπορούν να διακλαδώνονται ή να τερματίζουν σε τυχαίο σημείο σχηματίζοντας μοναδικά γεωμετρικά σχήματα σε όποιο βαθμό τα απομονώσουμε και έχουν την ονομασία singular region με ιδιαίτερα σημεία τα δέλτα (delta) και τα κεντρικά (core) σύμφωνα με την διεύθυνση ή την κατεύθυνση που διατρέχουν. Με αυτή τη διάταξη μπορούν να χαρακτηριστούν με τις ονομασίες Τόξο, Βρόγχος και Δακτύλιος με διάφορους συνδυασμούς και επεκτάσεις όπως διπλός Βρόγχος όταν υπάρχει δυο φορές τέτοιος σχηματισμός.



Εικόνα 11, Οι διάφοροι σχηματισμοί των δακτυλικών αποτυπωμάτων [35]

Συνεχίζουμε στα **πλεονεκτήματα** των δακτυλικών αποτυπωμάτων **[35]** τα οποία είναι τα εξής:

- Τα συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων είναι πλέον οικονομικά και εύκολα στη χρήση.
- Τα δακτυλικά αποτυπώματα έχουν το στοιχείο όπως είδαμε της μονιμότητας, παραμένουν δηλαδή αμετάβλητα στη πάροδο του χρόνου.
- Μπορούν να ταυτοποιήσουν μοναδικά όλους τους ανθρώπους εκτός από ένα 2% λόγω τραυματισμών του δέρματος ή κάποιους κληρονομικούς παράγοντες.
- Είναι ώριμη τεχνολογία και έχει επικρατήσει με τα χρόνια ως τρόπος φυσιολογικού βιομετρικού.
- Τα σκάνερ πλέον λειτουργούν με υψηλή ποιότητα μειώνοντας σχεδόν εντελώς τα περιστατικά σφάλματος ή κακόβουλου αντιγράφου.
- Έχουν το πλεονέκτημα όλων των βιομετρικών, το να μη χρειάζεται να θυμάσαι κωδικούς ή να έχεις κάρτες και token.
- Έχουν ευκολία χρήσης και ταχύτητα επεξεργασίας του δείγματος.

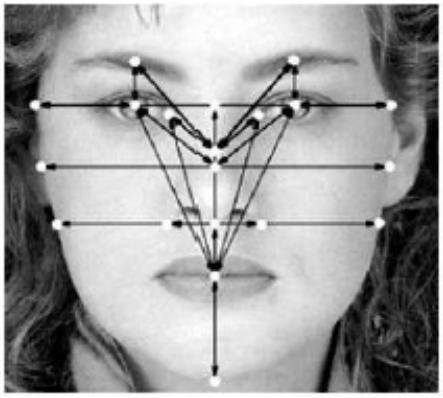
Τώρα ως προς τα **μειονεκτήματα** των δακτυλικών αποτυπωμάτων μπορούμε να αναφέρουμε τα ακόλουθα,

- Η δειγματοληψία γίνεται σε ένα τομέα του δακτύλου με αποτέλεσμα σε περίπτωση μη καλής αρχικής εφαρμογής να υπάρχει πιθανότητα σφαλμάτων.

- Υπάρχουν σύγχρονες μέθοδοι υφαρπαγής, αντιγραφής και χρησιμοποίησης των δακτυλικών αποτυπωμάτων του νόμιμου κατόχου.
- Η αρχική εισαγωγή πιθανό να χρειαστεί να επαναληφθεί.
- Τα αποτυπώματα σε ανθρώπους που εργάζονται σε συγκεκριμένους τομείς όπως χημικής βιομηχανία ή μηχανολογία μπορούν να επηρεαστούν.
- Διάφορες αιτίες όπως γρατζουνιές, κοψίματα μπορούν να επηρεάσουν το αποτέλεσμα.
- Τα αποτυπώματα μας δεν είναι εντελώς ασφαλή μια που τα αφήνουμε παντού κυριολεκτικά κάθε ημέρα και εφόσον υποκλαπούν η ζημιά είναι μόνιμη αφού δεν μπορούμε να τα αλλάξουμε όπως θα κάναμε με ένα password.

Θα συνεχίσουμε με μια τρίτη βιομετρική τεχνολογία, αυτή της **αναγνώρισης του προσώπου** (*face recognition*) **[2].**

Τα φυσικά βασικά χαρακτηριστικά του προσώπου (μάτια, μύτη, χείλια, φρύδια, αυτιά και σαγόνι) έπαιζαν πάντα τον κρισιμότερο ρόλο στην αναγνώριση των προσώπων. Λόγω της γεωμετρίας του ανθρώπινου προσώπου και των σημείων που ενώνουν τα ανωτέρω σημεία έγινε αντιληπτό ότι μπορεί να χρησιμοποιηθεί ως ένα βιομετρικό στοιχείο αναγνώρισης. Τα γεωμετρικά σημεία του προσώπου που συνήθως συγκρίνονται φαίνονται στην ακόλουθη εικόνα.



Εικόνα 12, γεωμετρικά σημεία ελέγχου αναγνώρισης προσώπου,[2]

Για να γίνει αυτό αρχικά χρησιμοποιήθηκε η στατική εικόνα του ατόμου σε κάμερα για αντιπαραβολή με την αποθηκευμένη εικόνα του, και από αυτό έχει

την ονομασία στατική αναγνώριση προσώπου. Πρόσφατα όμως και όπως είδαμε και από την περίπτωση της Τάμπα στη Φλόριδα των ΗΠΑ το 2001, έχει ξεκινήσει η σε πραγματικό χρόνο αναγνώριση προσώπων μέσα σε πλήθος ανθρώπων από κάμερες υψηλής ανάλυσης που σκάναρουν πολλαπλές φορές τα πρόσωπα και συγκρίνουν τις λήψεις με τα αποθηκευμένα πρόσωπα που τους ενδιαφέρουν.
Έρευνες πραγματοποιούνται ώστε να επιτευχθεί ακόμα μεγαλύτερη ακρίβεια και αξιοπιστία της αναγνώρισης με χρήση τρισδιάστατων λήψεων με συνδυασμό καμερών καθώς και πιο ευαίσθητους αισθητήρες στις κάμερες λήψης ώστε να εντοπίζονται περισσότερα στοιχεία του προσώπου όπως τυχόν σημάδια ή ρυτίδες μειώνοντας περισσότερο τα σφάλματα.

Τα **πλεονεκτήματα της αναγνώρισης προσώπου** που θα μπορούσαμε να πούμε είναι τα εξής **[35]**

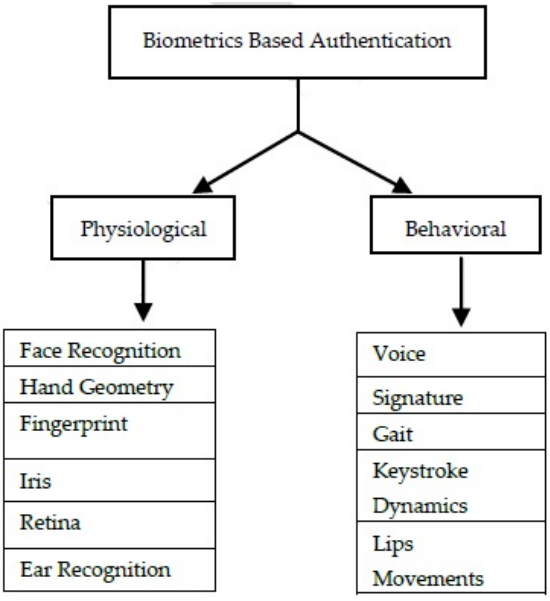
- Δεν απαιτεί την συνεργασία του ατόμου για τη λήψη του δείγματος.
- Σε σύνδεση με το προηγούμενο δεν απαιτεί άμεση ή συγκεκριμένη επαφή με το άτομο πράγμα που βοηθάει σε εισόδους χώρων εργασίας χωρίς να είναι πολύ επεμβατικό στην ιδιωτικότητα του ατόμου.
- Το ανωτέρω του προσφέρει και το τίτλο της φιλικότητας προς το χρήστη (user-friendly).
- Συστήματα σε αεροδρόμια, γήπεδα και ανοικτούς χώρους μπορούν να εντοπίσουν κάποιον ύποπτο (ή μια ομάδα από ύποπτους που πλησιάζουν στο προφίλ του) ανάμεσα σε μεγάλο αριθμό ανθρώπων.
- Το προηγούμενο είναι και το μεγάλο πλεονέκτημα του, το ότι μπορεί να κάνει ελέγχους μεγάλης κλίμακας πράγμα που δεν μπορεί να επιτύχει άλλο βιομετρικό στοιχείο.
- Μπορεί να ταυτοποιήσει σε δεύτερο χρόνο σε επέμβαση περιστατικού (incident response) ασφάλειας συγκρίνοντας τις αποθηκευμένες ήδη λήψεις με την πρόσφατη φωτογραφία του ατόμου που είναι ύποπτος (reverse investigation).

Ας δούμε τώρα τα **μειονεκτήματα της αναγνώρισης προσώπου** ως βιομετρική μέθοδο ελέγχου:

- Η αναγνώριση προσώπου δεν μπορεί πάντα να αποδώσει λόγω των συνθηκών που μπορεί να επικρατούν (φως, εμπόδια, ταχύτητα και κατεύθυνση ατόμου για να αναφέρουμε μόνο μερικά)
- Το ντύσιμο του ατόμου όπως κουκούλες, σκούφοι, γυαλιά ηλίου, καπέλα, μακριά μαλλιά μπορούν να κάνουν αδύνατο τον εντοπισμό.
- Η ποιότητα και η ευκρίνεια της εικόνας παίζει σημαντικό ρόλο.
- Πολλά συστήματα αδυνατούν να εντοπίσουν άτομα που παίρνουν διάφορες εκφράσεις στο πρόσωπο οι οποίες αλλοιώνουν τα χαρακτηριστικά και την γεωμετρία του. Παράδειγμα είναι η έκφραση του προσώπου που έχουμε στην φωτογραφία του διαβατηρίου και η οποία είναι πολύ επίσημη και σοβαρή, πράγμα που λίγες φορές έχουμε στην διάρκεια της ημέρας. Αυτό αποτελεί και τη σοβαρή αδυναμία αυτής της μεθόδου.
- Περίπλοκο και ακριβό σύστημα ελέγχου σε σχέση με άλλα.

Είδαμε δυο από τις βασικές φυσιολογικές βιομετρικές τεχνολογίες για να δούμε με πιο τρόπο επιτυγχάνεται η αναγνώριση και ποια είναι τα πλεονεκτήματα τους αλλά και ποιοι είναι οι περιορισμοί της κάθε τεχνολογίας.

Θα δούμε τώρα και ένα βιομετρικό στοιχείο συμπεριφοράς όπως είναι η **αναγνώριση της ομιλίας** (*voice recognition*) και θα ασχοληθούμε εκτενώς με ένα άλλο βιομετρικό της συμπεριφοράς που είναι και το θέμα της διατριβής, την δυναμική του ρυθμού πληκτρολόγησης στο επόμενο κεφάλαιο. Θυμίζουμε ότι τα βιομετρικά χωρίζονται σε δυο κατηγορίες **[2]** που περιέχουν κυρίως αλλά δεν περιορίζονται μόνο σε αυτά που είναι τα εξής,



Εικόνα 13, βιομετρικές τεχνολογίες, [2]

Η αναγνώριση της ομιλίας του ανθρώπου είναι ένα βιομετρικό στοιχείο συμπεριφοράς (*behavioral*). Αυτό σημαίνει ότι η φωνή λαμβάνεται από μια μονάδα εισόδου το μικρόφωνο, μετατρέπεται σε ηλεκτρικό σήμα και μετά μετατρέπεται και αποθηκεύεται για περαιτέρω επεξεργασία. Αυτό το σήμα περιλαμβάνει ένα φάσμα συχνοτήτων που χαρακτηρίζει μοναδικά τον άνθρωπο.

Εικόνα 14, Φάσμα συχνοτήτων δείγματος αναγνώρισης φωνής,[35]

Η φωνή του ανθρώπου θα μπορούσαμε να πούμε ότι συνδυάζει φυσιολογικό και συμπεριφορικό βιομετρικό. Και αυτό γιατί τα χαρακτηριστικά της ομιλίας καθορίζονται από την φυσιολογία του σώματος δηλαδή του στόματος, της

μύτης, των χειλιών, των φωνητικών χορδών για να αναφέρουμε τα πιο κύρια. Αλλά καθορίζονται τελικά ως συμπεριφοράς κύρια γιατί επηρεάζεται από την ηλικία, την εκπαίδευση, την συναισθηματική κατάσταση και την υγεία του ατόμου. Η καταγραφή της από μικρόφωνο επηρεάζεται σε μεγάλο βαθμό από τον θόρυβο ή τις παρεμβολές του περιβάλλοντος. Τα **πλεονεκτήματα** αυτής της μεθόδου αναγνώρισης είναι,

- Η ομιλία θεωρείται μια βιομετρική είσοδος που δεν απαιτεί πολλές δοκιμές ή εκπαίδευση από τον χρήστη και για αυτό είναι πιο γρήγορη μέθοδος από άλλες.
- Θεωρείται μη επεμβατική και δεν χρειάζεται καμία ενέργεια ή χειρισμό από τον χρήστη πέρα από το να πει κάποια συγκεκριμένη λέξη ή πρόταση.
- Είναι ιδανική για ανθρώπους που δεν μπορούν να χρησιμοποιήσουν τα χέρια τους λόγω κινητικού προβλήματος, μυϊκής ασθένειας ή άλλης δυσχέρειας.
- Γίνεται αποφυγή προβλημάτων που μπορεί να παρουσιαστούν με άλλες εισαγωγές όπως τα πληκτρολόγια λόγω ελλιπούς βασικής εκπαίδευσης ή λόγω μαθησιακών δυσκολιών με αποτέλεσμα ανορθογραφία ή αναγραμματισμός ή αναριθμητισμός.
- Μεγαλύτερη ταχύτητα μεθόδου λόγω του ότι οι περισσότεροι άνθρωποι μιλούν γρηγορότερα από ότι πληκτρολογούν ή χειρίζονται άλλες συσκευές εισόδου.

Ως **μειονεκτήματα** μπορούμε να αναφέρουμε τα εξής,

- Συστήματα επιρρεπή σε θορύβους που μπορούν να οδηγήσουν σε σφάλμα δειγματοληψίας του δείγματος, λόγω της λήψης του από μικρόφωνο.
- Πρέπει να υπάρχει μικρή απόσταση του χρήστη από το μικρόφωνο ώστε να γίνεται σωστή λήψη της φωνής. Όσο αυξάνει η απόσταση μεγαλώνουν τα σφάλματα δειγματοληψίας.
- Μπορεί να παραβιαστεί μέσω προ-ηχογραφημένου μηνύματος από κάποιον χάκερ ή άλλο κακόβουλο άτομο.

- Απαιτεί χρόνο στην αρχική δειγματοληψία λόγω ρυθμίσεων στη φωνή του κάθε χρήστη.
- Προβλήματα λόγω προφοράς από χρήστες που μιλούν διαφορετικές γλώσσες.
- Προβλήματα λόγω ομοιότητας ήχων λέξεων μεταξύ τους όπως οι αγγλικές λέξεις two, to και too.
- Ακριβός εξοπλισμός σύλληψης, επεξεργασίας και αποθήκευσης σήματος αρχικών δειγματοληψιών.

Από ότι είδαμε μέχρι τώρα με τις τρεις μεθόδους βιομετρικού ελέγχου πρόσβασης κάθε μια έχει θετικά, αρνητικά και κάποια είναι καταλληλότερα από άλλα βάσει του πεδίου εφαρμογής που χρησιμοποιούνται. Στον ακόλουθο πίνακα συνοψίζονται τα στοιχεία της κάθε μιας μεθόδου που εξετάσαμε καθώς και κάποιες άλλες για αναφορά.

Biometrics	Accuracy	Cost	Size of template	Long term stability	Security level
Facial recognition	Low	High	Large	Low	Low
Iris scan	High	High	Small	Medium	Medium
Finger print	Medium	Low	small	Low	Low
Finger vein	High	Medium	Medium	High	High
Voice recognition	Low	Medium	Small	Low	Low
Lip recognition	Medium	medium	Small	Medium	High

Εικόνα 15, σύγκριση βιομετρικών τεχνολογιών σύμφωνα με τα χαρακτηριστικά ασφαλείας τους, [35]

2.6 Τύποι βιομετρικών τεχνολογιών behavioral biometrics

Θα συνεχίσουμε με τα συμπεριφορικά βιομετρικά δηλαδή τα βιομετρικά που σχετίζονται με τη συμπεριφορά και το τρόπο που διακρίνει μοναδικά το άτομο από άλλα, όπως η υπογραφή, ο γραφικός χαρακτήρας, ο ρυθμός

πληκτρολόγησης, ο τρόπος χρήσης οθόνων αφής, το περπάτημα, ο τρόπος ομιλίας, ο τρόπος κίνησης του ποντικιού, ώστε να μας βοηθήσει να καταλάβουμε την φυσιολογία και τον μηχανισμό που επιτυγχάνεται η αναγνώριση, πράγμα το οποίο θα μας φανεί χρήσιμο στην εξέταση των keystroke dynamics.
Αυτό το είδος βιομετρικών δεν είναι αποτέλεσμα βιολογικών και φυσιολογικών στοιχείων που δίνουν στο άτομο εκ γενετής βιομετρικά αμετάβλητα στοιχεία όπως τα δακτυλικά αποτυπώματα αλλά χαρακτηρίζουν τον τρόπο που έχει μάθει ο συγκεκριμένος άνθρωπος να εκτελεί αυτές τις καθημερινές λειτουργίες, τρόπος που τελικά τον διακρίνει μοναδικά από κάποιον άλλο και μπορεί να χρησιμοποιηθεί για εξακρίβωση της ταυτότητας του.
Μεγάλο πλεονέκτημα αυτών των βιομετρικών είναι ότι σε μεγάλο βαθμό δεν απαιτούν εξειδικευμένο εξοπλισμό και μπορούν να συλλεχθούν από τις ήδη διαθέσιμες συσκευές εισόδου (μικρόφωνο, πληκτρολόγιο, οθόνες αφής) απαιτώντας μόνο το ανάλογο λογισμικό σύγκρισης και ελέγχου. Αυτό το στοιχείο κάνει πιο απλή αλλά και πιο οικονομική, την ανάπτυξη και επέκταση αυτών των βιομετρικών.

Πρέπει πάντα να έχουμε στο μυαλό μας κατά τη σχεδίαση τέτοιων συστημάτων ποια μέθοδος είναι η καταλληλότερη για την συγκεκριμένη εφαρμογή ή και συνδυασμός αυτών. Για να γίνει αυτό πρέπει να έχουμε καταλήξει σε κάποια κριτήρια αξιολόγησης ώστε να βγάλουμε ασφαλή συμπεράσματα. Στην ακόλουθη εικόνα έχουμε ένα πίνακα **[19]** στον οποίο βλέπουμε το πλήθος των κριτηρίων ώστε να υπολογίσουμε κάθε πιθανή παράμετρο, έχοντας στο μυαλό μας πάντα το συνολικότερο επίπεδο ασφάλειας των πληροφοριών, των δεδομένων και των υπολογιστικών συστημάτων με τις μονάδες και τις συσκευές που την αποτελούν. Ειδικά στον τομέα των βιομετρικών αυτό αποτελεί την απόλυτη πρόκληση αφού σε ενδεχόμενη απώλεια τους δεν μπορούμε να τα αλλάξουμε ή να τα αντικαταστήσουμε.
Θα αναλύσουμε την αναγνώριση υπογραφής ως τρόπο βιομετρικού συμπεριφοράς μια που χρησιμοποιήθηκε και πριν την έλευση της ψηφιακής τεχνολογίας για αξιόπιστη μέθοδο εξακρίβωσης της ταυτότητας.

ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΒΙΟΜΕΤΡΙΚΗΣ ΜΕΘΟΔΟΥ	
1	Καπάλληλος αλγόριθμος
2	Ασφαλής αλγόριθμος
3	Σωστή επιλογή κρυπτογραφικών κλειδιών
4	Ασφαλής Βάση Δεδομένων
5	Ασφαλή Πρωτόκολλα
6	Ασφαλή Δίκτυα και Καταπεμπένα Συστήματα
ΚΡΙΤΗΡΙΑ ΕΠΙΛΟΓΗΣ ΒΙΟΜΕΤΡΙΚΗΣ ΣΥΣΚΕΥΗΣ	
1	**Λειτουργικά**
1.1	Ευκολία χρήσης ▪ Ελάχιστος χρόνος εγγραφής, αυθεντικοποίησης – επαλήθευσης του χρήστη ▪ Ελάχιστες ενέργειες του χρήστη ▪ Ελάχιστη εκπαίδευση του χρήστη ▪ Ελάχιστη αποθήκευση στοιχείων
1.2	Αποδοχή του κοινού ▪ Φιλικότητα ως προς το χρήστη ▪ Ασφάλεια χρήστη ▪ Κανονεσηθικής ▪ Συμβατότητα με άλλες μεθόδους ▪ Προστασία ιδιωτικότητας ▪ Ευκολία χρήσης ▪ Αξιοπιστία
1.3	Μοναδικότητα (ως προς το αποτέλεσμα)
1.4	Ανθρώπινοι παράγοντες ▪ Μη οχληπικό (χωρίς φυσική επαφή με το χρήστη) ▪ Χωρίς διακρίσεις (ενάντια σε ηλικία, επάγγελμα, φυλή κλπ)

2	**Τεχνικά**
2.1	Ελάχιστος χρόνος αυθεντικοποίησης
2.2	Χαμηλό επίπεδο αποδοχής σφάλματος
2.3	Αποτελεσματικότητα
2.4	Ταχύτητα
2.5	Ακρίβεια
2.6	Ανεξάρτητο από περιβαλλοντολογικές συνθήκες
3	Οικονομικά
3.1	Κόστος εξοπλισμού
3.2	Κόστος εγκατάστασης
3.3	Κόστος εκπαίδευσης
3.4	Κόστος και χρόνος αναβάθμισης
3.5	Κόστος προστασίας του εξοπλισμού
4	Κατασκευαστές
4.1	Υποστήριξη
4.2	Ανταλλαγή δεδομένων

Εικόνα 16, Πίνακας Κριτηρίων Βιομετρικών Μεθόδων, [19]

Η **αναγνώριση υπογραφής** (*signature recognition*) είναι η χειρόγραφη αναπαράσταση του ονόματος, του επωνύμου ή μιας συντομογραφίας αυτών και έχει καθιερωθεί ως μέθοδος πιστοποίησης της ταυτότητας του ανθρώπου σε κρίσιμες εφαρμογές όπως τραπεζικές και συμβολαιογραφικές εργασίες. Η υπογραφή είναι ένα αποτέλεσμα από τον τρόπο που γράφει κάποιος και τις επαναλήψεις που έχει κάνει για να αποκτήσει μια σχεδόν πανομοιότυπη υπογραφή κάθε φορά. Την σύγχρονη εποχή χωρίζεται πλέον σε δυο κατηγορίες, την **online** στην οποία η υπογραφή εισάγεται σε συσκευές εισόδου όπως tablet, pen displays ή άλλο touch screen κατά την οποία λαμβάνεται και συγκρίνεται με τα ήδη αποθηκευμένα δείγματα και τη συνάφεια των σχημάτων, τον προσανατολισμό, ακόμα και την πίεση σε συγκεκριμένα σημεία. Αφού συγκριθεί επιστρέφει το ποσοστό της ταύτισης (matching)**[16].**

Εδώ να πούμε ότι κάνουμε μια εισαγωγή με την υπογραφή γιατί αυτή η μέθοδος με αυτά τα χαρακτηριστικά έχει την ονομασία signature dynamics δηλαδή δυναμική της υπογραφής, πράγμα που θα ξαναδούμε και στα keystroke dynamics.

Η δεύτερη κατηγορία λοιπόν είναι η **offline** κατά την οποία η σύλληψη της υπογραφής επιτυγχάνεται με σκάνερ και επειδή γίνεται η αποθήκευση της καλύτερης και ευκρινέστερης έκδοσης χάνεται το στοιχείο της αρχικής εκπαίδευσης του αλγορίθμου για την δυναμική του τρόπου γραφής (πως γράφει, με τι προσανατολισμό, πίεση κ.α.).

Για να είναι η μέθοδος αξιόπιστη στην επιβεβαίωση της ταυτότητας των ατόμων πρέπει ο τρόπος που υπογράφει κάποιος να επαναλαμβάνει με αρκετή ακρίβεια αυτή κάθε φορά ώστε κάποιος που θέλει να τη πλαστογραφήσει να γίνεται αντιληπτός. Ως βιομετρικό η υπογραφή λόγω της έστω και ελάχιστα διαφορετικού κάθε φορά τρόπου γραφής κατανοούμε ότι δεν έχει το στοιχείο της μονιμότητας (*permanence*) σε τέτοιο βαθμό που το έχει ένα άλλο φυσιολογικό βιομετρικό και το όριο της αποδοχής της από το σύστημα πρέπει να προβλέπει τους επίδοξους πλαστογράφους. Εδώ λοιπόν είναι το πλεονέκτημα της δυναμικής online υπογραφής γιατί δίνεται σημασία και στον τρόπο αλλά και το ρυθμό που ο άνθρωπος υπογράφει, πράγμα που δυσκολεύει πολύ κάποιον

κακόβουλο. Σε περίπτωση υποκλοπής της υπογραφής είτε ψηφιακά είτε εγγράφως μπορεί να αλλάξει ως μη μόνιμο βιομετρικό, πιο εύκολα έστω, σε αντίθεση με την ίριδα του ματιού για παράδειγμα.

Ποια είναι τα στοιχεία όμως που απαρτίζουν την γραφή μας και που μπορούν να χρησιμοποιηθούν ως παράμετροι ελέγχου της μοναδικότητας, άρα και της ταυτότητας του χρήστη; Χρησιμοποιούμε τις συντεταγμένες τις τροχιάς της γραφής (*trajectory coordinates*) αλλά και άλλα όπως το βαθμό της πίεσης που ασκείται πάνω στη πένα, η αρχική επιτάχυνση αλλά και η ταχύτητα της γραφής καθώς και η γωνία κλίσης της πένας (pen-tilt) **[47],[48].**
Ουσιαστικά αυτές οι παράμετροι μπορούν να ταξινομηθούν σε δυο κατηγορίες τις καθολικές (*global*) και τις τοπικές (*local*). Ως **global** χαρακτηριστικά θεωρούμε την ταχύτητα της γραφής, το συνολικό εμβαδό ενός ιδεατού τετραγώνου που καταλαμβάνουμε για την υπογραφή μας (*bounding box*), ανάλυση Φουριέ των συντεταγμένων της τροχιάς της, ο αριθμός των επαφών της πένας με την οθόνη καθώς και η ροή της υπογραφής. Τα **local** χαρακτηριστικά ουσιαστικά απεικονίζουν τη σχέση μεταξύ δυο σημείων για παράδειγμα την απόσταση και τη κλίση μεταξύ τους.
Οι άνθρωποι βεβαίως δεν γράφουν με το ίδιο ακριβώς τρόπο κάθε φορά αλλά υπάρχουν μικροδιαφορές στον τρόπο γραφής τους και τα συστήματα προνοούν για μικρές παρεκκλίσεις στο μοτίβο αλλά τα περισσότερα συστήματα δίνουν σημασία στη δυναμική της γραφής και όχι στο κατεξοχήν κείμενο ή υπογραφή δηλαδή όλα τα στοιχεία που είδαμε παραπάνω. Παρόλα αυτά έχει φανεί ότι η ταχύτητα σαν χαρακτηριστικό είναι σημαντική παράμετρος σε τέτοιο βαθμό που μπορεί να γίνει αποδεκτή από πλαστογράφο παρά τις διαφορές στο σχήμα της υπογραφής **[11].** Το τυπικό μέγεθος αρχείου που χρησιμοποιείται κατά την εισαγωγή της υπογραφής είναι περίπου τα 20ΚΒ. Το αντίστοιχο αρχείο της αποθηκευμένης πρότυπης υπογραφής που συγκρίνεται με το υποβαλλόμενο περιέχει περίπου 3 με 10 δείγματα προτύπων και κυμαίνεται σε μερικά ΚΒ. Η ακρίβεια της αναγνώρισης υπογραφής κυμαίνεται τελικά με FAR= 8% και FRR=2%.

Η επέκταση της τεχνολογίας αναγνώρισης της υπογραφής μας ανοίγει τους ορίζοντες για τη πλήρη αναγνώριση της γραφής ως κείμενο και όχι μόνο στο πεδίο της υπογραφής ή της μονογραφής, πράγμα θα μπορούσε να χρησιμοποιηθεί ως δεύτερο βαθμό ελέγχου με εισαγωγή μικρού χειρόγραφου κειμένου όπως τη πόλη που γεννηθήκατε ή ποιο είναι το όνομα της μητέρας σας. Με αυτό τον τρόπο θα μπορούσε να γίνεται αντιπαραβολή με περισσότερο εμβάθυνση στο βιομετρικό στοιχείο του τρόπου της γραφής του ατόμου, μεγαλώνοντας τον βαθμό της ασφάλειας.

2.7 Επιθέσεις σε βιομετρικά συστήματα

Η έλευση των βιομετρικών και η επακόλουθη αύξηση των μέτρων ασφαλείας στα συστήματα είτε συμβατικά είτε ψηφιακά, έφερε και την ανάγκη των επιτηδείων και των κακόβουλων ανθρώπων για εξέλιξη δηλαδή να κινηθούν προς την αναζήτηση τρόπων παραβίασης των ελέγχων εξακρίβωσης της ταυτότητας δηλαδή της ταυτοποίησης ώστε να μπορούν να αποκτήσουν ψηφιακή πρόσβαση ή μέσω της πλαστοπροσωπίας να υποδύονται τον νόμιμο κάτοχο της ταυτότητας και να επιτυγχάνουν πρόσβαση σε ευαίσθητες υπηρεσίες όπως κρατικές, στρατιωτικές, τραπεζικές ή νομικές. Αυτή η πράξη ονομάστηκε και έχει επικρατήσει πλέον ως κλοπή της ταυτότητας ή **identity theft** και σε αυτή την υποενότητα θα ασχοληθούμε με το ψηφιακό μέρος των μεθόδων και των τρόπων που χρησιμοποιούνται.

Στον σχεδιασμό της ασφάλειας των υπολογιστικών συστημάτων λαμβάνουμε υπόψη το γεγονός των αμέτρητων κινδύνων, και ο κύριος σκοπός της είναι η απαγόρευση χρήσης των υπολογιστικών συστημάτων και πόρων από μη εξουσιοδοτημένο χρήστη αλλά και ταυτόχρονα η προστασία των δεδομένων και της πληροφορίας από άμεση ή έμμεση απώλεια, αποκάλυψη ή τροποποίηση τους. Για να προστατέψουμε τα ευαίσθητα δεδομένα των βιομετρικών στοιχείων θα πρέπει να πάρουμε μέτρα που καλύπτουν τους εξής κύριους άξονες:

- ❖ Στρατηγική οργάνωσης και διαχείρισης της ασφάλειας του πληροφοριακού συστήματος με δημιουργία κατάλληλης πολιτικής ασφάλειας.
- ❖ Σχεδιασμός, ανάπτυξη και συντήρηση των πληροφοριακών πόρων με όλες τις προδιαγραφές ασφάλειας.

Όπως γνωρίζουμε πλέον λόγω των δισεκατομμυρίων χρηστών των κάθε είδους συσκευών όπως έξυπνα τηλέφωνα, λάπτοπ, ΗΥ και τάμπλετ που είναι σχεδόν πάντα συνδεδεμένα στο διαδίκτυο, η ασφάλεια των πληροφοριών και των επικοινωνιών έχει γίνει πιο κρίσιμη από ποτέ. Ειδικό βάρος έχει πέσει στο να δημιουργηθούν μέθοδοι και εφαρμογές που να εξακριβώνουν την πραγματική ταυτότητα του νόμιμου χρήστη. Τα βιομετρικά είναι ένας ασφαλής και σίγουρος τρόπος ταυτοποίησης του χρήστη, αλλά ταυτόχρονα και ένα στοιχείο που μπορεί να υποκλαπεί σε οποιαδήποτε στιγμή και να χρησιμοποιηθεί από ένα κακόβουλο άτομο. Λόγω της ιδιότητας των βιομετρικών στοιχείων να μην μπορούν να είναι απόρρητα και απροσπέλαστα τον καθένα (τουλάχιστον τα πιο πολλά) όπως ακριβώς τα δακτυλικά αποτυπώματα που τα αφήνουμε σε εκατοντάδες σημεία κάθε ημέρα, μπορούν σχετικά εύκολα να ληφθούν, να αντιγραφούν και να χρησιμοποιηθούν.

Για το λόγο αυτό γίνονται έρευνες βελτίωσης της χρήσης των βιομετρικών όπως τη ''**liveness detection**'' δηλαδή τη δυναμική και όχι στατική καταγραφή των βιομετρικών στοιχείων ή αλλιώς την απαίτηση από το σύστημα λήψης περισσότερων από ένα δείγμα βιομετρικών για πολλαπλή σύγκριση ώστε να επικυρωθεί ότι ο φορέας του βιομετρικού είναι ο πραγματικός και όχι κάποιος πλαστογράφος **[32].**

Επίσης ερευνητική ανάπτυξη έχει το λεγόμενο και ως ''**multimodal biometric fusion**'' που είναι ουσιαστικά ο συνδυασμός διαφόρων βιομετρικών μεθόδων, όπως εισαγωγή δακτυλικού αποτυπώματος και αναγνώριση υπογραφής.

Ποιες όμως επιθέσεις (*attacks*) πραγματοποιούνται εναντίον των βιομετρικών στοιχείων; Είναι βέβαιο από πριν ότι όπως κάθε σύστημα έτσι και η αναγνώριση των βιομετρικών στοιχείων έχει ευπάθειες και μπορεί να χτυπηθεί σε οποιοδήποτε σημείο της διαδικασίας της ταυτοποίησης και της εξακρίβωσης, με γνωστούς τρόπους όπως το replay attack και το man-in-the-middle attack. Ο

μεγαλύτερος κίνδυνος από τις επιθέσεις είναι η επίθεση γνωστή ως **Spoofing Attack.** Το spoofing είναι ουσιαστικά η προσπάθεια μίμησης μέσω αντιγραφής από κακόβουλο άτομο των γνήσιων βιομετρικών στοιχείων του νόμιμου κατόχου ώστε να επιτύχει την σύνδεση ή την συναλλαγή. Υπάρχουν διαφορετικές μέθοδοι να το επιτύχουν αντίστοιχα με το κάθε βιομετρικό αλλά το αποτέλεσμα τους είναι να παρουσιάσουν ένα πλαστό αντίγραφο του βιομετρικού που έχουν υποκλέψει με κάποιο τρόπο.

Διάφοροι μέθοδοι spoofing έχουν καταγραφεί στη βιβλιογραφία όπως οι **[47], [48]:**

Η πλαστοπροσωπία μέσω καταναγκασμού (**Coercive Impersonation**) στην οποία ο επιτιθέμενος εξαναγκάζει με τη βία τον νόμιμο χρήστη να κάνει είσοδο στην υπηρεσία.

Η επίθεση τύπου επανάληψης (**Replay attack**) που βασίζεται σε χρήση υποκλαπέντος βιομετρικού κατά την εκπομπή του σε δίκτυο, από συσκευή εισόδου ή από το αποθηκευτικό μέσο, σε προγενέστερο χρόνο και χρησιμοποίηση του στη συσκευή λήψης της υπηρεσίας.

Η επίθεση μίμησης (**Impersonation Attack**) στην οποία ο επιτιθέμενος αλλάζει την εμφάνιση του, την φωνή ή την υπογραφή του ώστε να μοιάζει με αυτή του ατόμου.

Θα σταθούμε λίγο περισσότερο στην επίθεση τύπου επανάληψης (*Replay attack*) με παράδειγμα πάνω στην αναγνώριση της υπογραφής. Η υποκλοπή της υπογραφής του θύματος μπορεί να γίνει σε οποιοδήποτε χρόνο ακόμα και από έγγραφα που έχει υπογράψει και που έρχονται με κάποιο τρόπο στη κατοχή του εγκληματία (πχ ακόμα και από τα σκουπίδια του σπιτιού ή της επιχείρησης). Η επίθεση με πλαστογράφηση της υπογραφής του κατόχου είναι η πιο συνηθισμένη επίθεση και χωρίζεται σε δυο τύπους: την **skilled forgery** που πραγματοποιείται με ακριβή αντιγραφή της υπογραφής από ένα ικανό πλαστογράφο που έχει στη κατοχή του την υπογραφή σε έγγραφο ή που έχει δει ή φωτογραφήσει την υπογραφή του θύματος σε σύστημα online εξακρίβωσης, και την τυχαία ή μηδενικής προσπάθειας (**random ή zero-effort forgery**) που γίνεται χωρίς καμία πρότερη γνώση της υπογραφής μέσω πραγματικού στοιχείου, αλλά με τυχαίες υποβολές υπογραφών και έχοντας την ελπίδα ότι θα πέσει σε περίπτωση false accept rate (*FAR*). Παράλληλα έχουν δημιουργηθεί

κατάλληλα εργαλεία και προγράμματα ώστε να μπορεί να γίνει υποκλοπή της υπογραφής του νόμιμου κατόχου, τα οποία διακρίνονται σε τρεις κλάσεις:

Η τυφλή πλαστογραφία (**Blind Forgery**) γίνεται έχοντας καμία γνώση της υπογραφής είτε από την εικόνα της είτε από τη δυναμική της γραφής της, πέρα από απλά το ονοματεπώνυμο του θύματος και υποβάλλοντας τυχαίες εκδόσεις.

Η χαμηλής δυναμικότητας πλαστογραφία (**Low-Force Forgery**) έχει ως στοιχείο το περίγραμμα της υπογραφής από το ιχνογράφημα της σε ένα χαρτί που μπορεί να ανακτηθεί με μολύβι. Και αυτή η περίπτωση δεν περιέχει στοιχεία της δυναμικής της γραφής. Τέλος έχουμε την επίθεση **brute force** στην οποία ένας δείκτης προβάλλει την υπογραφή την ώρα που γίνεται και την καταγράφει μαζί με την δυναμική της στο κακόβουλο άτομο ή πρόγραμμα.

Βλέπουμε ότι στην επίθεση επανάληψης (*Replay attack*) η τεχνική είναι να συλλάβει ο κακόβουλος το νόμιμο βιομετρικό και να το αναπαράγει με τους τρόπους που είδαμε. Μια μέθοδος αντιμέτρων σε αυτού του τύπου την επίθεση είναι το σύστημα να καταγράφει την υπογραφή του κατόχου και αφού γίνει η είσοδος με αυτή τη συγκεκριμένη υπογραφή να αναλύεται πλήρως και να αποθηκεύεται με ένδειξη ώρας και ημερομηνίας (timestamp), με σκοπό σε περίπτωση που εισαχθεί ξανά **η ίδια ακριβώς υπογραφή να απορριφθεί** μια που δεν υπάρχει περίπτωση μια υπογραφή να είναι 100% ίδια για δεύτερη φορά.

Ειδικά για τις τρεις πιο κοινές βιομετρικές τεχνολογίες, τα δακτυλικά αποτυπώματα, την αναγνώριση προσώπου και ίριδας που έχουν ερευνηθεί έχει δοθεί ιδιαίτερη σημασία στον παράγοντα της δυναμικότητας κατά την σύλληψη του βιομετρικού στοιχείου, και όχι απλά μια στατικής λήψης του, που έχει το όνομα όπως το συναντήσαμε και στην αρχή της υπό-ενότητας ''**liveness detection'' [32].**

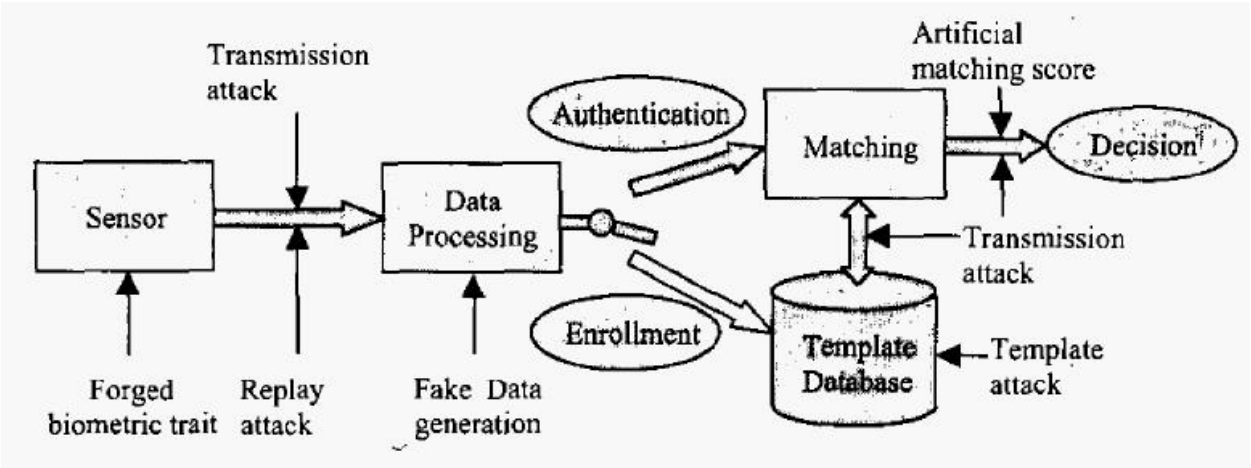
Οι τεχνικές αυτού του τύπου μπορούν να μπουν στις εξής τρεις κατηγορίες:

- Τις εγγενείς ιδιότητες (*Intrinsic properties*) του ζωντανού σώματος που του δίνουν μεγάλο αριθμό μετρήσιμων χαρακτηριστικών όπως: την πυκνότητα και φυσική ελαστικότητα, την χωρητικότητα, την ηλεκτρική διαπερατότητα και αντίσταση, την απορροφητικότητα του φωτεινού φάσματος και το χρώμα του δέρματος.

- Τα εκπεμπόμενα σήματα και παλμούς του ζωντανού σώματος όπως τους καρδιακούς παλμούς, την πίεση του αίματος, και τα ηλεκτρικά σήματα των καρδιακών μυών.
- Τις σωματικές αποκρίσεις σε εξωτερικά ερεθίσματα. Αυτά είναι μέθοδοι πρόκλησης-απόκρισης που αντιδρούν αντανακλαστικά είτε ηθελημένα είτε όχι. Ζητώντας από το χρήστη να χαμογελάσει κινητοποιώντας τους μύες του προσώπου είναι ένα παράδειγμα ηθελημένης συμπεριφορικής απόκρισης. Αντιθέτως η διαστολή της κόρης του ματιού είναι ένα παράδειγμα ακούσιας μη ηθελημένης απάντησης, το οποίο μπορεί να προκληθεί με το άναμμα ενός φλας για να ελέγξει την αντίδραση και να αποφασίσει αν είναι όντως άνθρωπος ή κάποιο αντίγραφο.

Αξίζει να αναφέρουμε ένα ακόμα τρόπο επίθεσης ώστε να δούμε ποιες τεχνικές έχουν αναπτύξει οι κακοποιοί ώστε να μπορέσουν να υποκλέψουν μια τόσο πολύτιμη πληροφορία όπως τα βιομετρικά.

Είναι η επίθεση μετάδοσης (*Transmission attack*) και είναι γνωστή και ως **'man in the middle attack'** στην οποία ο επιτιθέμενος στέλνει ένα κατασκευασμένο σήμα ως χρήστης εισάγοντας το πλαστό στοιχείο ανάμεσα στο πομπό και το δέκτη του συστήματος. Μπορεί να υποκλέψει και την πληροφορία του νόμιμου χρήστη αν δεν έχουν υπάρξει αρκετά μέτρα ασφάλειας. Τέτοια μέτρα είναι η κρυπτογράφηση της πληροφορίας, η μετάδοση μέσω ασφαλούς καναλιού επικοινωνίας, προστασία του υλικού με τέτοιο τρόπο ώστε να μη μπορούν να παραβιαστούν με φυσική παρουσία.



Εικόνα 17, τύποι επιθέσεων στα βιομετρικά συστήματα , [32].

Βλέπουμε πόσο ενδιαφέρον έχει το πεδίο των βιομετρικών τεχνολογιών και πόσους κλάδους εμπλέκει με στόχο την ασφάλεια της πληροφορίας. Ήδη έχουμε δει ότι λόγω των επιθέσεων και της κρισιμότητας της προστασίας και της πρόσβασης σε υπηρεσίες αλλά και η μοναδικότητα των βιομετρικών κάνει την προστασία τους κάτι παραπάνω από επιτακτική ανάγκη.

Φαίνεται ότι η λύση των **multimodal biometrics**, των συνδυαστικών δηλαδή βιομετρικών και η σύντηξη τους (*fusion*) είναι ένα μέσο να προσδώσει την ασφάλεια στο πεδίο της δυναμικότητας των βιομετρικών χαρακτηριστικών άρα να επιβεβαιώσει και την ταυτότητα του χρήστη. Από το επόμενο κεφάλαιο θα ασχοληθούμε με τη δυναμική της πληκτρολόγησης (keystroke dynamics) που είναι και το θέμα της εργασίας και που έχει να προσφέρει πολλά σε αυτό το τομέα.

Κεφάλαιο 3

Βιομετρικά τύπου Keystroke Dynamics

Τα Keystroke Dynamics ή δυναμική της πληκτρολόγησης είναι συμπεριφορικό βιομετρικό στοιχείο (*behavioral biometric*) με το οποίο μπορούμε να αναγνωρίσουμε και να εξακριβώσουμε την ταυτότητα ενός ατόμου μέσω του τρόπου και του ρυθμού πληκτρολόγησης σε πληκτρολόγιο ως συσκευή εισόδου. Σε αυτό το κεφάλαιο θα δούμε τη θεωρία πάνω στην οποία στηρίζεται και εφαρμόζεται αυτός ο τρόπος βιομετρικής αναγνώρισης.

3.1 Εισαγωγή στα βιομετρικά Keystroke Dynamics

Το βιομετρικό συμπεριφοράς **keystroke dynamics** εστιάζει στην εξαγωγή ποσοτικής πληροφορίας σχετικά με τα χαρακτηριστικά του ρυθμού της πληκτρολόγησης κατά την διάρκεια εισαγωγής από τον χρήστη της πληροφορίας μέσω πληκτρολογίου συμβατικού αλλά και αφής. Αυτό μας παρέχει τη δυνατότητα εφαρμογών όπως την αναγνώριση και εξακρίβωση της ταυτότητας του χρήστη κατά την χρήση ΗΥ, κινητών τηλεφώνων, ΑΤΜ αλλά και κάθε πιθανής συσκευής που έχει πληκτρολόγιο. Είδαμε ήδη ότι από τον 19ο αιώνα είχε παρατηρηθεί η μοναδικότητα του ρυθμού του κώδικα Μορς των χειριστών του τηλέγραφου. Ωστόσο η ενδελεχής ανάλυση και έρευνα της ουσιαστικής αναγνώρισης του χρήστη μέσω αυτού του χαρακτηριστικού και η ανάδειξη του ως βιομετρικό χαρακτηριστικό έγινε πολύ πιο πρόσφατα από τον Spillane το 1975 **[29, 44].** Τα Keystroke dynamics είναι ένα μη παρεμβατικό βιομετρικό που γίνεται εύκολα αποδεκτό από τους χρήστες. Μη παρεμβατικό

σημαίνει ότι δεν απαιτεί διαδικασία σκαναρίσματος ούτε ειδικά μηχανήματα, πράγμα με το οποίο πολλοί χρήστες νιώθουν άβολα και θεωρούν ως εισβολή στο προσωπικό τους χώρο και στα προσωπικά τους δεδομένα αλλά και ο υποσυνείδητος φόβος της κατάχρησης των βιομετρικών στοιχείων από κάποιον κακόβουλο άνθρωπο ή οργανισμό.

Αντιθέτως η πληκτρολόγηση είναι μια καθημερινή σχεδόν μηχανική διαδικασία και ο χρήστης το θεωρεί φιλικό και γνώριμο τρόπο εισαγωγής δεομένων. Λόγω της μη συλλογής φυσιολογικών βιομετρικών στοιχείων όπως την ίριδα του ματιού δεν το θεωρεί ως κάτι ξένο, επικίνδυνο, μη σύνηθες και άβολο, άρα μπορούμε να κατηγοριοποιήσουμε τα **keystroke dynamics** ως φιλικά προς το χρήστη.

Επιπλέον η συλλογή των βιομετρικών δεδομένων δεν απαιτεί εξειδικευμένο εξοπλισμό, αλλά μια συσκευή γνώριμη που χρησιμοποιεί συνεχώς, το ίδιο πληκτρολόγιο που γνωρίζει και θα χρησιμοποιήσει ή που ήδη χρησιμοποιεί το άτομο. Παρ 'όλα αυτά ο ρυθμός της πληκτρολόγησης, παρουσιάζει μεγάλη μεταβλητότητα των στοιχείων ακόμα και για τον ίδιο χρήστη, καθώς εξαρτάται άμεσα από το χρησιμοποιούμενο πληκτρολόγιο, τη φυσική και συναισθηματική κατάσταση του χρήστη, τη φυσική στάση του χρήστη κατά την πληκτρολόγηση και άλλους παράγοντες που επιδρούν εκείνη τη στιγμή, και που μπορούν να μεταβάλουν αρκετά τις μετρήσεις από το σύστημα αναγνώρισης. Αυτά είναι στοιχεία που πρέπει να ληφθούν προσεκτικά υπόψη κατά το σχεδιασμό ενός συστήματος αναγνώρισης βασισμένου στα keystroke dynamics.

Η αναγνώριση της πληκτρολόγησης μπορεί να ταξινομηθεί ως στατική και συνεχή ή δυναμική **[8].** Η **στατική** αναφέρεται στην ανάλυση κατά τη διάρκεια συγκεκριμένων στιγμών όπως κατά τη διάρκεια της εισόδου σε λογαριασμό (*login*) κατά την οποία ο χρήστης καλείται να εισάγει κάποιο συγκεκριμένο κείμενο όπως το όνομα χρήστη και τον κωδικό. Σε αυτή τη περίπτωση το σύστημα αναγνώρισης χρησιμοποιείται ως μέθοδος επαλήθευσης, με την απαίτηση της ταυτότητας να επιβεβαιώνεται μέσω μιας βιομετρικής σύγκρισης των χαρακτήρων ένα προς ένα με τα ήδη προ-αποθηκευμένα βιομετρικά στοιχεία. Αντιθέτως, όταν χρησιμοποιείται η **συνεχής** αναγνώριση, η ανάλυση

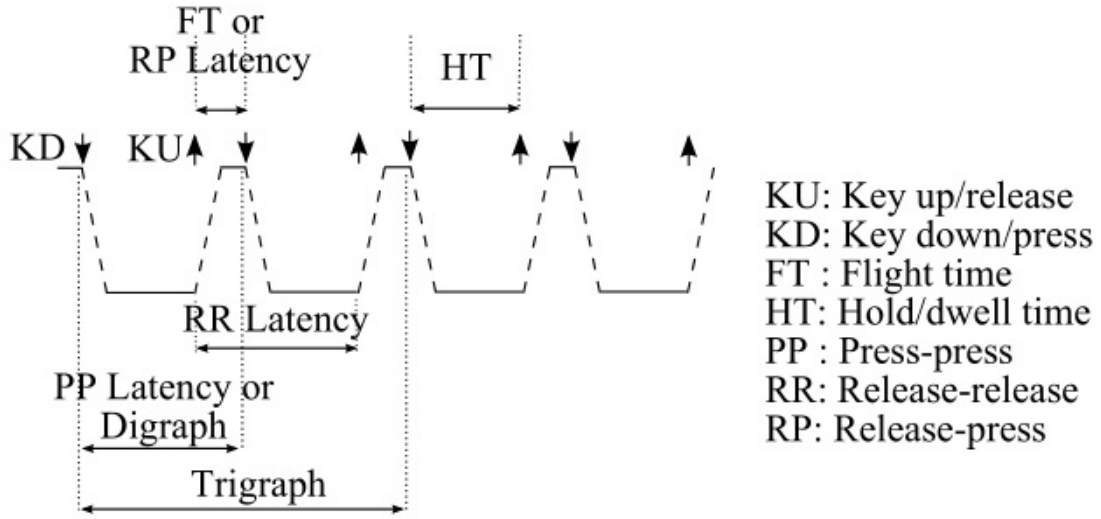
του ρυθμού πληκτρολόγησης πραγματοποιείται συνεχώς κατά τη διάρκεια ολόκληρης της σύνδεσης, στην οποία γίνεται έλεγχος και πάνω στην ανάλυση ελεύθερου κειμένου και όχι συγκεκριμένου ψάχνοντας να βρει ουσιαστικά ταυτίσεις στον τρόπο πληκτρολόγησης το λεγόμενο *pattern*. Συγκεκριμένα με αυτό το τύπο του σεναρίου το σύστημα αναζητά στη βάση δεδομένων σημεία ώστε να ταιριάζουν με τα αποθηκευμένα δείγματα μέσω πολλών συγκρίσεων και ουσιαστικά σπάζοντας το ελεύθερο κείμενο σε αναγνώριση μεμονωμένων χαρακτήρων, αριθμών ή γραμμάτων ή και συνδυασμών όπως θα δούμε. Αυτοί οι συνδυασμοί επιλέγονται ώστε να υπάρξει εγγύηση υψηλού επιπέδου σταθερό και αξιόπιστο αποτέλεσμα μέσα από πολλές δοκιμές αλλά και στην πορεία της λειτουργίας του συστήματος αφού εκπαιδεύεται και αυτό κάθε φορά που πληκτρολογεί ο χρήστης.

Έχει παρατηρηθεί ότι γνωστά κείμενα ή ακολουθίες χαρακτήρων είναι πιο πιθανό να δίνουν σταθερό αποτέλεσμα, και έτσι οι χρήστες μπορούν να κάνουν μια δοκιμαστική εισαγωγή του κειμένου για 10 φορές κατά τη διάρκεια της εγγραφής στην υπηρεσία ώστε να εκπαιδεύεται όχι μόνο το σύστημα για το ρυθμό του χρήστη αλλά να εξοικειωθεί και ο χρήστης με το συγκεκριμένο κείμενο ώστε να πλησιάζει στο μέγιστο βαθμό το συνήθη ρυθμό του τρόπου πληκτρολόγησης του συγκεκριμένου ανθρώπου. Έχει επίσης παρατηρηθεί ότι ασφαλή συμπεράσματα βγαίνουν αν το σύνολο των χαρακτήρων δεν είναι πολύ μικρό και οι χαρακτήρες εκτείνονται σε όλο το πληκτρολόγιο.

Οι όροι που έχουν επικρατήσει για την ανάλυση της πληκτρολόγησης των συνδυασμών των χαρακτήρων που αναφέραμε στην προηγούμενη παράγραφο είναι το δίγραμμα ή **digraph** που είναι δυο συνεχόμενοι χαρακτήρες που πληκτρολογούνται από το χρήστη, τρεις συνεχόμενοι χαρακτήρες λέγονται τρίγραμμα ή **trigraph** και γενικά οι ν χαρακτήρες ονομάζονται **n-graph** σε περίπτωση που απαιτηθεί από συγκεκριμένη περίπτωση η επέκταση της μέτρησης του χρόνου σε περισσότερους χαρακτήρες. Αυτοί οι όροι είναι χρήσιμοι όπως θα δούμε κατά την ανάλυση της συμπεριφοράς του χρήστη.

Επίσης η κρίσιμη πληροφορία που μπορεί να εξαχθεί κατά την πληκτρολόγηση είναι ο χρόνος ο οποίος είναι το κάθε πλήκτρο πατημένο και που λέγεται **hold**

time ο οποίος πιο συχνά λέγεται και χρόνος πατήματος και παραμονής του πλήκτρου **dwell time**. Υπάρχουν οι χρόνοι υστέρησης που είναι οι χρόνοι μεταξύ της πληκτρολόγησης ή πατήματος δυο συνεχόμενων πλήκτρων με τον όρο **PP:press-press latency** αλλά και ο χρόνος άφεσης δυο συνεχόμενων πλήκτρων με τον όρο **RR:release-release latency**. Αυτό μπορεί να επεκταθεί βεβαίως για εμπλουτισμό της πληροφορίας και σε trigraph. Στην ακόλουθη εικόνα φαίνονται οι πιθανοί συνδυασμοί από τους οποίους μπορούμε να εξάγουμε πληροφορία για το χρόνο.

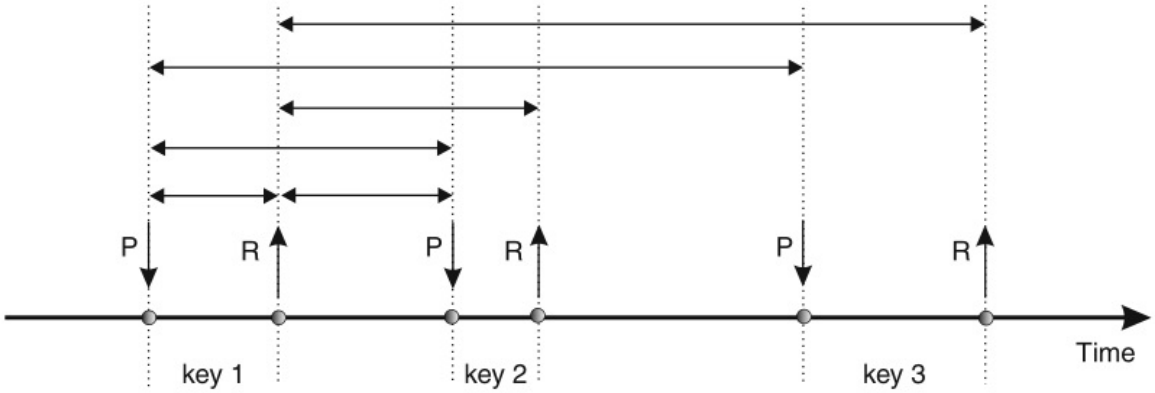


Εικόνα 18, όρια χρόνων διαφορετικών σημείων πληκτρολόγησης [8].

Πληροφορία μπορεί να εξαχθεί βεβαίως και από άλλα στοιχεία κατά την πληκτρολόγηση όπως η ταχύτητα της πληκτρολόγησης, ο αριθμός των λαθών, ο αριθμός της χρήσης του πλήκτρου διόρθωσης / επιστροφής (*backspace*), η χρήση του αριθμητικού πληκτρολογίου και η χρήση ειδικών πλήκτρων όπως 'Alt' και 'Shift'.

Στην επόμενη εικόνα περιγράφονται τα γεγονότα (events) από τη στιγμή που πατιέται ένα πλήκτρο (Press, P) μέχρι τη στιγμή που απελευθερώνεται (Release, R) και τα ενδιάμεσα διαστήματα. Όλα αυτά φέρουν τις μοναδικές ιδιότητες του χρήστη στο χρόνο που διαρκεί η πληκτρολόγηση και που είδαμε πιο πάνω και η μονάδα μέτρησης είναι το millisecond (ms). Σε αυτό το σημείο να σημειώσουμε ότι η δυναμική της πληκτρολόγησης περιέχει και ερευνά και πρόσθετες ιδιότητες όπως την δύναμη της πίεσης στο πλήκτρο, την κίνηση των δακτύλων

ιδιότητες που δίνουν πιο πλούσια πληροφορία, απαιτούν όμως ειδικό εξοπλισμό για να τις συλλάβουμε και να τις αξιοποιήσουμε πέρα του απλού πληκτρολογίου, και δεν θα επεκταθούμε σε αυτές στη παρούσα εργασία .



Εικόνα 19, Γεγονότα πληκτρολόγησης στο χρόνο,[8]

Τα keystroke dynamics έχουν αναλυθεί εκτενώς με χρήση του παραδοσιακού πληκτρολογίου τύπου QWERTY, και ως αόρατος και μη παρεμβατικός τρόπος βιομετρικού ελέγχου, έχει ιδιαίτερα ελκυστικά χαρακτηριστικά και έχει προταθεί να συνδυάζεται με όχι μόνο την απαίτηση της εισαγωγής των ονομάτων χρήστη και κωδικών εισόδου αλλά και με τον έλεγχο του ρυθμού της πληκτρολόγησης κατά τη διάρκεια αυτής της διαδικασίας επιτυγχάνοντας την επιβεβαίωση διπλής μεθόδου (*two factor authentication*) στον ίδιο χρόνο που απαιτεί για την κλασική είσοδο και μάλιστα μέσω της ίδιας συσκευής εισόδου χωρίς να απαιτεί άλλο εξοπλισμό. Αυτή η στατική ανάλυση να σημειώσουμε ότι δεν καλύπτει το σύστημα από την αντικατάσταση του νόμιμου χρήστη από κάποιον κακόβουλο μετά την επιτυχή είσοδο στην οποία μπορεί να έχει εξαναγκαστεί να κάνει από κάποιον κακοποιό πράγμα που επιτυγχάνει η συνεχής ανάλυση της πληκτρολόγησης και μετά την επιτυχή είσοδο.

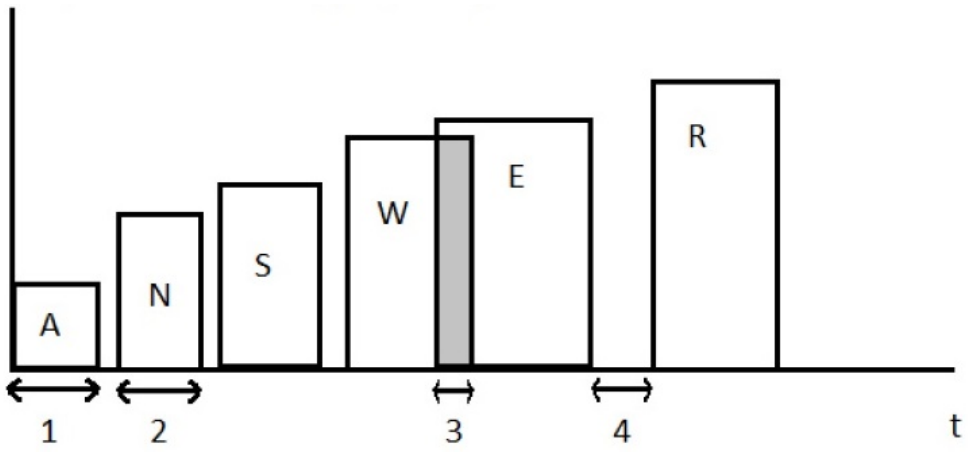
Αυτό θα μπορούσε να χρησιμοποιηθεί πέρα από τη προφανή σκοπιά της ασφάλειας των υπολογιστών αλλά και της εγκληματολογίας (*forensics*) και για την παρακολούθηση της παραγωγικής γραφής και γενικά της συγκέντρωσης του χρήστη στην διαδικασία, γεγονός που θα μπορούσε να φανεί χρήσιμο στην διάγνωση και θεραπεία περιπτώσεων άνοιας και μαθησιακών δυσκολιών, ζητήματα που θα τα ξαναδούμε στα ανοικτά ερευνητικά θέματα.

3.2 Αυθεντικοποίηση με χρήση Keystroke Dynamics

Ο τρόπος που τα keystroke dynamics μπορούν να χρησιμοποιηθούν για την εξακριβωμένη είσοδο του ατόμου γίνεται όπως είδαμε μέσω του πληκτρολογίου και η διαδικασία αυτή επιτυγχάνεται με κάποια λογική σειρά, βήματα δηλαδή όπως μια συνταγή, που στην Πληροφορική ονομάζεται αλγόριθμος. Θα δούμε μια περίπτωση δημιουργίας και χρήσης ενός τέτοιου αλγόριθμου και πειράματος από την εργασία των **[22],** όπου το σύστημα χρησιμοποιεί ως μέσα πιστοποίησης της ταυτότητας τον χρόνο πατήματος και παραμονής του πλήκτρου που είδαμε ότι λέγεται **hold / dwell time,** το κενό χρονικά διάστημα μεταξύ της πίεσης των πλήκτρων και ο χρόνος που θεωρείται ως χρόνος κοινής πίεσης δυο συνεχόμενων πλήκτρων, δηλαδή πριν απελευθερωθεί το πρώτο και έχει σχεδόν πατηθεί το επόμενο, χρόνος που ονομάζεται **Overlapping**.

Το τελευταίο στοιχείο το έχει χρησιμοποιήσει ο ερευνητής γιατί έχει αποδειχτεί ότι κάποιος που πληκτρολογεί πολύ γρήγορα, πατάει τόσο γρήγορα τα πλήκτρα που σε μερικά ειδικά σημεία ή λέξεις ή σε συνήθεις συνδυασμούς όπως στο δικό του όνομα χρήστη (*username*) η πληκτρολόγηση γίνεται με πολύ γρήγορους ρυθμούς, γεγονός που προσδίδει μια παραπάνω δικλείδα ασφάλειας αφού ο νόμιμος χρήστης δηλαδή αυτός που πληκτρολογεί για αρκετό χρονικό διάστημα το ίδιο συνδυασμό έχει εξοικειωθεί με αυτό και επιτυγχάνει πιο γρήγορους ρυθμούς σε σημείο που έχει ως αποτέλεσμα, κάποια πλήκτρα ειδικά, να τα πατάει πριν ακόμα αφήσει εντελώς το προηγούμενο. Οι χρόνοι όπως έχουμε αναφέρει είναι της τάξεως των millisecond με σύμβολο το ms ή το msec που είναι το 1/1000 ή το 10^{-3} του δευτερολέπτου και στη συνέχεια θα χρησιμοποιούμε αυτή την υποδιαίρεση του χρόνου. Βλέπουμε στην ακόλουθη εικόνα τα χαρακτηριστικά που μετρώνται το *dwell time* την περίοδο ουσιαστικά της πληκτρολόγησης ενός πλήκτρου, το *overlapping* που μόλις είδαμε και την παύση ή *interval time* δηλαδή το κενό ανάμεσα σε δυο πληκτρολογήσεις πλήκτρων ή σε δυο καταστάσεις από τη πλήρη απελευθέρωση του

προηγούμενου πλήκτρου στην έναρξη της πίεσης του επόμενου, στοιχεία που θα μας φανούν ιδιαίτερα χρήσιμα στην δική μας ανάλυση στο επόμενο κεφάλαιο.



Εικόνα 20, διαστήματα πίεσης πλήκτρων dwell, overlap και interval[22]

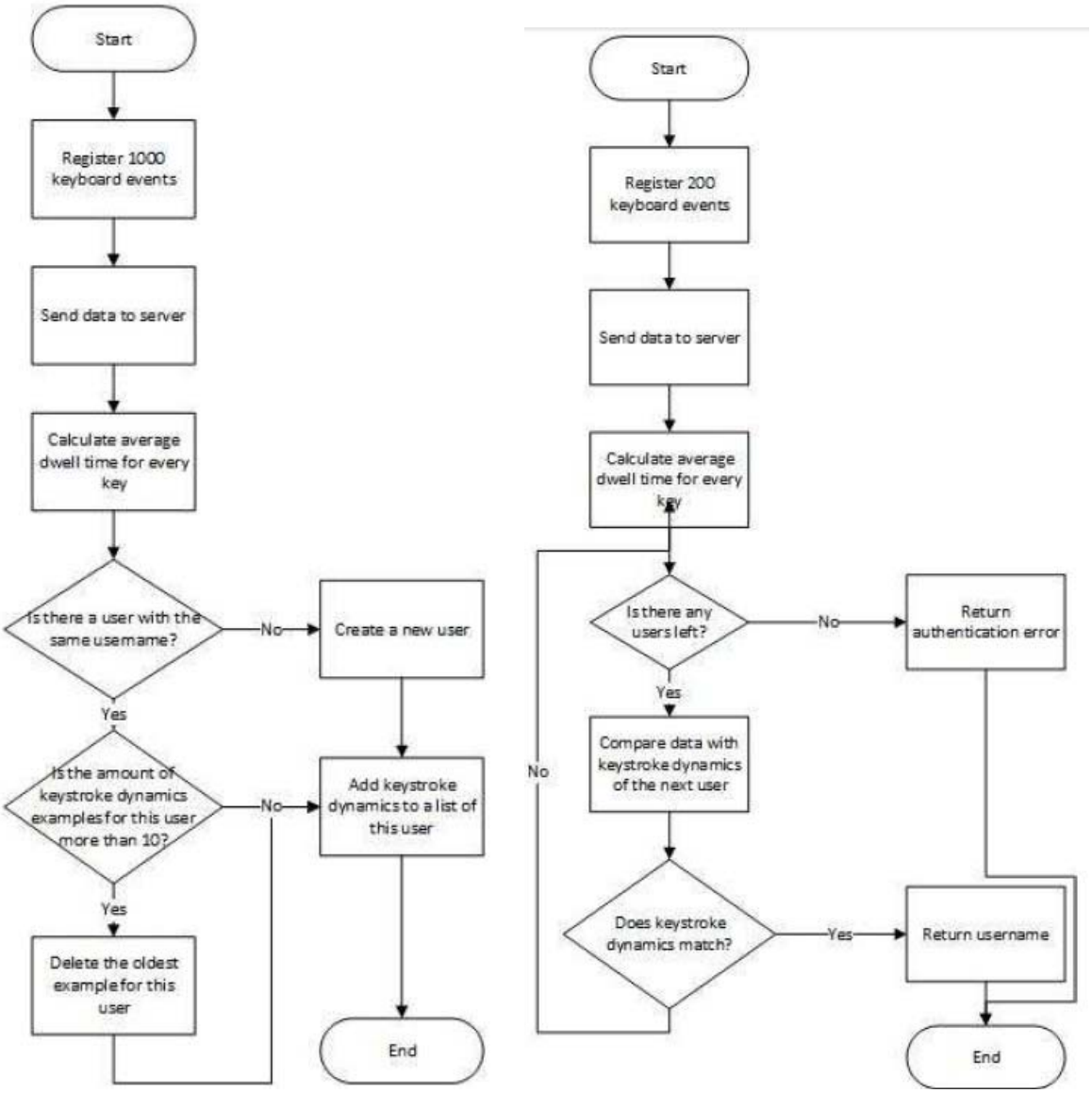
Στην εικόνα φαίνεται πλέον ξεκάθαρα η έννοια του overlap στα πλήκτρα **W** και **E**, ενώ στο **R** έχουμε τη φάση διακοπής interval, και εδώ σημειώνουμε ότι τα γράμματα σχηματίζουν την λέξη answer ως την απάντηση στο ερώτημα του συστήματος για εισαγωγή username / password. Εδώ ο ερευνητής θέλει να καταδείξει ακριβώς αυτό, την διαφορά ταχύτητας πληκτρολόγησης ανάμεσα σε κάποιους συνδυασμούς που τελικά είναι και μοναδικοί από άνθρωπο σε άνθρωπο. Σε αυτή λοιπόν την έρευνα **[22]** δημιουργείται ένας αλγόριθμος αναγνώρισης του ατόμου και επιβεβαίωσης της ταυτότητας του. Ο αλγόριθμος έχει δυο φάσεις και αξίζει να το μελετήσουμε μια και μας εισάγει στην τεχνική των keystroke dynamics και από τη πλευρά της ουσιαστικής ανάλυσης του ρυθμού μέσω αλγοριθμικού ελέγχου.

Ο αλγόριθμος που δημιούργησαν οι ερευνητές **[22]** έχει την ακόλουθη μορφή των δυο σταδίων που δείχνεται στην ακόλουθη εικόνα για να δούμε την ροή των εργασιών και να καταλάβουμε τη φιλοσοφία του. Αριστερά βλέπουμε τη πρώτη φάση κατά την οποία γίνεται ο έλεγχος του ρυθμού πληκτρολόγησης με τη χρήση του χρόνου πατήματος (*dwell time*) του χρήστη ώστε τελικά να ταυτοποιηθεί ή όχι.

Ξεκινάει με την αποθήκευση 1000 γεγονότων πληκτρολόγησης του συνόλου των χρηστών και αποθήκευση τους στο σέρβερ ως δεδομένα αναφοράς. Έπειτα

έχουμε την εξαγωγή του μέσου όρου του χρόνου των κάθε ίδιων πλήκτρων για κάθε χρήστη. Ακολουθεί ο έλεγχος αν σε νέα εισαγωγή ονόματος χρήστη για είσοδο στην υπηρεσία το όνομα χρήστη συμπίπτει με κάποιο ενός ήδη αποθηκευμένου χρήστη, και αν όχι δημιουργείται νέα λίστα εγγραφών για το νέο χρήστη. Αν υπάρχει όμως ήδη χρήστης με αυτό το όνομα χρήστη προσθέτει το συγκεκριμένο χρόνο στην λίστα του και εφόσον οι εγγραφές του συγκεκριμένου χρήστη υπερβαίνουν τις 10, διαγράφει το παλαιότερο με το νεώτερο έχοντας τη λογική FIFO (*First-In, First-Out*).

Στην επόμενη φάση του αλγορίθμου γίνεται ο έλεγχος της εξακρίβωσης του χρήστη μόνο από την εισαγωγή του ονόματος χρήστη. Αν συμπίπτει το keystroke dynamic του username που εισήγαγε ο χρήστης με το αποθηκευμένο προχωράει τη διαδικασία για το password αλλιώς εμφανίζει σφάλμα authentication error αφού δεν συμπίπτει ο ρυθμός πληκτρολόγησης του χρήστη με το μέσο όρο των αποθηκευμένων αυτού του ατόμου.



Εικόνα 21, αλγόριθμος αναγνώρισης χρήστη με keystroke dynamics, [22]

Με αυτό τον τρόπο οι ερευνητές έδειξαν τη σύνδεση της ταυτότητας των χρηστών μέσω των keystroke dynamics όπως φαίνεται στους ακόλουθους πίνακες. Στον πρώτο φαίνεται το dwell time για ένα χρήστη και στον δεύτερο φαίνεται η σύγκριση των μέσων όρων του σε σχέση με άλλο χρήστη.

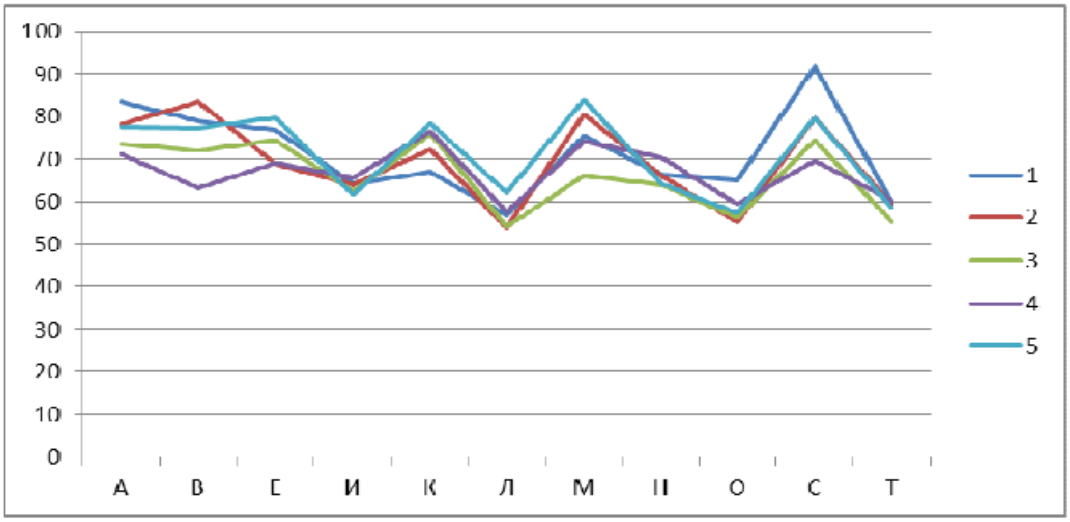


Figure 4. Comparison of the dwell time for one user

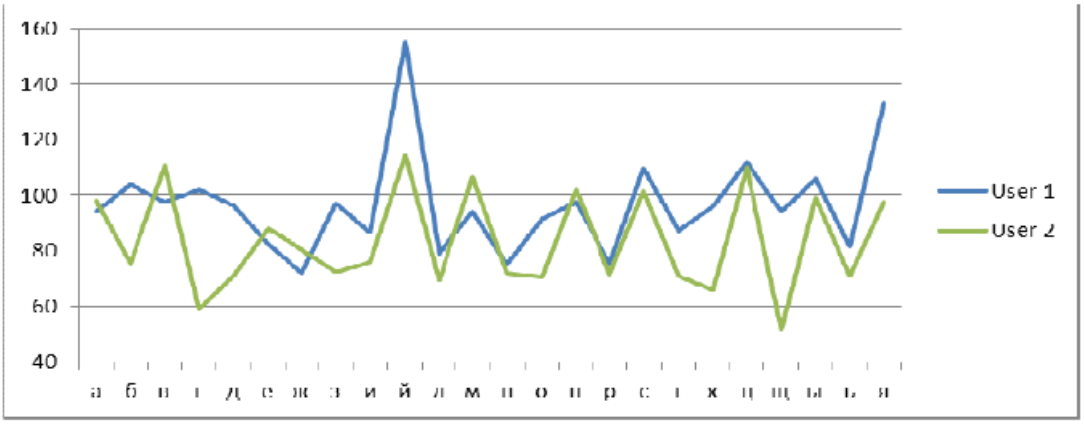


Figure 5. Comparison of the dwell time for two different users

Εικόνα 22, σύγκριση dwell time μεταξύ δεδομένων του ίδιου χρήστη και στη συνέχεια αυτού του χρήστη με κάποιον άλλο [22].

Με αυτό τον τρόπο λοιπόν οι ερευνητές κατέδειξαν ότι όντως διαφαίνεται πρακτικά η διαφορά του ρυθμού πληκτρολόγησης ανάμεσα σε διαφορετικούς χρήστες και μάλιστα με ακρίβεια της τάξης του 0.875%.

Η διαδικασία της σύγκρισης γενικά γίνεται μέσω κάποιων μαθηματικών μεθόδων που είναι είτε μέσω της βιολογικής προσέγγισης με χρήση αλγόριθμων βασισμένων στα νευρωνικά δίκτυα (*neural networks-based algorithms*) είτε με αλγόριθμους λήψης απόφασης με χρήση στατιστικής και πιθανοτήτων (*probabilistic - statistical methods*), αλλά και άλλα όπως υβριδικά (*hybrid*) και τεχνικές αναγνώρισης προτύπων (*pattern recognition*).

Οι αλγόριθμοι βασισμένοι στα νευρωνικά δίκτυα παρέχουν υψηλή ακρίβεια αλλά απαιτούν υψηλή υπολογιστική ισχύ, ενέργεια και ακριβότερο εξοπλισμό

ανάλυσης και δεν μπορούν να χρησιμοποιηθούν για υπολογισμούς σε πραγματικό χρόνο. Ακόμα η διαδικασία 'εκπαίδευσης- μάθησης' του συστήματος με νευρωνικά δίκτυα απαιτεί μακρό χρονικό διάστημα, και βέβαια υπάρχει η αδυναμία να 'μάθει' το σύστημα στην αρχική περίοδο μέσω παραδειγμάτων ώστε να μην αντιλαμβάνεται τις περιπτώσεις παράνομων χρηστών που με πολλές δοκιμές συνήθως προσπαθούν να αποκτήσουν πρόσβαση. **[34]**

Οι μέθοδοι πιθανοτήτων – στατιστικής (*probabilistic - statistical methods*), απαιτούν τον υπολογισμό κάποιων στατιστικών χαρακτηριστικών (μέσος όρος, διάμεσος, τυπική απόκλιση) πάνω στη βάση της σύγκρισης δυναμικά του δείγματος του χρήστη με του ήδη αποθηκευμένου δείγματος του. Αυτή η μέθοδος εκτός του ότι είναι πιο αποδοτική λόγω της ταχύτητας του αποτελέσματος, έχει το προτέρημα της μη απαίτησης υψηλών επιπέδων υπολογιστικής ισχύος και βέβαια σε πραγματικές συνθήκες που δυνητικά κάνουν έλεγχο σε μεγάλο αριθμό αιτήματα διαφορετικών χρηστών ταυτόχρονα σε πραγματικό χρόνο κάνει την χρήση μεθόδων πιθανοτήτων – στατιστικής στον έλεγχο των keystroke dynamics πολύ ελκυστική. Κατά την ανάλυση της μεθόδου των ερευνητών **[22]** είδαμε ότι ο αλγόριθμος αναγνώρισης είναι δύο σταδίων: Στο πρώτο στάδιο το πρόγραμμα συλλέγει το σετ των στατιστικών δεδομένων του χρήστη και το δεύτερο που πραγματοποιείται η σύγκριση των μόλις υποβληθέντων στοιχείων με τις συνήθεις τιμές του χρήστη. Αυτή η σύγκριση μπορεί να γίνει με τη βοήθεια οποιουδήποτε μέτρου εγγύτητας και οι ερευνητές εδώ χρησιμοποιούν την Ευκλείδεια απόσταση (*Euclidean distance*), η οποία υπολογίζεται από τον τύπο:

$$P = \sqrt{\sum_{i=1}^{N} (t_{et} - t_{cur})^2}$$

Τύπος 1, τύπος υπολογισμού Ευκλείδειας απόστασης (Euclidean Distance)

Στον τύπο το N είναι ο αριθμός των διαφορετικών χαρακτήρων, το t_{et} είναι ο τυπικός χρόνος dwell για ένα πλήκτρο και το t_{cur} ο σε πραγματικό χρόνο dwell για το συγκεκριμένο πλήκτρο, αυτό που πάτησε μόλις ο χρήστης, δηλαδή γίνεται

η σύγκριση του τυπικού χρόνου ενός πλήκτρου με το τυπικό χρόνο του χρήστη. Η έννοια της απόστασης έχει σκοπό να μετρήσει το πόσο διαφέρουν μεταξύ τους δυο παρατηρήσεις και να μας δείξουν πόσο ίδιες ή όχι είναι μεταξύ τους με ποσοτικό τρόπο. Με την Ευκλείδεια απόσταση εδώ εξετάζουμε ως μεταβλητές τον χρόνο πληκτρολόγησης για κάθε διαφορετικό χρήστη αλλά και τους μεταξύ τους χρόνους. Πρέπει να σημειώσουμε εδώ ότι επειδή έχουμε την ύπαρξη των τετραγωνικών αποκλίσεων (βλέπε τύπο) οι ακραίες τιμές έχουν μεγάλη επίδραση στον τελικό υπολογισμό της απόστασης.

Εδώ είναι το σημείο που αξίζει να πούμε σχετικά με τα **σφάλματα μέτρησης** (error metrics). Είδαμε ότι στην φάση της αυθεντικοποίησης / εξακρίβωσης του χρήστη τα δεδομένα που λαμβάνονται κατά τη φάση της πληκτρολόγησης, αναλύονται στατιστικά ώστε να εξάγουμε το βιομετρικό μέγεθος τους. Στη φάση της εξακρίβωσης της ταυτότητας γίνεται έλεγχος αν το βιομετρικό στοιχείο ταιριάζει με κάποιο ή κάποια από τη βάση δεδομένων, δηλαδή πρόκειται για μια διαδικασία ελέγχου ενός προς πολλά στοιχεία (one-to-many). Δυο δείκτες σφαλμάτων χρησιμοποιούνται ουσιαστικά για να ελέγξουμε την επίδοση της βιομετρικής ταυτοποίησης **[8].** Το ένα είναι το Εσφαλμένο ποσοστό αποδοχής, πιο γνωστό ως False Acceptance Rate (**FAR**) το οποίο είναι το ποσοστό των μη νόμιμων χρηστών που τους επιτρέπεται εσφαλμένα η είσοδος και που ορίζεται από τον ακόλουθο τύπο,

$$FAR = \frac{Number\ of\ false\ matches}{Total\ number\ of\ impostor\ match\ attempts}$$

Τύπος 2, τύπος υπολογισμού False Accept Rate (FAR)

Και το δεύτερο είναι το Εσφαλμένο ποσοστό απόρριψης γνωστό ως False Rejection Rate (**FRR**) που είναι το ποσοστό των νόμιμων χρηστών που δεν γίνονται δεκτοί από το σύστημα και που ορίζεται από τον τύπο,

$$FRR = \frac{Number\ of\ false\ rejections}{Total\ number\ of\ genuine\ match\ attempts}$$

Τύπος 3, τύπος υπολογισμού False Reject Rate (FRR)

Βλέπουμε στην εργασία των Banerjee και Woodard **[8]** ότι στη βιβλιογραφία χρησιμοποιείται και ο όρος equal error rate (**EER**) αντί των FAR/FRR. Το EER ορίζεται ως τιμή που με το βαθμό της μεταβολής των FAR/FRR και όταν τείνουν να γίνουν ίσα μεταξύ τους αυτή η τιμή παίρνει το όνομα EER. Δηλαδή αυτός ο όρος μας καταδεικνύει όταν το ένα ποσοστό, εσφαλμένης αποδοχής είναι ίσο με το άλλο, εσφαλμένης απόρριψης, και τελικά όσο μικρότερο βαθμό έχει το EER τόσο καλύτερο θεωρείται το βιομετρικό σύστημα. Γενικά μπορούμε να δεχτούμε ότι υψηλότερες τιμές FAR είναι αποδεκτές σε εφαρμογές με όχι υψηλά επίπεδα ασφάλειας ενώ αντίθετα απαιτούμε υψηλό βαθμό FRR σε ευαίσθητες και κρίσιμες εφαρμογές και συστήματα.

3.3 Οι Αλγόριθμοι ταξινόμησης στα Keystroke Dynamics

Έχουμε ήδη αναφέρει αρκετές φορές ότι τα βιομετρικά keystroke dynamics αναλύουν όχι το τι πληκτρολογεί κάποιος αλλά το πώς το πληκτρολογεί. Είδαμε στην μελέτη του αλγορίθμου αναγνώρισης τη χρήση της Ευκλείδειας απόστασης ως τρόπο αναγνώρισης της υποβληθείσας αλφαριθμητικής ακολουθίας χαρακτήρων (*string sequence*) με σύγκριση των αποθηκευμένων με στατιστική ανάλυση.

Η πιο απλή μορφή στατιστικής μεθόδου ανάλυσης είναι μέσω του υπολογισμού του μέσου όρου (*mean*) και της τυπικής απόκλισης (*standard deviation*) των δεδομένων **[8].** Με αυτά μπορούμε να συγκρίνουμε το υποβληθέν κείμενο με τα αποθηκευμένα με σύγκριση ελέγχων υποθέσεων, όπως t-test και μετρήσεις απόστασης όπως την απόλυτη απόσταση (*absolute distance*), την σταθμισμένη απόλυτη απόσταση (*weighted absolute distance*), την Ευκλείδεια απόσταση και άλλα. Ερευνητές που χρησιμοποίησαν την απόλυτη απόσταση για την ταυτοποίηση πέτυχαν FAR σε ποσοστό 0.25% και FRR σε ποσοστό 16.36% και σε άλλη περίπτωση άλλοι ερευνητές χρησιμοποιώντας διανυσματική ανάλυση (*vector analysis*) για την ταξινόμηση των χρηστών πέτυχαν ακρίβεια αποτελεσμάτων της τάξης του 95%. Ο ακόλουθος πίνακας δείχνει την κύρια

εργασία που έχει γίνει από τις ομάδες των ερευνητών στην κατεύθυνση της δημιουργίας αυθεντικοποίησης και ταυτοποίησης των χρηστών χρησιμοποιώντας στατιστικούς αλγόριθμους. Εδώ πρέπει να σημειώσουμε ότι παρότι τα αποτελέσματα είναι εντυπωσιακά βασίζονται σε αριθμό πειραματικών δειγμάτων που είναι σχετικά χαμηλός.

Table 2: Authentication and identification using statistical algorithms

Study	Features	Classification	TT	Env.	Subjects	Samples	Error Rates (%)		
							FAR	FRR	EER
Gaines et al. [56]	1	Statistical	S	C	6	36	-	-	-
Umphress & Williams [151]	1	Statistical	S	C	17	34	6	12	-
Leggett and Williams [95]	1	Digraph Test	S,D	C	36	72	5.5	5	-
Bleha et al. [20]	1	Min. dist. classifier	S	C	39	171	2.8	8.1	-
Joyce & Gupta [83]	1	Abs. distance	S	C	33	975	0.25	16.67	-
Napier et al. [109]	1,3	Statistical	S	C	24	-	-	-	3.8
Mahar et al. [100]	1	Statistical	S	C	67	-	-	-	17.6
Furnell et al. [55]	1	Statistical	D	C	30	60	15	0	-
Tapiador & Sigüenza [146]	1	Statistical	S	U	9	1620	-	-	-
Coltell et al. [40]	1	Statistical	S	C	10	-	>70	≈0	-
Bergadano et al. [16]	1,2	Statistical	S	C	44	220	0	2.3	-
Monrose et al. [106]	1,3	Statistical	S	C	20	481	20	20	-
Araújo [7]	1,3	Statistical	S	C	30	553	1.89	1.45	-
Gunetti et al. [62]	1,2	Distance measure	D	U	30	-	8.33	3.33	-
Gunetti et al. [63]	1,2	Distance measure	D	U	31	-	≈0	≈ 2.0	-
Gunetti & Picardi [61]	1,2	Relative, Abs. distance	S, D	C	205	765	0.005	5	0.5
Revett et al. [124]	1	Statistical	S	U	43	≈688	-	-	5.58
de Magalhaes [48]	1,3	Statistical	S	U	43	≈688	-	-	≈ 5.0
Lv & Wang [99]	3,4	Statistical classifiers	S	C	100	5000	1.4	1.4	1.41
Modi & Elliott [105]	1	Statistical classifiers	S,D	C	42	6300	0.33	94.87	-
Montalváo et al. [108]	1	Statistical	S D	C	-	-	- -	- -	6.2 12.7
Bocchat et al. [21]	1,3	Statistical	S	C	-	-	0	3.83	-
Lee et al. [94]	1,3	Hypothesis	S	U	16	3200	≈4.5	≈5.5	-
Choraś & Mroczokwski [36] Choraś & Mroczokwski [37]	1,2	Degree of disorder	S	U	18	≈810	0	0-55	-
Davoudi & Kabir [47]	1,2,3	Statistical	D	C	21	-	9	5	-
Giroux et al. [60]	1,3	Mean	S	U	11	880	0	-	-
Killourhy & Maxion [91]	1,3	Manhattan(‡)	S	C	51	20400	-	-	9.6
Bours & Barghouthi [22]	1,3	Statistical	D	U	25	1620	-	-	-
Douhou & Magnus [49]	1,3	Statistical	S	U	1254	-	16	1	-
Chudá & Ďurfina [38]	1,3	Angle b/w latencies	S	-	15	-	8.4 3.6	2.5 4.7	- -
Xi et al. [159]	1,2	nGdv-V nGdv-C	D	U	205	765	9.43 1.65	24.7 2.75	- -
Study	**Features**	**Classification**	**TT**	**Env.**	**Subjects**	**Samples**	**Identification Rate (%)**		
Shepherd [142]	1,3	Statistical	S	-	4	-	99		
Monrose & Rubin [107]	1,3	Statistical	S,D	U	31	-	90		
DSouza [51]	1	Statistical	S	C	11	-	76		
Guven & Sogukpinar [66]	1	Vector Analysis	S	C	-	-	89.3 / 95†		
Bergadano et al. [17]	1,2	Distance measure	S, D	C	40	364	90		
Gunetti et al. [62]	1,2	Distance measure	D	U	30	-	≈90		
Gunetti et al. [63]	1,2	Distance measure	D	U	31	-	90		
Villani et al. [155]	1,3	Euclidean dist.	D	C U	118	-	98.3 99.4		
Janakiraman & Sim [78]	1,3	Histogram	D	U	22	-	9.91 – 100*		
Teh et al. [148]	1,3	DSM$^{\triangle}$	S	C	50	-	93.64		
Lv et al. [98]	4	Statistical classifiers	S	C	50	3000	6.6		
Rybnik et al. [131]	1,3	Statistical	S	C	37	-	72.97		
Samura & Nishimura [135]	1,3	Euclidean dist.	S	C	112	-	90.7 – 100		

1 - Latency, 2 - Trigraph/N-graph, 3 - Key hold time, 4 - Key Pressure, 5 - Rhythms/acoustic cues

TT - Testing type, S - Static, D - Dynamic, C - Controlled, U - Uncontrolled.

(†) Using data from experienced users a higher accuracy level was achieved; (*) For English words the highest identification rate was 9.91%, while for non-English words the highest accuracy was 100%; (‡) - In this paper, comparison of 14 algorithms were performed, of which the Manhattan distance performed the best; ($^{\triangle}$) DSM - Direction Similarity Measure

Εικόνα 23, πλήθος των στατιστικών αλγόριθμων, [8]

Στον πίνακα βλέπουμε ενδιαφέρουσες πληροφορίες και θα δούμε όρους που τους εξηγήσαμε ήδη, σχετικά με τις στατιστικές μεθόδους αξιολόγησης και ανάλυσης των keystroke dynamics όπως τον τρόπο στατιστικής ταξινόμησης των αποτελεσμάτων (*statistical classification*), τον αριθμό των ατόμων και των δειγμάτων και το αποτέλεσμα σε ποσοστά FAR, FRR και EER. Επίσης βλέπουμε τον τρόπο που έγινε η διεξαγωγή του πειράματος σε ελεγχόμενο ή μη περιβάλλον (*controlled / uncontrolled*), τη μέθοδο πληκτρολόγησης (*στατική ή συνεχής*) και το ποσοστό επιτυχούς αναγνώρισης του ατόμου. Σχεδόν σε όλες τις περιπτώσεις έχουμε την μέτρηση του στοιχείου του ρυθμού πληκτρολόγησης *latency* και του *key hold / dwell time*.

Επίσης και σε άλλη μελέτη **[18],** παρατηρούμε στον ακόλουθο πίνακα τις μεθόδους στατιστικής ανάλυσης που χρησιμοποιούνται με τα σχόλια τους ώστε να εντοπίσουμε ποια θα είναι κατάλληλη τελικά για το δικό μας πείραμα και σύμφωνα με τα δικά μας ζητούμενα,

Sl. No.	Method	Remarks
1	Mean and standard deviation [17]	Successive keystrokes is recorded and used for authentication with the result of 4% FAR and 0% IPR for seven users
2	Mean, standard deviation and digraph [48]	The mean, standard deviation of keystroke latencies and digraph between reference profile and test data are compared. A result of 17% FAR and 30% FRR was obtained
3	Geometric distance [19]	The Mahalanobis distance function was used to determine similarity between reference and verification profiles and achieved good performance
4	Euclidean distance [18]	Euclidean distance measure between two vectors of typing of characters, total time periods and the pressure is measured and stored as template
5	Mean reference signature (mean and standard deviation) [3]	Built a mean reference signature for eight sets of the users' keystroke patterns consisting of username, password, first name, and last name and computed norm and achieved 16.7% FAR and 0.25% IPR
6	Degree of disorder [26]	Used timing information to obtain the relative order of trigraphs. It reduces the effect of variations in the absolute timing data on the authentication mechanism with 4% FAR and 0.01% IPR
7	N-graphys [49]	Method to compare typing samples of free text with less than 5% IPR and less than 0.005% FAR
8	*k*-Nearest neighbor approach [33]	Input needs only to be verified against limited user profiles within a cluster which effectively reduces the verification load significantly with the similar performance as [12]
9	Manhattan distance [34]	Manhattan distance was used to find the distance between referring keystroke feature vector and the feature vector to be classified with overall accuracy of 75.68%
10	Mean and variance [50]	Rollover capability was proposed to correctly determine the intervals and used mean and variance to determine the feature subset and for identification
11	Hidden Markov model [51]	HMM has ability of handling stochastic process and achieved an EER of 3.6%

Εικόνα 24, Σύνοψη των αναφερόμενων μεθόδων στατιστικής ταξινόμησης των keystroke dynamics, [18].

Έχουμε δει ήδη στην προηγούμενη ενότητα σχετικά με την Ευκλείδεια απόσταση, η οποία μας δείχνει πόσο μεταξύ τους απέχουν δυο μετρήσεις. Είδαμε επίσης ότι γίνεται ευρέως χρήση των γνωστών μεθόδων του μέσου όρου και της

τυπικής απόκλισης όπου το εισαχθέν όνομα χρήστη ή όποιος άλλος συνδυασμός έχει επιλεγεί συγκρίνεται με τους χρόνους στη βάση δεδομένων ώστε να γίνει ή όχι εξακρίβωση της ταυτότητας του χρήστη.

Διαβάζοντας εργασία άλλων ερευνητών πάνω στα keystroke dynamics **[1]** βλέπουμε με ενδιαφέρον ότι αναφέρεται σε πείραμα που χρησιμοποιώντας ως μέτρο κωδικό password μήκους 10 χαρακτήρων πάνω σε 4 διαφορετικά στοιχεία ελέγχου keystroke dynamics (dwell, interval, digraph και trigraph) έκαναν μετρήσεις με χρήση των στατιστικών μεγεθών του μέσου όρου και της τυπικής απόκλισης για σύγκριση των χρόνων που εισάγονται με τα ήδη αποθηκευμένα. Σε αυτό το πείραμα λοιπόν έγινε όχι μόνο αντιπαραβολή των νόμιμων χρηστών με τα στοιχεία των 'παράνομων' που προσπαθούν να εισέλθουν χωρίς καμία γνώση του τρόπου πληκτρολόγησης των χρηστών απλά μαντεύοντας με τυχαίο τρόπο τον τρόπο γραφής αλλά και με μια δεύτερη ομάδα 'παράνομων' ατόμων που έχοντας το ρόλο του παρανόμου τους δόθηκε η δυνατότητα να παρατηρούν τον τρόπο πληκτρολόγησης των νόμιμων χρηστών ώστε να έχουν ακριβώς με το στοιχείο της παρατήρησης πιο πολλές πιθανότητες να παρεισφρήσουν στο σύστημα. Με αυτό το πείραμα λοιπόν επετεύχθη σε όλες τις περιπτώσεις ρυθμοί σφάλματος FRR = 1.45% και FAR = 1.89%, και τα δυο εντυπωσιακά αποτελέσματα για αυτά τα είδη στατιστικής ανάλυσης.

Εδώ μπορούμε να αναφέρουμε και μια άλλη στατιστική μέθοδο που χρησιμοποιούν οι ερευνητές, την απόσταση Μανχάταν (Manhattan distance ή όπως ονομάζεται και αλλιώς City block distance) η οποία έχει πολλά κοινά σημεία με την Ευκλείδεια απόσταση με τη διαφορά ότι για τον υπολογισμό της απόστασης δεν χρησιμοποιεί την ύψωση στο τετράγωνο αλλά απόλυτες αποκλίσεις. Λόγω του ίδιου σχεδόν τρόπου υπολογισμού με την Ευκλείδεια δίνει σχεδόν πάντα περίπου τα ίδια αποτελέσματα και στις περιπτώσεις εμφάνισης ακραίων τιμών λόγω της απόλυτου τιμής. Εδώ πρέπει να πούμε ότι με την χρήση των μεθόδων της απόστασης δεν λαμβάνονται υπόψη οι στατιστικές ιδιότητες των παρατηρήσεων όπως για η μεταβολή της κάθε μεταβλητής. Ο τύπος εύρεσης της απόστασης Μανχάταν είναι ο ακόλουθος

$$d(x,y)=\sum_{i=1}^{p}|x_i-y_i|$$

Τύπος 4, τύπος υπολογισμού Manhattan Distance

Εκτός από αυτά βέβαια υπάρχουν και τα γνώριμα μέσος όρος και τυπική απόκλιση. Η μέση τιμή είναι το άθροισμα των παρατηρήσεων διά του πλήθους των παρατηρήσεων ή αλλιώς το άθροισμα των τιμών του πληθυσμού του δείγματος δια το πλήθος του δείγματος. Όταν έχουμε ένα δείγμα με μέγεθος *ν* και οι παρατηρήσεις σε μια μεταβλητή *X* είναι $t_1 \ldots t_v$, τότε η μέση τιμή συμβολίζεται με $\bar{x}$ και εξάγεται από τον τύπο:

$$\bar{x}=\frac{t_1+t_2+\ldots+t_v}{v}=\frac{\sum_{i=1}^{v}t_i}{v}=\frac{1}{v}\sum_{i=1}^{v}t_i$$

Τύπος 5, τύπος υπολογισμού μέσου όρου

στο οποίο έχουμε τις τιμές από 1 έως *ν* δια του *ν*. Η μέση τιμή είναι το σπουδαιότερο και χρησιμότερο μέτρο της Στατιστικής και για αυτό είναι χρήσιμο να θυμηθούμε τα πλεονεκτήματα και τα μειονεκτήματα του. Ως θετικά λοιπόν στοιχεία την ταχύτητα και την ευκολία του υπολογισμού της και την ανάδειξη της κεντρικής τιμής των κατανομών. Έχει αδυναμία στο γεγονός ότι επηρεάζεται άμεσα από την αλλαγή σε οποιαδήποτε από τις τιμές των δεδομένων και για αυτό το λόγο είναι ιδιαίτερα ευαίσθητη στις ακραίες τιμές (outliers).

Άλλο στατιστικό μέτρο που χρησιμοποιείται ευρέως στην ανάλυση είναι η τυπική απόκλιση. Για να δούμε τι κάνει ακριβώς θα δούμε πολύ γρήγορα την διακύμανση που είναι ο μέσος όρος των τετραγώνων των αποκλίσεων των τιμών από τη μέση τιμή τους. Ένα μειονέκτημα όμως αυτού του μέτρου είναι η μη έκφραση στις μονάδες της μονάδας μέτρησης που χρησιμοποιούμε και που

τις εκφράζει στο τετράγωνο. Η τυπική απόκλιση αφαιρεί αυτό το μειονέκτημα της διασποράς των παρατηρήσεων, και παίρνουμε την θετική τετραγωνική ρίζα της διακύμανσης και με αυτό τον τρόπο έχουμε ακριβώς τη μονάδα μέτρησης που θέλουμε. Ο τύπος της είναι πολύ απλός και είναι ο ακόλουθος,

$$s = \sqrt{s^2}$$

Τύπος 6, τύπος υπολογισμού τυπικής απόκλισης

Τα θετικά στοιχεία της τυπικής απόκλισης είναι ότι λαμβάνει υπόψη όλες τις τιμές της κατανομής και μπορεί να χρησιμοποιηθεί για τον υπολογισμό των παραμέτρων του πληθυσμό όντας ο πιο ευαίσθητος από τους δείκτες της διασποράς. Αρνητικό έχει την ευαισθησία σε ακραίες τιμές (outliers) και ότι είναι λίγο πιο περίπλοκος από τη μέση τιμή. Αν και υπάρχουν πολλά προγράμματα που υπολογίζουν αυτά τα μεγέθη όπως και όλα τα υπόλοιπα στατιστικά μεγέθη είναι χρήσιμο να γνωρίζουμε τι είναι το κάθε ένα και πως υπολογίζεται μαθηματικά. Στη συνέχεια στο πείραμα μας θα χρησιμοποιηθούν μέθοδοι πιθανοτήτων – στατιστικής (probabilistic - statistical methods), που όπως είδαμε απαιτούν τον υπολογισμό κάποιων στατιστικών χαρακτηριστικών (μέσος όρος, διάμεσος, τυπική απόκλιση), για το λόγο της ταχύτητας, του αριθμού του δείγματος αλλά και τη μη ανάγκη συνεχούς εκπαίδευσης του συστήματος.

Κεφάλαιο 4

Ερευνητική διαδικασία

Στο παρόν κεφάλαιο θα εργαστούμε πάνω στην πειραματική διαδικασία με χρήση ερωτηματολογίου και εφαρμογής για λήψη των keystroke dynamics από ομάδα ανθρώπων. Θα γίνει έλεγχος αν υπάρχει στατιστική διαφορά μεταξύ τους ώστε να δούμε ότι πράγματι υπάρχει δυνατότητα διαχωρισμού και εντοπισμού του χρήστη μέσω των keystroke dynamics. Αυτό γίνεται με χρήση κωδικού που έχει χρησιμοποιηθεί σε έρευνες και που με αντιπαραβολή με τα στοιχεία από ευρέως χρησιμοποιούμενα data sets να δούμε πιθανές συγκλίσεις και διαφορές.

4.1 Κύκλος έρευνας

Είναι πολύ χρήσιμο ξεκινώντας να αναφέρουμε σχετικά με τα διαφορετικά στάδια που διανύουμε κατά την διενέργεια της ερευνητικής διαδικασίας γνωστό και ως ο κύκλος της έρευνας **[13].** Η αρχή αυτής της διαδικασίας γίνεται με την ***αναγνώριση ενός ερευνητικού προβλήματος***, στάδιο κατά το οποίο αναγνωρίζονται τα θέματα και πραγματικά προβλήματα που υπάρχουν στο τομέα και που η εργασία μας φιλοδοξεί να προσφέρει κάτι καινούργιο σχετικά με αυτό το θέμα. Εδώ έχουμε ήδη δει σχετικά με τον κίνδυνο ασφάλειας πρόσβασης και το πρόβλημα της ασφάλειας διαφύλαξης των κλασικών βιομετρικών στοιχείων μας. Επόμενο στάδιο στην έρευνα είναι η ***ανασκόπηση της βιβλιογραφίας***, στο οποίο αναζητώ στην βιβλιογραφία πληροφορίες σχετικά με την υπάρχουσα γνώση πάνω στο θέμα που εργάζομαι, ώστε να εμπλουτιστεί τελικά με τη δική μας εργασία. Μπορεί να χρησιμοποιηθεί και ως σημείο αναφοράς όπως θα χρησιμοποιήσουμε εδώ τα data sets από ήδη διενεργηθείσες έρευνες ως ομάδα ελέγχου των δικών μας ευρημάτων. Στη συνέχεια έχουμε τον *σκοπό της έρευνας* στο οποίο εστιάζουμε και καταλήγουμε

σε συγκεκριμένα ερευνητικά ερωτήματα ή υποθέσεις, ουσιαστικά το κίνητρο της εργασίας μας.

Το επόμενο στάδιο είναι η ***συγκέντρωση των δεδομένων*** που αποτελούν τα στοιχεία τα οποία θα μας δώσουν τα μέσα για να απαντηθούν τα ερωτήματα ή και να ανοίξουν νέα θέματα και ερωτήματα. Αυτό το στάδιο εμείς θα το επιτύχουμε με δυο τρόπους με το ερωτηματολόγιο και με το πείραμα εισαγωγής κωδικού. Έπειτα θα έχουμε την ***ανάλυση των δεδομένων*** με στατιστικά εργαλεία που θα μας βοηθήσουν να καταλήξουμε σε συμπεράσματα και να ερμηνεύσουμε τα αποτελέσματα. Αυτό θα γίνει και με χρήση πινάκων και σχημάτων. Αφού ολοκληρωθούν τα προηγούμενα στάδια έχουμε το τελευταίο μέρος που είναι η ***αναφορά και αξιολόγηση*** της έρευνας μας. Αυτά είναι τα στάδια της ερευνητικής διαδικασίας τα οποία και ακολουθούν στις ακόλουθες ενότητες αυτής της εργασίας.

4.2 Σκοπός της έρευνας

Ο σκοπός της έρευνας είναι η διερεύνηση του ελέγχου προσπέλασης (access control) με τη χρήση Behavioral Biometrics, δίνοντας έμφαση στις υφιστάμενες εφαρμογές και τεχνολογίες, τα προβλήματα τους, τις παρούσες και μελλοντικές απειλές και προκλήσεις, δίνοντας έμφαση στο βιομετρικό στοιχείο συμπεριφοράς **keystroke dynamics** με σχεδιασμό πειράματος που θα συνοδεύεται με software υλοποίηση με χρήση keylogger για εισαγωγή συγκεκριμένου pattern αλφαριθμητικών χαρακτήρων από ομάδα ατόμων και ανάλυση των στοιχείων, ώστε να μελετηθεί σε ποιο βαθμό είναι αξιόπιστος και έγκυρος τρόπος προσπέλασης, σε σύγκριση με τις ήδη διαθέσιμες βάσεις δεδομένων (*datasets*) από άλλες έρευνες τους κινδύνους που μπορούν να οδηγήσουν σε επιθέσεις και αλλαγές με τεχνικό ή φυσικό τρόπο με πειραματισμό και με πιο προτάσεις ώστε να δειχθεί με ποιο ή ποιους τρόπους θα μπορούσε να βελτιωθεί το επίπεδο ασφάλειας του χρήστη αφού με ταυτόχρονη εισαγωγή των credentials έχουμε με την χρήση των keystroke dynamics προσθήκη ακόμα ενός τρόπου αυθεντικοποίησης επιτυγχάνοντας απευθείας το

two factor authentication (*password + keystroke dynamics biometric*) και έρευνα αντίστοιχων περιστατικών από τη βιβλιογραφία. Επίσης να εντοπιστούν πιθανοί ανασταλτικοί παράγοντες όπως ηθικά, τεχνικά και άλλα ζητήματα κατά τη χρήση των βιομετρικών keystroke dynamics, ειδικά με την έλευση του GDPR. Βλέπουμε ότι θα προσεγγίσουμε το θέμα από πολλές πλευρές ώστε να αναδείξουμε όσα περισσότερα ευρήματα μπορούμε και να επιβεβαιώσουμε ή να απορρίψουμε άλλα που αναφέρονται στη βιβλιογραφία.

4.3 Μεθοδολογία

Η μεθοδολογία της παρούσης έρευνας περιλαμβάνει έρευνα της βιβλιογραφίας, με ανάλυση των ειδών βιομετρικής τεχνολογίας για τον έλεγχο πρόσβασης σε υπηρεσίες, δίνοντας βάση στα προβλήματα που υπάρχουν σήμερα καθώς και στις μελλοντικές προκλήσεις, και που αποτελούν τη θεωρητική προσέγγιση αυτής της εργασίας λαμβάνοντας υπόψη κοινωνικά, οικονομικά, ηθικά και τεχνικά ζητήματα.

Θα προταθεί ερωτηματολόγιο διαδικτυακά ώστε να ερευνηθεί πόσο επιφυλακτικοί είναι ακόμα οι άνθρωποι και αν υπάρχει διαφορά μεταξύ των κλασικών φυσιολογικών βιομετρικών και των keystroke dynamics δηλαδή αν θεωρούνται περισσότερο φιλικά προς το χρήστη και ταυτόχρονα λιγότερο επεμβατικά στην ιδιωτικότητα του.

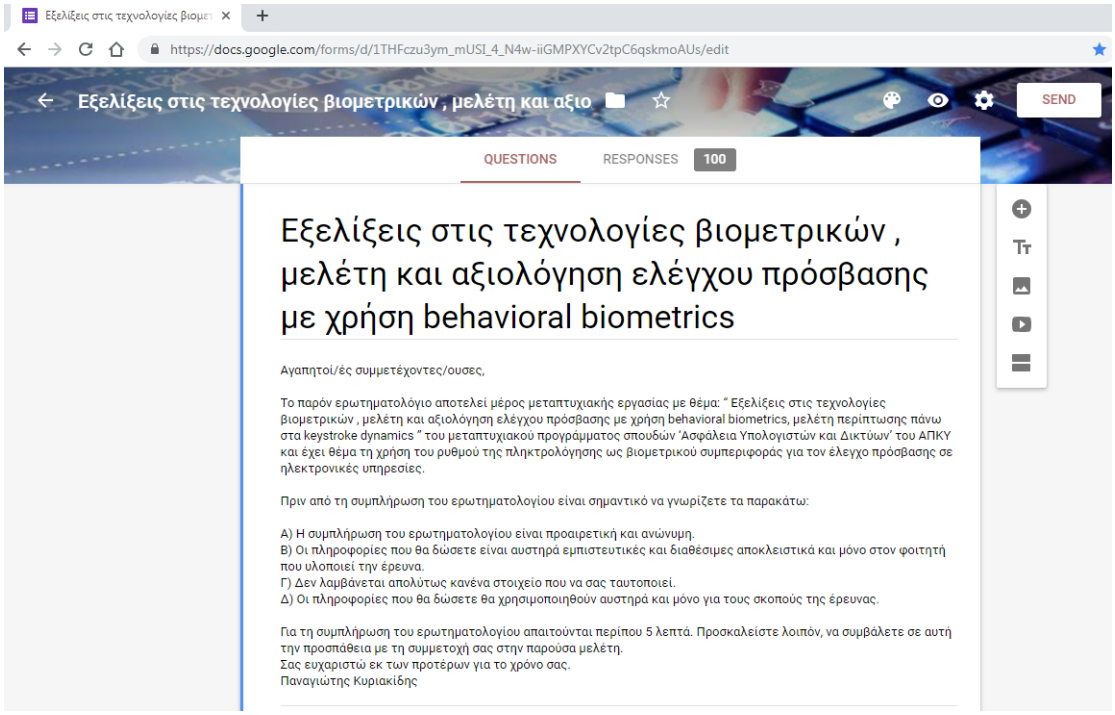
Συμπληρωματικά θα πραγματοποιηθεί πείραμα με εφαρμογή python συγκεκριμένου αλφαριθμητικού κωδικού από ομάδα συμμετεχόντων και καταγραφή των δεδομένων ώστε να αναλυθούν με πειραματικό τρόπο να αποδειχθεί η αξιοπιστία των βιομετρικών keystroke dynamics σε σύγκριση με τα ευρήματα των μεγάλων βάσεων δεδομένων από άλλες έρευνες.

4.4 Ερωτηματολόγιο

Δημιουργήθηκε στο Google forms ερωτηματολόγιο με 23 ερωτήσεις σχετικά με τα βιομετρικά στοιχεία με στόχο να βρεθεί η σχέση τους με το εκπαιδευτικό επίπεδο και τη εμπειρία χρήσης ΗΥ αλλά και η γενικότερη στάση του κοινού απέναντι στη χρήση βιομετρικών στοιχείων κατά τη χρήση διαδικτυακών υπηρεσιών. Επίσης θέλουμε να δούμε πόσο γνωστό είναι το βιομετρικό συμπεριφοράς keystroke dynamics και να δούμε κατά πόσο τελικά θεωρείται πιο φιλικό και λιγότερο επεμβατικό από τους χρήστες των ΗΥ σε σχέση με την ασφάλεια των διαδικτυακών υπηρεσιών.

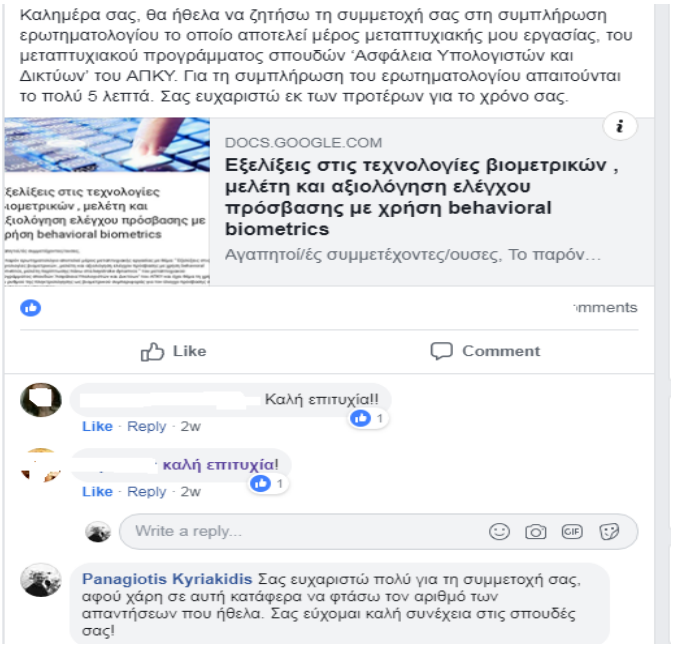
Γίνεται προσπάθεια να μετρηθεί η συνήθης αμυντική στάση εναντίον της χρήσης των βιομετρικών και να τονιστεί στους χρήστες ότι ήδη γίνεται χρήση καθημερινά ακόμα και αν πλέον δεν το αντιλαμβάνονται. Γίνεται επίσης προσπάθεια να εξαχθούν συμπεράσματα σχετικά με την εκπαίδευση και την γνώση των χρηστών σχετικά με την ασφάλεια των υπολογιστών μέσω διάφορων ερωτήσεων. Ο **αριθμός των συμμετεχόντων** ατόμων στη συμπλήρωση του ερωτηματολογίου ήταν **εκατό (100) άτομα**. Τα συμπεράσματα θα αναφερθούν στο επόμενο κεφάλαιο και στην ενότητα Ανάλυση και ερμηνεία των δεδομένων. Σημειώνεται ότι δεν υπήρχε προαιρετική ερώτηση. Το ερωτηματολόγιο με το εισαγωγικό κείμενο και τις ερωτήσεις με τις διαθέσιμες απαντήσεις βρίσκεται στο **Παράρτημα Β**.

Ακολουθεί screenshot της σελίδας του ερωτηματολογίου με τη δομή και τη διεύθυνση του.



Εικόνα 25, σελίδα του ερωτηματολογίου στο Google forms

Ακολουθεί επίσης ένα απόσπασμα από ενδεικτική ανάρτηση στο facebook για πρόσκληση συμμετοχής στο ερωτηματολόγιο και οι ευχαριστίες με τη κατάκτηση του στόχου του αριθμού των συμμετεχόντων.



Εικόνα 26, screenshot από ανάρτηση σε σελίδα ομάδας φοιτητών στο facebook

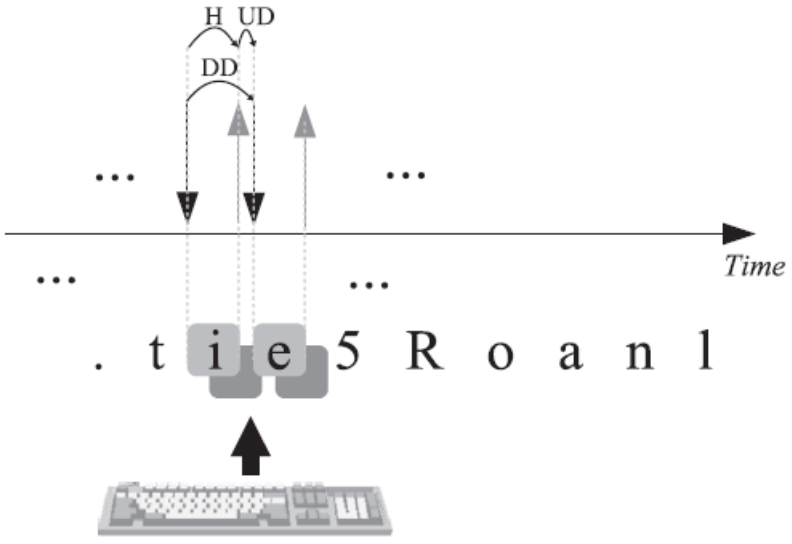
4.5 Πείραμα

Είδαμε σε προηγούμενο κεφάλαιο σχετικά με τον τρόπο που γίνεται η διεξαγωγή των πειραμάτων και την αναφορά σε ελεγχόμενο ή μη περιβάλλον (controlled / uncontrolled) όπου το ελεγχόμενο βρίσκεται κάτω από την επιτήρηση του ερευνητή ενώ το μη ελεγχόμενο αφήνει ελευθερία στον χρήστη σχετικά με το χρόνο και τόπο για τη διεξαγωγή του πειράματος. Η πιο σημαντική διαφορά μεταξύ τους είναι όμως ότι με την ελεγχόμενη διασφαλίζεται η συνθήκη ότι κάθε δείγμα λαμβάνεται με τους ίδιους όρους από κάθε συμμετέχοντα ώστε να υπάρξει ομοιογένεια των αποτελεσμάτων. Σε αυτή την ενότητα πραγματοποιείται πείραμα εισαγωγής κωδικού και σύλληψης των χρόνων των συμμετεχόντων. Ο κωδικός που χρησιμοποιήσαμε είναι ο "`try4-mbs`" και είναι ο ίδιος με αυτόν που έχει ήδη χρησιμοποιηθεί σε έρευνες **[23, 26]** και τα ευρήματα τους βρίσκονται δημόσια διαθέσιμα σε βάσεις δεδομένων.

Εδώ είναι χρήσιμο να γράψουμε λίγα πράγματα, για τις άλλες βάσεις δεδομένων και για τη μέθοδο ώστε να αντιληφθούμε το σκεπτικό των ερευνητών και θα επιστρέψουμε στον κωδικό "`try4-mbs`" των Loy et al που χρησιμοποιήσαμε. Κάθε διαθέσιμη βάση δεδομένων λοιπόν έχει το όνομα του κωδικού που χρησιμοποιείται, και έτσι ας δούμε πρώτη την βάση δεδομένων με κωδικό το ".tie5Roanl", με μήκος δέκα χαρακτήρων ο οποίος επιλέχτηκε από τους ερευνητές ως ένας δύσκολος κωδικός που δεν μπορεί να το μαντέψει κάποιος. Η μέθοδος αυτή έλαβε 400 δείγματα εισαγωγής κωδικών από 51 άτομα και έγινε και έλεγχος της ορθότητας της εισαγωγής δηλαδή με καταγραφή στον αριθμό των λαθών των χρηστών. Σε αυτό το σημείο και από την πλευρά της ασφάλειας των υπολογιστών πρέπει να παρατηρήσουμε ότι χρησιμοποιώντας ένα πολύ δύσκολο κωδικό, οι χρήστες σε μεγάλο βαθμό για να τον θυμούνται αρχίζουν και τον γράφουν σε σημειωματάρια αλλά και σε άλλα σημεία, καταλήγοντας να γίνεται πια πολύ ανασφαλής ο τρόπος φύλαξης του κωδικού και όχι ο ίδιος ο κωδικός και τελικά γίνεται εύκολο να υποκλαπεί. Εδώ είναι ένα καλό σημείο που μπορούμε να κρατήσουμε αυτό το προφανές στοιχείο για να ενισχύσουμε την ιδέα της χρησιμότητας των keystroke dynamics ως συμπληρωματική μέθοδος ταυτοποίησης σε συνδυασμό με το ζεύγος username/ password.

Επόμενη δημόσια διαθέσιμη βάση δεδομένων είναι η “Greyc” των Giot et al **[15],** η οποία συνέδεσε το βιομετρικό του ρυθμού της πληκτρολόγησης σε σχέση με το πληκτρολόγιο το οποίο χρησιμοποιείται. Οι συμμετέχοντες για διάρκεια ενός μηνός εισήγαγαν τον κωδικό ‘greyc laboratory’ μετά από μια περίοδο προσαρμογής και μάθησης του, από έξι φορές σε δυο διαφορετικά πληκτρολόγια. Αυτές οι προσπάθειες καταγράφονταν και ενώ ο συνολικός αριθμός των ατόμων ήταν 133, μόνο τα στοιχεία από τους 100 χρησιμοποιήθηκαν.

Τέλος έχουμε την βάση δεδομένων με τον κωδικό που χρησιμοποιήσαμε και εμείς των Loy, 2005, τον “try4-mbs”. Οι ερευνητές **[23]** χρησιμοποίησαν αυτό το κωδικό για μείωση των σφαλμάτων, έχοντας ταυτόχρονα το σχετικά ασφαλές μήκος κωδικού των οκτώ χαρακτήρων περιέχοντας γράμματα, αριθμό και σύμβολο. Αυτός ο κωδικός έχει ως χαρακτηριστικό την έλλειψη των κεφαλαίων γραμμάτων, την λήψη των στοιχείων πληκτρολόγησης ‘’DD, down – down’’ και την εξοικείωση των συμμετεχόντων με τον κωδικό πριν την εισαγωγή τους. Σε αυτό το πείραμα έλαβαν μέρος 100 άτομα και έγινε χρήση και ειδικού πληκτρολογίου για σύλληψη όχι μόνο του ρυθμού αλλά και του επιπέδου της πίεσης των πλήκτρων, δηλαδή της δύναμης που ασκείται στο πλήκτρο βελτιώνοντας τα βιομετρικά δεδομένα αυτού του στοιχείου με μια ακόμα παράμετρο. Εδώ να θυμηθούμε ότι το ‘DD, down - down’ είναι το διάστημα του χρόνου μεταξύ της πληκτρολόγησης δυο διαφορετικών πλήκτρων.



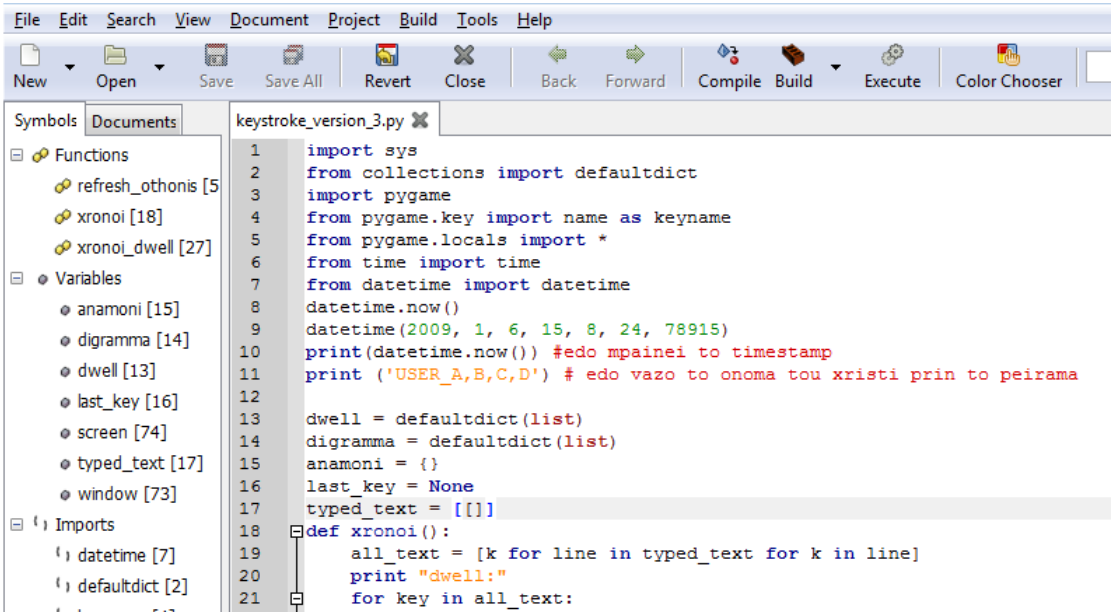
Εικόνα 27, Απεικόνιση των Down – Down, Hold time και Up – Down , [26]

Στο δικό μας πείραμα χρησιμοποιήθηκε όπως είδαμε αυτός ο κωδικός των Loy et al 2005, τον "`try4-mbs`". Η διαδικασία που ακολουθήθηκε ήταν η εξής. Έγινε χρήση κώδικα Python 2.7 (**Παράρτημα Α**) για απεικόνιση των χρόνων Hold-time και διγράμματος (digraph), από **δώδεκα (12) συμμετέχοντες**. Έγινε αναζήτηση μέσω της βιβλιοθήκης αλλά και των github και stackoverflow για κομμάτια κώδικα πάνω στο θέμα ώστε να φτιαχτεί μια εφαρμογή που να μας δώσει αυτά τα στοιχεία και να έχει περάσει από δοκιμές και μέσω της κοινότητας και των ομάδων να έχει βελτιωθεί και να δίνει ορθά αποτελέσματα **[49]**. Αυτά συγκεντρώθηκαν, ενοποιήθηκαν και βελτιώθηκαν περαιτέρω, έγιναν αλλαγές και προσαρμόστηκε κατάλληλα για την έρευνα. Η εισαγωγή κωδικού έγινε σε λάπτοπ Lenovo X240 για να εξασφαλιστεί η φορητότητα, με εξωτερικό πληκτρολόγιο 108 πλήκτρων με διασύνδεση USB 2.0. Τα στοιχεία του λάπτοπ είναι, OS Linux Mint 18 64bit, CPU Intel Core i5-4300U, 3MB Cache, 1.90 GHz, 8GB DDR3, 500GB SATA III HDD.

Εικόνα 28, Το πληκτρολόγιο OK05TGR, 108 πλήκτρων USB 2.0 που χρησιμοποιήθηκε.

Με αυτό τον τρόπο μειώθηκε η πιθανότητα σφαλμάτων λόγω μη εξοικείωσης των χρηστών με το πληκτρολόγιο του συγκεκριμένου λάπτοπ αφού το κανονικού μεγέθους πληκτρολόγιο είναι ίδιο με σχεδόν αυτά που χρησιμοποιούν ήδη οι χρήστες. Τα πληκτρολόγια των λάπτοπ λόγω του μεγέθους και της διαφορετικής διάταξης, απαιτούν περίοδο προσαρμογής ακόμα και από έμπειρους χρήστες, και με τη χρήση κανονικού μεγέθους πληκτρολογίου φάνηκε και στη πράξη μέσω των δοκιμών η ευκολία εισαγωγής του κωδικού στο κανονικό σε αντίθεση με τα πολλαπλά λάθη από το πληκτρολόγιο του λάπτοπ. Ο κώδικας περιέχει ένδειξη χρόνου του πειράματος (timestamp) και χρησιμοποιεί

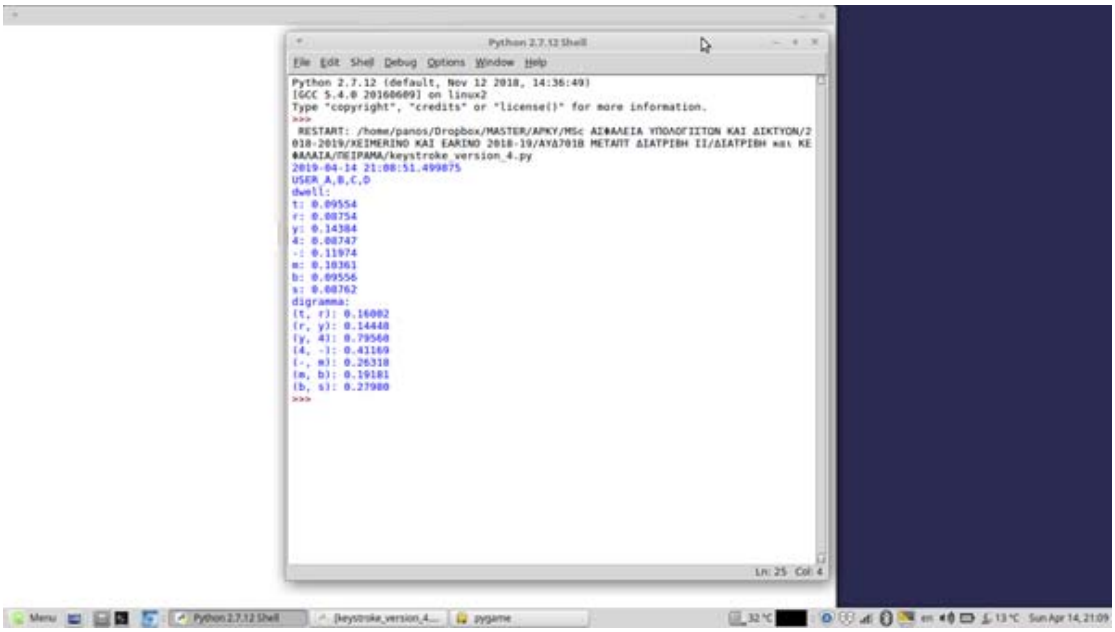
την βιβλιοθήκη Pygame 1.9.2 ώστε να υπάρξει οθόνη διεπαφής με τον χρήστη για οδηγίες στην οθόνη στους συμμετέχοντες και την ένδειξη του κωδικού μετά την επιτυχή εισαγωγή του.



Εικόνα 29, Ο κώδικας κατά τη φάση δοκιμών στο Geany text editor

Το password δεν φαίνεται κατά την πληκτρολόγηση γιατί παρατηρήθηκε ότι υπήρχε μια πρόσθετη καθυστέρηση γιατί ο χρήστης περίμενε να δει το γράμμα που πληκτρολόγησε και επηρέαζε το χρόνο εισαγωγής, και με την αλλαγή αυτή ο χρήστης δεν το βλέπει και αναγκαστικά παραμένει συγκεντρωμένος στην πληκτρολόγηση ώστε να επιτύχει τους προσωπικούς του χρόνους ανεπηρέαστος. Για αυτό μετά από **15 δοκιμαστικές εισαγωγές** του κωδικού για εξοικείωση ο χρήστης εισήγαγε τον κωδικό για να εξαχθούν οι χρόνοι σε msec. Παρατηρήθηκαν σχεδόν μηδενικές εσφαλμένες εισαγωγές (μια φορά μόνο λάθος εισαγωγή από χρήστη), πράγμα που σημαίνει ότι οι φορές προσαρμογής ήταν αρκετές και ότι το εξωτερικό πληκτρολόγιο όντως συνεισέφερε σε αυτό θετικά. Να πούμε σε αυτό το σημείο για να δώσουμε τη σημασία αυτών των λεπτομερειών, ότι γενικά στην επιστήμη των υπολογιστών υπάρχει εξειδικευμένος και μεγάλος κλάδος που είναι η βελτιστοποίηση της αλληλεπίδρασης και της επικοινωνίας μεταξύ του χρήστη και του υπολογιστή με τον διεθνή όρο “human - computer interaction”. Αυτός ο κλάδος ασχολείται με την έρευνα και την βελτίωση του περιβάλλοντος, της λογικής και της διεπαφής

(interface) των συστημάτων ώστε να γίνεται πιο φιλική και πιο αποδοτικά η χρήση του υπολογιστή ή άλλων συσκευών όπως τα smartphones από τον άνθρωπο. Κλείνοντας τη παρένθεση να πούμε ότι σε πραγματικό σύστημα ταυτοποίησης είναι φυσικό ότι οι χρόνοι μετά από δεκάδες επαναλήψεις να έχουν την τάση να μειώνονται. Το σύστημα λοιπόν πρέπει να προβλέπει σύμφωνα με την αρχή FiFo (first in – first out) ότι για παράδειγμα στην 101η εισαγωγή να αποθηκεύει αυτή τη τελευταία και να διαγράφει το χρόνο της πρώτης κ.ο.κ. ώστε να εξελίσσεται η μάθηση του συστήματος για το ρυθμό πληκτρολόγησης παράλληλα με τη ταχύτητα του χρήστη, ένας τρόπος ουσιαστικά που παραπέμπει σε μεθόδους machine learning. Στην επόμενη ενότητα θα δούμε τα αποτελέσματα του πειράματος.



Εικόνα 30, έξοδος προγράμματος στο τέλος της εισαγωγής του κωδικού

Κεφάλαιο 5

Συγκέντρωση, ανάλυση και ερμηνεία των δεδομένων

Είδαμε ότι η παρούσα εργασία εδράζεται πάνω σε δυο πειραματικά εργαλεία, το ερωτηματολόγιο που θα μας βοηθήσει να εξάγουμε πολύ χρήσιμες πληροφορίες σχετικά με την αποδοχή αλλά και την γνώση του κοινού πάνω στα βιομετρικά και πιο συγκεκριμένα στο βιομετρικό συμπεριφοράς που εξετάζουμε, και το πείραμα εισαγωγής κωδικού σε πρόγραμμα Python που θα μας δώσει τις μετρήσεις των χρόνων ώστε να διαπιστώσουμε τη μοναδικότητα των ατόμων μέσα από τα keystroke dynamics. Οι μετρήσεις που θα γίνουν θα αφορούν το Hold Time δηλαδή ο χρόνος που κρατείται ένα πλήκτρο πατημένο αλλά και το digraph που θα μας δίνει το χρόνο από τη στιγμή που πληκτρολογείται ένα πλήκτρο μέχρι και το χρόνο που θα αφεθεί το αμέσως επόμενο πλήκτρο.

5.1 Απαντήσεις Ερωτηματολογίου

Θα ξεκινήσουμε με την ανάλυση και ερμηνεία των αποτελεσμάτων του ερωτηματολογίου βήμα-βήμα ώστε να εξηγήσουμε και το ρόλο της κάθε ερώτησης. Υπενθυμίζουμε ότι όλες οι ερωτήσεις είχαν ως υποχρεωτική την απάντηση, πράγμα το οποίο θα εξηγηθεί στην πορεία.

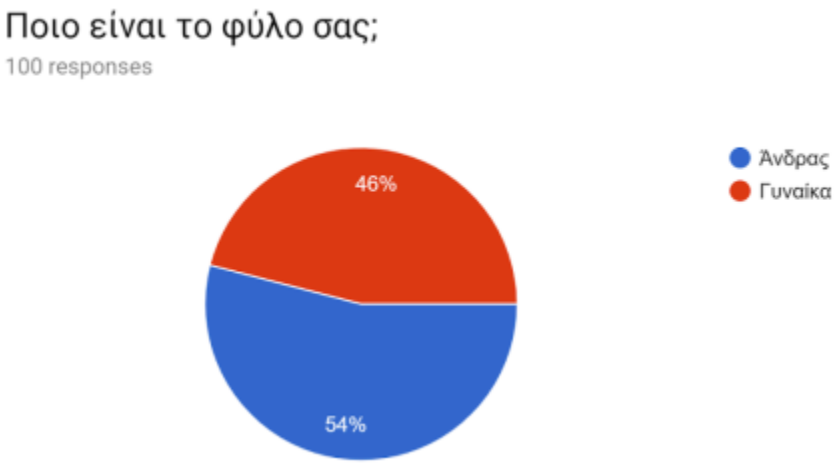
Το ερωτηματολόγιο δημιουργήθηκε ώστε να εξάγει πληροφορίες χωρίς να είναι κουραστικό, να μην χρειάζεται να περιηγηθεί και σε δεύτερη σελίδα, οι ερωτήσεις να είναι σύντομες και περιεκτικές και όλα αυτά σε ένα θέμα όπως τα βιομετρικά που γενικά είναι ευαίσθητο και το κοινό το αντιμετωπίζει με κάποιο σκεπτικισμό. Έγινε διαθέσιμο online την Κυριακή 31/3/19 και έγινε ενημέρωση στο κοινό μέσω πολλών καναλιών όπως e-mail, viber, skype, messenger,

facebook και με τη παράκληση να προωθηθεί από τους ληφθέντες και σε άλλους ώστε να μεγαλώσει η συμμετοχή.

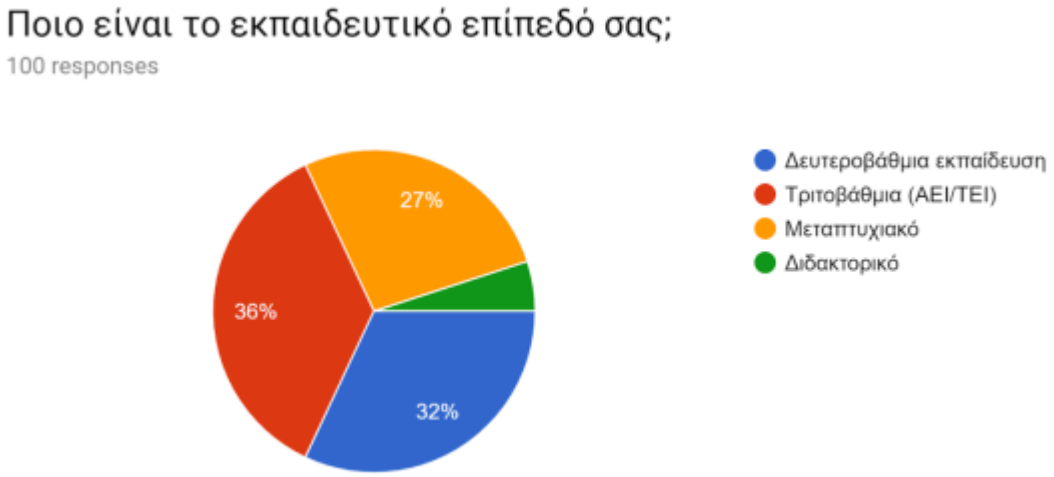
Η συμμετοχή και η απόκριση ήταν μεγάλη και φτάνοντας τον αριθμό των **εκατό (100) απαντήσεων,** το ερωτηματολόγιο έκλεισε το Σάββατο 6/4/19, και έγινε αποστολή και ανάρτηση της λήξης του ερωτηματολογίου με τις ευχαριστίες προς τους συμμετέχοντες.

Η 1η εισαγωγική ερώτηση είναι η : *Σε ποια ηλικιακή ομάδα ανήκετε;* Εδώ θέλουμε να ξεκινήσουμε με το ηλικιακό εύρος των συμμετεχόντων. Τα αποτελέσματα σε αυτή την ερώτηση ήταν: Στις ηλικίες 18-25, 4 συμμετέχοντες, στις ηλικίες 26-39, 38 συμμετέχοντες, στις ηλικίες 40-54, 47 συμμετέχοντες και στις ηλικίες 55+, 11 συμμετέχοντες.

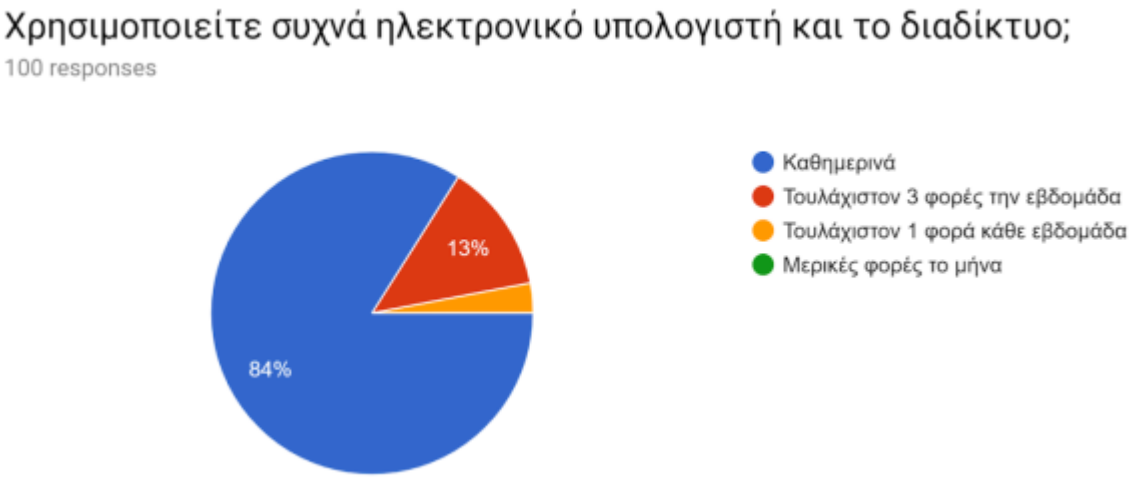
Η 2η ερώτηση στη συνέχεια είναι: *Ποιο είναι το φύλο σας;* Με αυτή την ερώτηση θέλουμε να δούμε το ποσοστό συμμετοχής των φύλων στην έρευνα μας, και τα ποσοστά αυτά είναι: 54 άνδρες και 46 γυναίκες.



Η 3η ερώτηση είναι : *Ποιο είναι το εκπαιδευτικό επίπεδό σας;* Με αυτή την ερώτηση θέλουμε να δούμε το επίπεδο της εκπαίδευσης. Τα αποτελέσματα ήταν, Δευτεροβάθμια εκπαίδευση, 32%, Τριτοβάθμια (ΑΕΙ/ΤΕΙ), 36%, Μεταπτυχιακό, 27%, Διδακτορικό 5%.



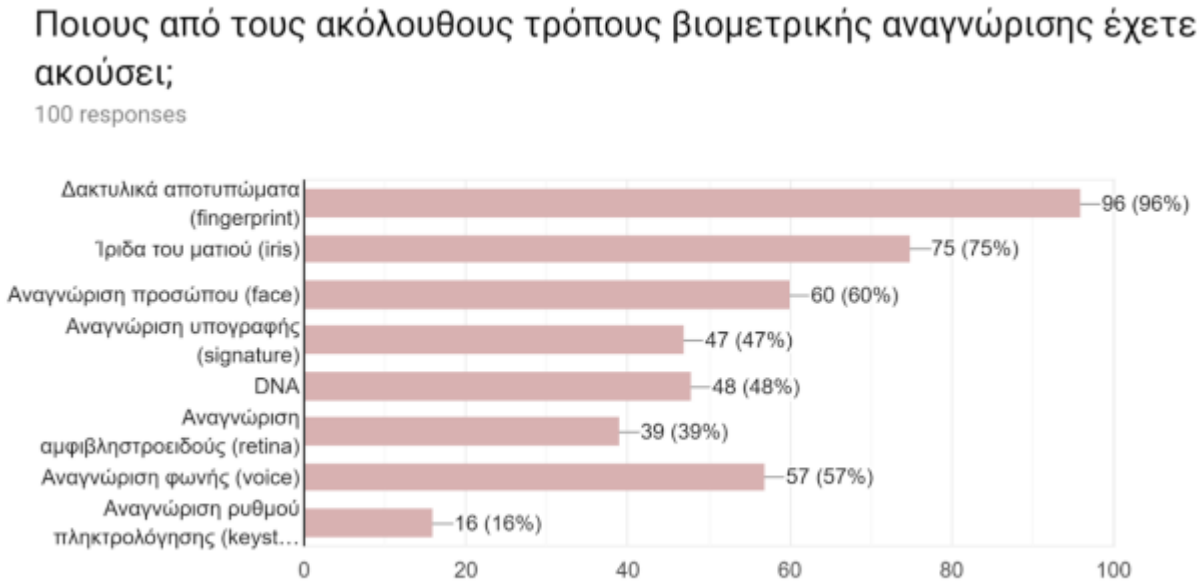
Η 4η ερώτηση που θέλει να βγάλει συμπεράσματα για την εμπειρία γνώσης χρήσης ΗΥ και του διαδικτύου είναι: *Χρησιμοποιείτε συχνά ηλεκτρονικό υπολογιστή και το διαδίκτυο;* Εδώ συντριπτικό ήταν το αποτέλεσμα της καθημερινής χρήσης με 84 άτομα, 13 άτομα κάνουν χρήση τουλάχιστον 3 φορές την εβδομάδα, μόνο 3 άτομα με τουλάχιστον 1 φορά χρήση την εβδομάδα και κανένας με πιο αραιή χρήση.



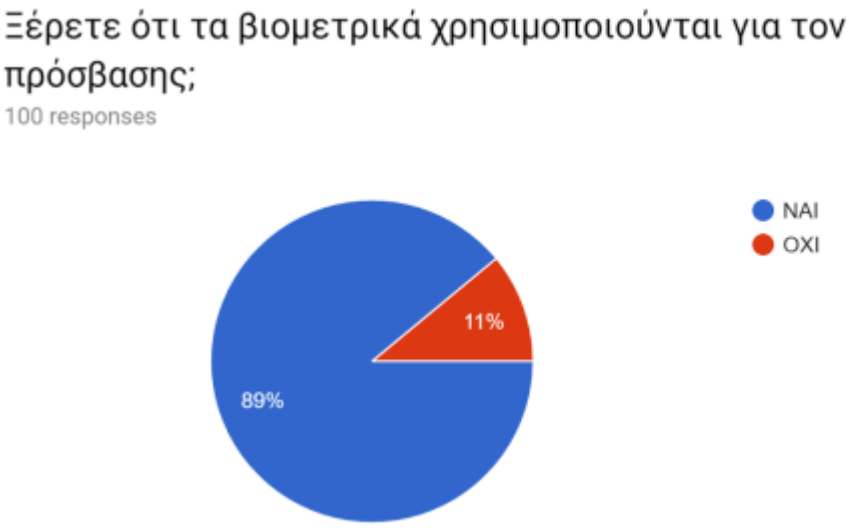
Στην 5η ερώτηση είναι η πρώτη ερώτηση σχετικά με τα βιομετρικά που είναι η: *Γνωρίζετε τι είναι τα βιομετρικά;* Και με επιλογές τα *Ναι, γνωρίζω Όχι δεν γνωρίζω, Έχω ακούσει αλλά δεν είμαι σίγουρος/η*. Εδώ έχουμε τα πρώτα ενδιαφέροντα ευρήματα αφού έχουμε 58% που γνωρίζουν τα βιομετρικά, 12% που δεν γνωρίζουν καθόλου και 30% που έχουν ακούσει αλλά δεν είναι σίγουροι. Δηλαδή 42% αθροιστικά δεν γνωρίζουν σίγουρα ή καθόλου σχετικά με τα βιομετρικά.

Η 6η ερώτηση είναι σχετικά με τη γνώση των συμμετεχόντων πάνω στους διαφορετικούς τύπους βιομετρικής αναγνώρισης. Εδώ είναι υποχρεωτική τουλάχιστον μια απάντηση μια που όλοι οι Έλληνες πολίτες υποχρεούνται σε έκδοση ταυτότητας από 15 ετών και άρα γνωρίζουν τουλάχιστον σχετικά με τα δακτυλικά αποτυπώματα : *Ποιους από τους ακόλουθους τρόπους βιομετρικής*

αναγνώρισης έχετε ακούσει; Με επιλογές 8 διαφορετικών τύπων βιομετρικών έχουμε με σειρά 96% γνωρίζουν τα δακτυλικά αποτυπώματα, 75% την ίριδα του ματιού, 60% την αναγνώριση προσώπου, 57% αναγνώριση της φωνής, 48% DNA, 47% αναγνώριση της υπογραφής, 39% αναγνώριση του αμφιβληστροειδούς και μόνο 16% γνωρίζουν το ρυθμό της πληκτρολόγησης (keystroke dynamics). Αυτό είναι ένα σημαντικό εύρημα μια που δείχνει την έλλειψη ενημέρωσης του κοινού για αυτό το τύπο του βιομετρικού της συμπεριφοράς.



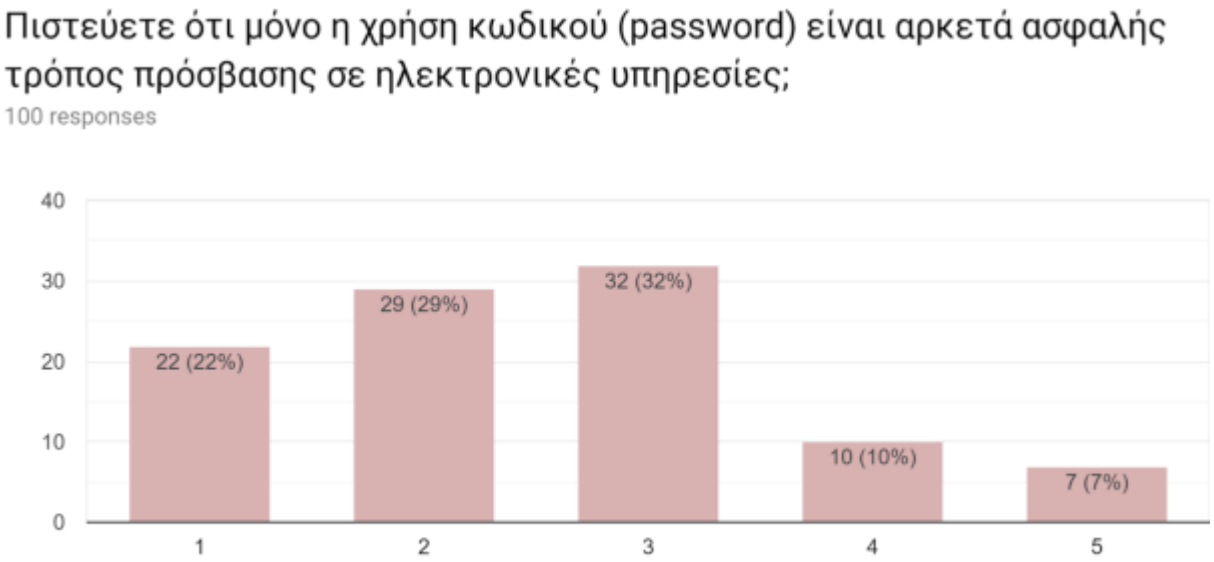
Η 7η ερώτηση είναι σχετικά με τη γνώση της εφαρμογής των βιομετρικών στοιχείων για τον έλεγχο πρόσβασης *Ξέρετε ότι τα βιομετρικά χρησιμοποιούνται για τον έλεγχο της πρόσβασης;* Με τα εξής αποτελέσματα ΝΑΙ 89%, ΟΧΙ 11%.



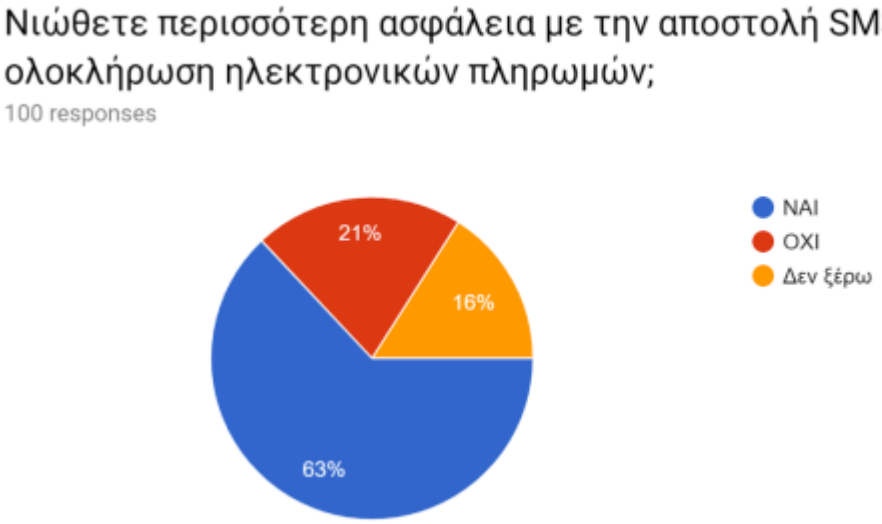
Συνεχίζουμε στην 8η ερώτηση που ουσιαστικά θυμίζει στους συμμετέχοντες το γεγονός της ύπαρξης των βιομετρικών τους σε δημόσια έγγραφα. Η ερώτηση είναι: *Γνωρίζετε ότι βιομετρικά στοιχεία σας περιέχονται ήδη στα δελτία ταυτότητας, διαβατήρια, άδεια οδήγησης, στη τράπεζα σας και αλλού;* Με τα εξής αποτελέσματα ΝΑΙ 69%, ΟΧΙ 31%. Δηλαδή εδώ έχουμε την παραδοχή ότι δεν γνωρίζουν την ύπαρξη των βιομετρικών σε τέτοιου είδους έγγραφα και συναλλαγές. Στην ταυτότητα τα δακτυλικά και η φωτογραφία αλλά στα διαβατήρια και στα νέου τύπου διπλώματα αλλά και η υπογραφή αποτελούν βιομετρικά στοιχεία.

Εικόνα 31, δίπλωμα ΕΕ με την φωτογραφία ειδικών προδιαγραφών και υπογραφή

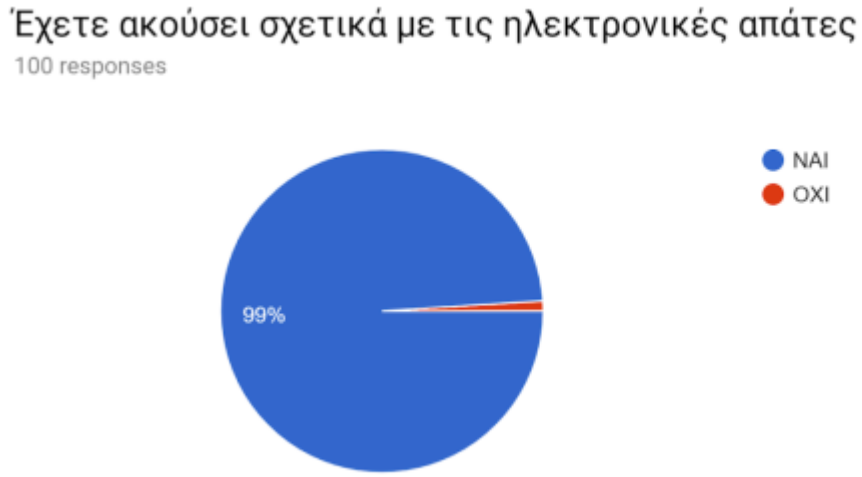
Συνεχίζουμε στην 9η ερώτηση που είναι σχετικά με το αίσθημα ασφάλειας μέσω του password: *Πιστεύετε ότι μόνο η χρήση κωδικού (password) είναι αρκετά ασφαλής τρόπος πρόσβασης σε ηλεκτρονικές υπηρεσίες;* Με απαντήσεις σε γραμμική διαβάθμιση από το 1 έως το 5: *Λιγότερο ασφαλής τρόπος 1, 2, 3, 4, 5 Πολύ ασφαλής τρόπος*. Εδώ βλέπουμε ότι μόνο το 17% θεωρεί πολύ και σχετικά ασφαλές τη χρήση μόνο του password, ενώ το 51% θεωρεί λιγότερο και σχετικά λιγότερο ασφαλές μόνο το password. 32% βρίσκεται στη μέση και από τη πλευρά της ασφάλειας των υπολογιστών καλό είναι να το θεωρήσουμε ότι κλίνει προς το μη ασφαλές και ότι θα προτιμούσε και κάποιο πρόσθετο μέτρο όπως το 2 factor.



Στην 10η ερώτηση, γίνεται προσπάθεια να εξαχθούν συμπεράσματα μέσα από ένα πραγματικό παράδειγμα two factor authentication, μέσα από την εμπειρία των χρηστών: *Νιώθετε περισσότερη ασφάλεια με την αποστολή SMS για τη ολοκλήρωση ηλεκτρονικών πληρωμών;* Με επιλογές τα: *ΝΑΙ, ΟΧΙ, Δεν ξέρω*. Εδώ ουσιαστικά επιβεβαιώνουμε την υπόθεση της προηγούμενης ερώτησης αφού με την αποστολή sms για επιβεβαίωση το 63% νιώθει περισσότερη ασφάλεια, με ένα σημαντικό 37% να μην ξέρει και να μην νιώθει ασφάλεια.

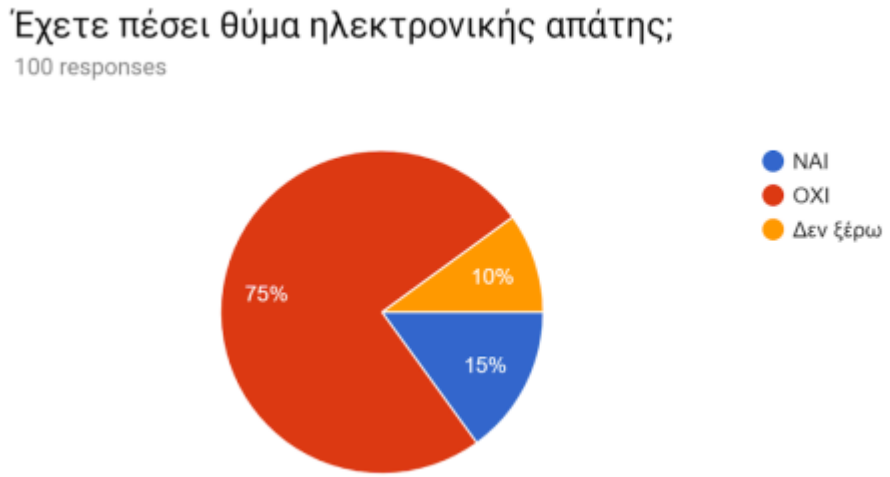


Στην 11η ερώτηση ρωτάμε για να μάθουμε σχετικά με την γνώση πάνω στην ασφάλεια των υπολογιστών και το ηλεκτρονικό έγκλημα: *Έχετε ακούσει σχετικά με τις ηλεκτρονικές απάτες;* Με το συντριπτικό 99% έχουμε την θετική απάντηση, ότι δηλαδή έχουν ακούσει για τις ηλεκτρονικές απάτες.



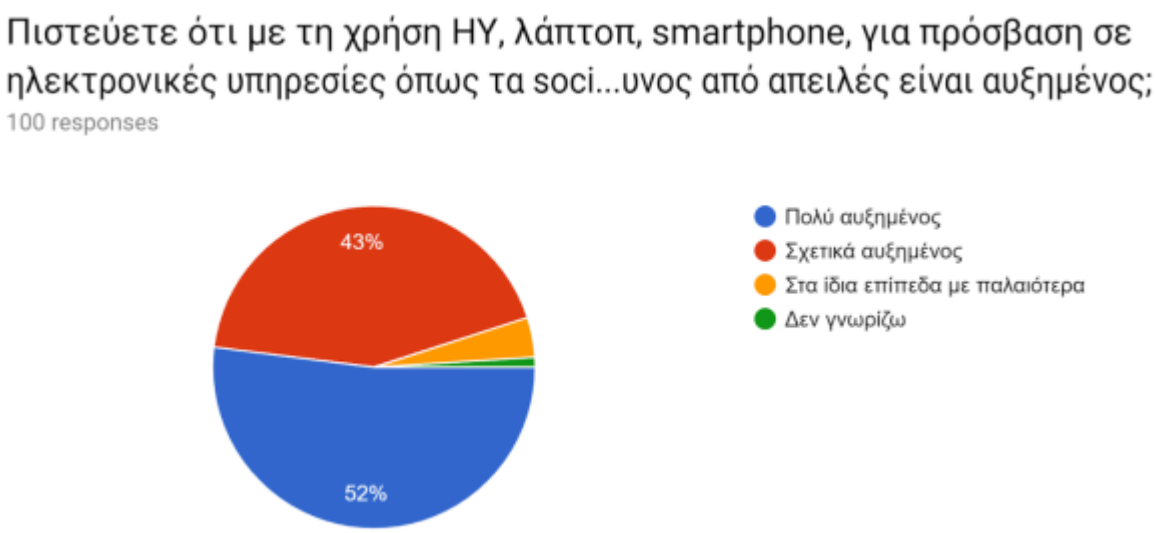
Στην 12η ερώτηση θέλουμε να μάθουμε αν υπήρξε περιστατικό που ο συμμετέχοντας να έπεσε θύμα ηλεκτρονικής απάτης: *Έχετε πέσει θύμα ηλεκτρονικής απάτης;*

Εδώ βλέπουμε ένα πολύ σημαντικό ποσοστό των 75% που δεν έχει πέσει θύμα ηλεκτρονικής απάτης. Έχουμε επίσης ένα ποσοστό του 15% που έχει πέσει και το σημαντικό εύρημα του 10% που δεν γνωρίζει αν και πότε έχει πέσει θύμα ηλεκτρονικής απάτης που σημαίνει ότι δεν γνωρίζει τον τρόπο να το επαληθεύσει.

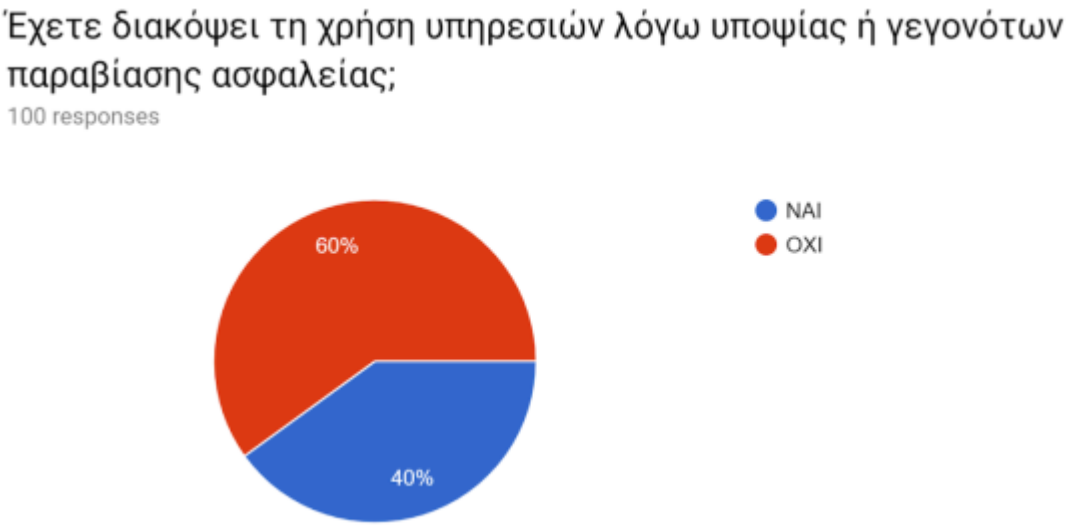


Στην επόμενη ερώτηση που είναι η 13η θέλουμε να μάθουμε αν γνωρίζουν ότι με την χρήση καθημερινά πολλαπλών συσκευών για σύνδεση σε ευαίσθητες και κρίσιμες υπηρεσίες, ο κίνδυνος από κακόβουλο λογισμικό ή phishing είναι αυξημένος: *Πιστεύετε ότι με τη χρήση ΗΥ, λάπτοπ, smartphone, για πρόσβαση σε ηλεκτρονικές υπηρεσίες όπως τα social media (facebook, twitter, instagram), ηλεκτρονική τραπεζική και ηλεκτρονικό ταχυδρομείο, ο κίνδυνος από απειλές είναι αυξημένος;*

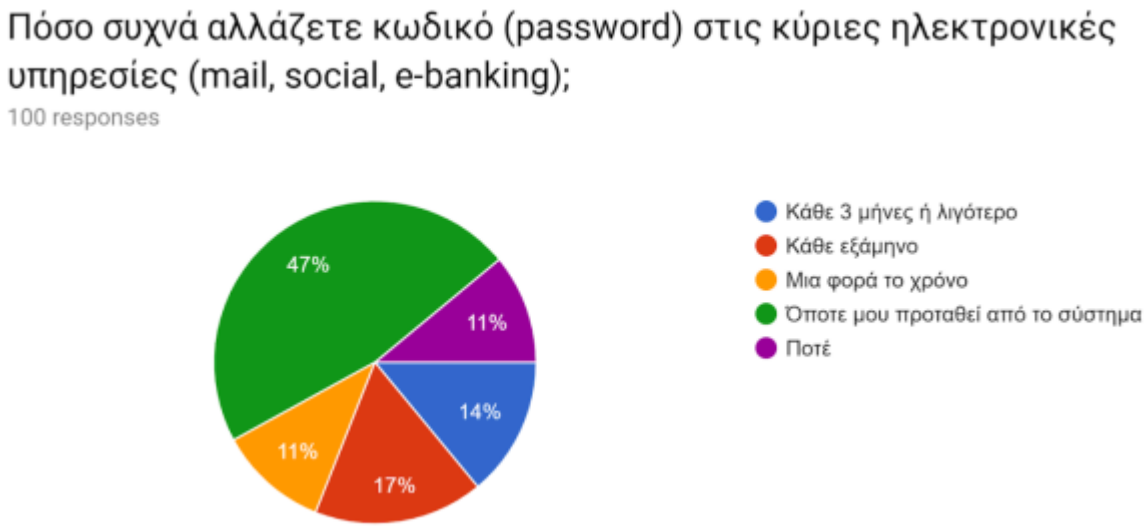
Έχουμε τα εξής ενδιαφέροντα αποτελέσματα: Πολύ αυξημένο κίνδυνο αντιλαμβάνεται το 52%, Σχετικά αυξημένο το 43%, Στα ίδια επίπεδα με παλαιότερα το 4%, και αυτοί που δεν γνωρίζουν το 1%. Άρα εδώ έχουμε ένα ισχυρό 95% που είναι ενημερωμένο σχετικά με τους κινδύνους λόγω της χρήσης ηλεκτρονικών υπηρεσιών από διαφορετικές συσκευές.



Στην ερώτηση 14 θέλουμε να μάθουμε αν έχει υπάρξει διακοπή σε υπηρεσία λόγω παραβίασης ασφαλείας: *Έχετε διακόψει τη χρήση υπηρεσιών λόγω υποψίας ή γεγονότων παραβίασης ασφαλείας;* Τα αποτελέσματα είναι: το 60% δεν έχει διακόψει, αλλά το σημαντικό ποσοστό των 40% έχει διακόψει τη χρήση υπηρεσιών λόγω υποψίας ή γεγονότων παραβίασης ασφαλείας.



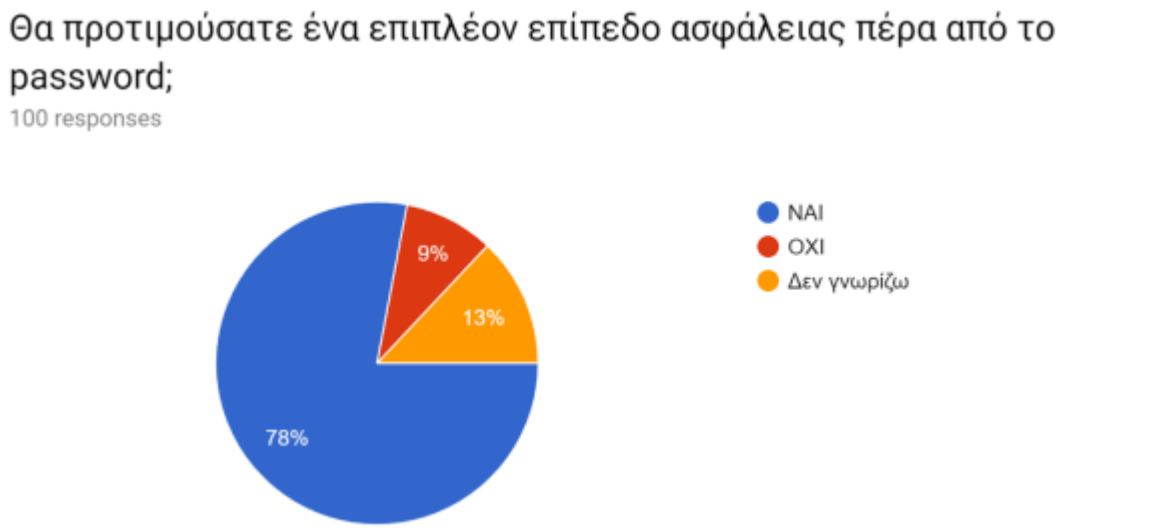
Στην 15η ερώτηση, ρωτάμε αν γίνεται και πόσο συχνά η αλλαγή των password: *Πόσο συχνά αλλάζετε κωδικό (password) στις κύριες ηλεκτρονικές υπηρεσίες (mail, social, e-banking);* Πολύ σημαντική ερώτηση και τα αποτελέσματα είναι Ποτέ το 11%, Όποτε προταθεί από το σύστημα το 47%, μια φορά το χρόνο το 11%, κάθε έξι μήνες το 17% και τέλος κάθε τρεις μήνες ή συχνότερα το 14%. Δηλαδή βλέπουμε με ενδιαφέρον ότι ένα ποσοστό 58% αλλάζει όποτε απαιτηθεί από το σύστημα ή και ποτέ, δημιουργώντας μια σημαντική ευπάθεια λόγω του ανθρώπινου παράγοντα.



Στην 16η ερώτηση μαθαίνουμε για μολύνσεις από κακόβουλο λογισμικό: *Έχει προσβληθεί από ιό ή άλλο κακόβουλο λογισμικό ο υπολογιστής ή άλλη συσκευή*

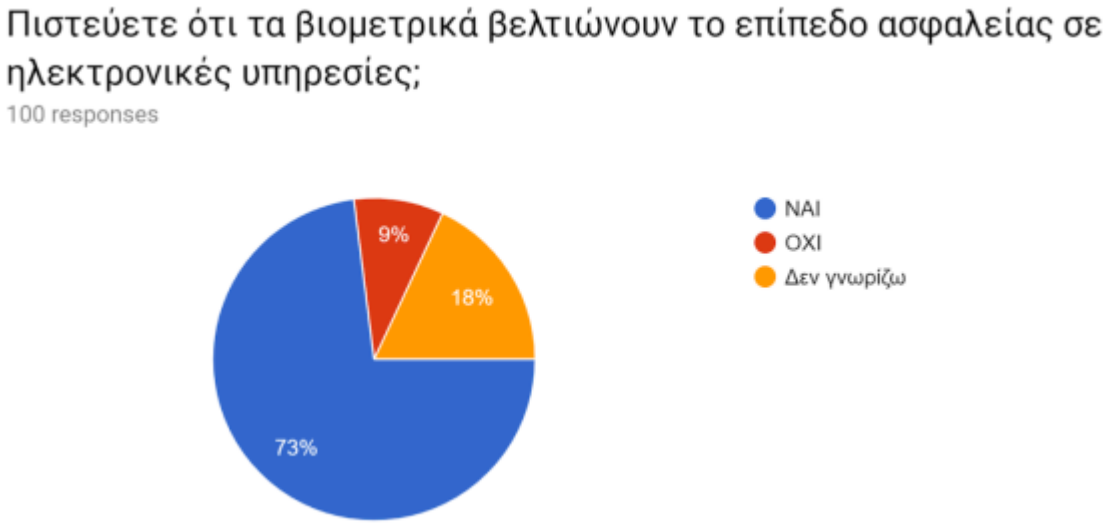
σας; Με αποτελέσματα τα ΝΑΙ σε 57%, ΟΧΙ 36% και δεν γνωρίζω το 7%, μπορούμε να πούμε ότι πάνω από τους 6 στους 10 χρήστες ΗΥ έχουν περιστατικό μόλυνσης από κακόβουλο λογισμικό ή πιθανό περιστατικό.

Στην 17η ερώτηση θέλουμε να βγάλουμε συμπεράσματα για το 2 factor authentication: *Θα προτιμούσατε ένα επιπλέον επίπεδο ασφάλειας πέρα από το password;* Και με επιλογές τα: ΝΑΙ 78%, ΟΧΙ 9% και Δεν γνωρίζω 13% έχουμε συντριπτική προτίμηση στο επιπλέον μέτρο ασφαλείας.

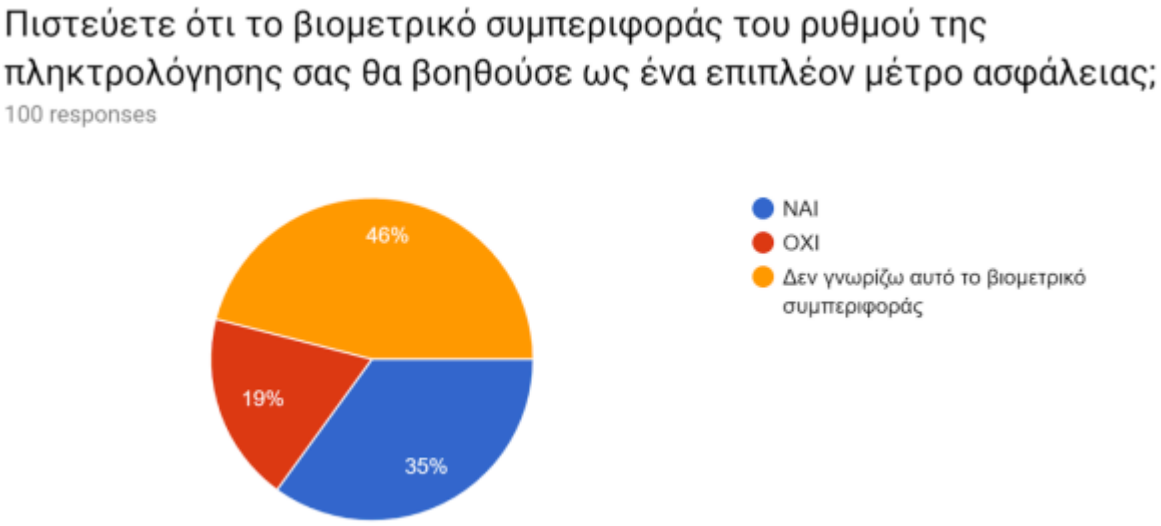


Η 18η ερώτηση θέλει να μάθει για την γνώμη των συμμετεχόντων πάνω στα βιομετρικά και ως πρόσθετο μέσο ασφάλειας: *Πιστεύετε ότι τα βιομετρικά βελτιώνουν το επίπεδο ασφαλείας σε ηλεκτρονικές υπηρεσίες;* Εδώ θα περίμενε

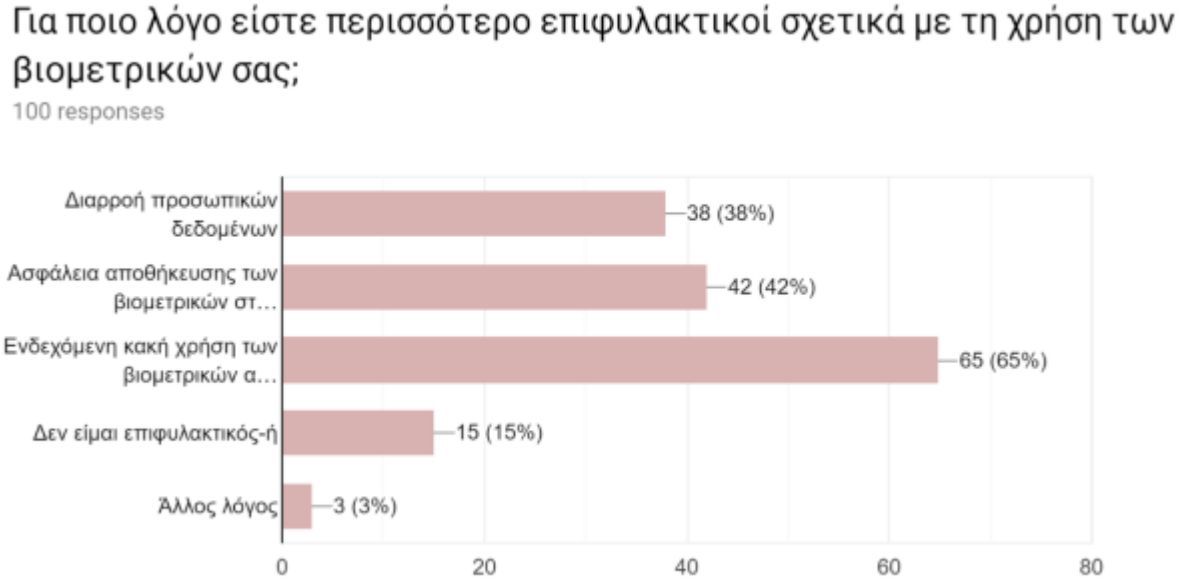
κάποιος να υπάρχει μια επιφύλαξη αλλά βλέπουμε με ενδιαφέρον ότι ΝΑΙ απαντάει το 73%, ΟΧΙ το 9% και ένα σημαντικό ποσοστό Δεν γνωρίζω με 18%. Δηλαδή ο κόσμος πιστεύει σε τουλάχιστον 78% ότι τα βιομετρικά όντως βελτιώνουν τα επίπεδα ασφαλείας.



Η 19η ερώτηση θέλει να αναδείξει τη γνώση των συμμετεχόντων πάνω στα keystroke dynamics: *Πιστεύετε ότι το βιομετρικό συμπεριφοράς του ρυθμού της πληκτρολόγησης σας θα βοηθούσε ως ένα επιπλέον μέτρο ασφάλειας;* Σημαντικά ευρήματα και εδώ με σημαντικότερο το 46% που δηλώνει ότι δεν γνωρίζει αυτό το βιομετρικό, ΟΧΙ ότι δεν το γνωρίζει δηλώνει ένα ποσοστό 19% και ΝΑΙ που ξέρει το βιομετρικό ή το αντιλαμβάνεται ένα 35%. Δηλαδή υπάρχει μια σχετική αποδοχή των keystroke dynamics από τουλάχιστον το 35% με ενδεχόμενη πιθανότητας αύξησης του ποσοστού με ενημέρωση του κοινού.



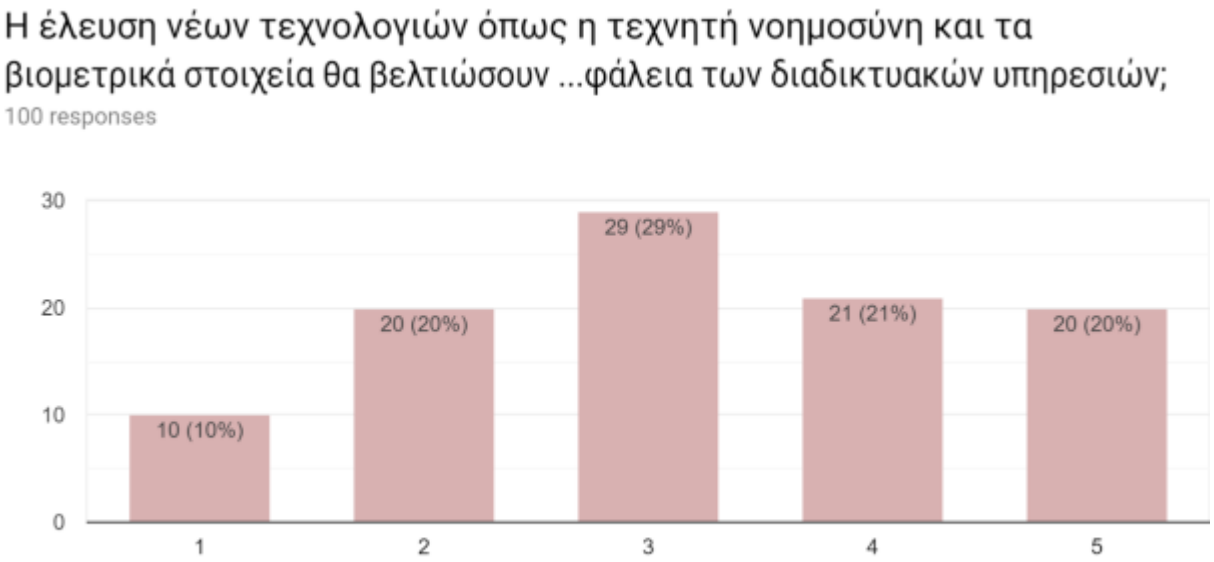
Η 20η ερώτηση είναι πάνω στους φόβους και τις επιφυλάξεις του κοινού πάνω στα βιομετρικά: *Για ποιο λόγο είστε περισσότερο επιφυλακτικοί σχετικά με τη χρήση των βιομετρικών σας;* Τα αποτελέσματα: Διαρροή προσωπικών δεδομένων 38%, Ασφάλεια αποθήκευσης των βιομετρικών στοιχείων 42%, Ενδεχόμενη κακή χρήση των βιομετρικών από τρίτους (ασφαλιστικές, κρατικές αρχές) 65%, Δεν είμαι επιφυλακτικός-ή 15%, Άλλος λόγος 3%. Εδώ βλέπουμε ότι μόνο το 15% δεν είναι επιφυλακτικοί απέναντι στη χρήση των βιομετρικών και το υπόλοιπο 85% έχει αμφιβολίες ή φόβους σχετικά με την φύλαξη ή την σωστή διαχείριση τους ακόμα και από κρατικές αρχές.



Στην 21η ερώτηση θέλουμε να μάθουμε ποιο βιομετρικό προτιμάει το κοινό ως πιο φιλικό και λιγότερο επεμβατικό (intrusive): *Ποιο βιομετρικό θα προτιμούσατε ως πιο φιλικό στη χρήση αλλά και θα θεωρούσατε λιγότερο επεμβατικό στη προσωπικότητα σας και στα προσωπικά σας δεδομένα;* Εδώ βλέπουμε ότι τα δακτυλικά αποτυπώματα είναι ξεκάθαρα η πρώτη επιλογή με 39%, πιθανά λόγω της εξοικείωσης τους με τη χρήση στην ταυτότητα. Δεύτερο βιομετρικό στην προτίμηση έρχεται το keystroke dynamics με 28% που ενώ σε προηγούμενη ερώτηση είχαμε μεγάλο ποσοστό (46%) που δεν το γνώριζε καθόλου πριν το ερωτηματολόγιο, σχεδόν το ποσοστό που το γνώριζε το προτιμάει ως πιο φιλικό και λιγότερο επεμβατικό. Ακολουθεί η αναγνώριση της υπογραφής με 25%, η αναγνώριση της φωνής με 24% και η ίριδα του ματιού με 18%. Πιο χαμηλά έχουμε την αναγνώριση του προσώπου με 12%, τον αμφιβληστροειδή με 6% και τελευταίο με 4% το DNA. Άρα στην πρώτη τετράδα προτίμησης των χρηστών έχουμε πέρα από τα δακτυλικά αποτυπώματα, τρία βιομετρικά συμπεριφοράς (φωνή, υπογραφή, πληκτρολόγηση), στοιχείο σημαντικό για την συνολική αποδοχή των βιομετρικών μέσω αυτού του τύπου των βιομετρικών σε σχέση με τα φυσιολογικά. Εδώ να υποθέσουμε ότι αν γνώριζαν οι συμμετέχοντες τους κινδύνους και την μη αντικατάσταση λόγω της μονιμότητας των δακτυλικών αποτυπωμάτων, τα αποτελέσματα πιθανά να ήταν εντελώς διαφορετικά.

Στην 22η ερώτηση θέλουμε να μάθουμε την αποδοχή του κοινού για χρήση βιομετρικού από ηλεκτρονική υπηρεσία: *Προκειμένου να εξυπηρετηθείτε καλύτερα, θα επιλέγατε να χρησιμοποιηθεί κάποιο βιομετρικό στοιχείο σας από διαδικτυακή υπηρεσία;* Με επιλογές από 1 έως 5: Δεν θα επέλεγα σίγουρα 1,2,3,4,5 Σίγουρα θα επέλεγα, βλέπουμε ότι σίγουρα ή απλά θα επέλεγα απάντησαν το 33%, σε αντίθεση με το 44% που σίγουρα ή μάλλον δεν θα το επέλεγε. Ένα 23% βρίσκεται στη μέση της κλίμακας και προφανώς θα το αλλάξει κατάλληλα σύμφωνα με την ενημέρωση που θα έχει πάνω στο θέμα.

Στην τελευταία 23η ερώτηση θέλουμε να μάθουμε πόσο αποδοχή έχουν γενικά νέες τεχνολογίες στον έλεγχο πρόσβασης: *Η έλευση νέων τεχνολογιών όπως η τεχνητή νοημοσύνη και τα βιομετρικά στοιχεία θα βελτιώσουν την ασφάλεια των διαδικτυακών υπηρεσιών;* Με επιλογές: Διαφωνώ πλήρως 1,2,3,4,5 Συμφωνώ απόλυτα, βλέπουμε ότι οι συμμετέχοντες σε ποσοστό 41% συμφωνούν απόλυτα ή σχετικά ότι θα βελτιώσουν την ασφάλεια των διαδικτυακών υπηρεσιών σε αντίθεση με το 30% που δεν συμφωνούν. Στην μέση της κλίμακας βρίσκεται ένα υπολογίσιμο 29% που δεν είναι σίγουρο για το αποτέλεσμα και προφανώς θα θέλει περισσότερες εξηγήσεις και διασφαλίσεις για να καταλήξει τελικά.



Βλέπουμε ότι εξήχθησαν σημαντικά δεδομένα από το ερωτηματολόγιο τα οποία θα αναλύσουμε περαιτέρω στα συμπεράσματα.

5.2 Μετρήσεις πειράματος

Θα συνεχίσουμε την παράθεση των δεδομένων με το δεύτερο σκέλος της πειραματικής διαδικασίας, τους χρόνους του ρυθμού της πληκτρολόγησης. Είδαμε ότι στο δικό μας πείραμα χρησιμοποιήθηκε η γλώσσα Python ως μέθοδος σύλληψης των χρόνων πληκτρολόγησης των χρηστών. Τα στοιχεία που χρησιμοποιήθηκαν ως βιομετρικοί δείκτες του ρυθμού πληκτρολόγησης των χρηστών είναι το hold-time και ο χρόνος διγράμματος (digraph), από 12 συμμετέχοντες.

Ας δούμε τις παραμέτρους που προσδίδουν στο πείραμα μας την προστασία από παράγοντες που θα μπορούσαν να επηρεάσουν τους χρόνους μεταξύ των χρηστών. Όπως είδαμε χρησιμοποιήθηκε πληκτρολόγιο κανονικού μεγέθους, που είναι πιο οικεία συσκευή εισόδου στους χρήστες. Και οι δώδεκα συμμετέχοντες έχουν εμπειρία στη χρήση ΗΥ και καθημερινή χρήση σε αυτόν. Έγινε μια μικρή δοκιμαστική εισαγωγή του κωδικού `‘try4-mbs’` ώστε να υπάρξει μια αρχική εξοικείωση των χρηστών με αυτόν. Ο αριθμός των δοκιμαστικών εισαγωγών του κωδικού ήταν 15 φορές, αριθμός ικανοποιητικός

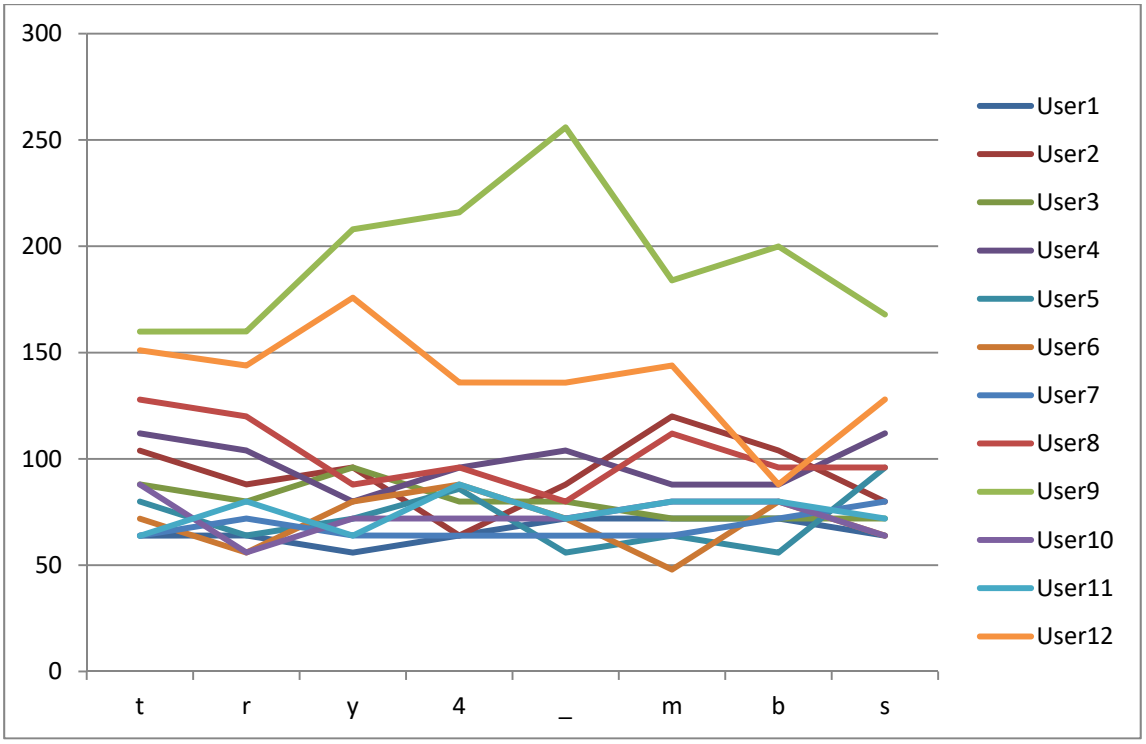
για αρχική εξοικείωση. Ακολούθησε το πείραμα με την εισαγωγή του κωδικού τρεις φορές στο πρόγραμμα. Εδώ θέλουμε να τονίσουμε ότι θέλουμε να δούμε την διαφορά των keystroke dynamics στην **αρχική περίοδο χρήσης** ενός νέου κωδικού ο οποίος μπορεί να αλλάζει είτε λόγω πρότασης του συστήματος, είτε λόγω συνήθειας του χρήστη για περιοδική αλλαγή κωδικών αλλά και ακόμα σε περιστατικό παραβίασης της ασφάλειας. Θέλουμε να δούμε λοιπόν τι διαφορές υπάρχουν από χρήστη σε χρήστη την αρχική περίοδο χρήσης ενός νέου κωδικού. Σε αυτές τις τρεις εισαγωγές των κωδικών έγινε ο υπολογισμός της μέσης τιμής, και στον κωδικό και στο κάθε δίγραμμα για απεικόνιση του ρυθμού του κάθε χρήστη.

Τα αποτελέσματα των μετρήσεων του hold time είναι τα εξής,

Χαρακτήρας	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms
	User1	**User2**	**User3**	**User4**	**User5**	**User6**	**User7**	**User8**	**User9**	**User10**	**User11**	**User12**
t	63,89	103,87	87,97	111,97	79,88	71,89	63,9	127,89	159,88	87,89	63,83	151,08
r	63,93	87,96	79,88	103,94	63,95	55,91	71,93	119,97	159,93	55,94	79,95	143,89
y	55,91	95,91	95,94	79,93	71,89	79,9	63,97	87,92	207,97	71,92	63,88	175,85
4	63,94	63,92	79,93	95,9	85,83	87,9	63,91	95,92	215,94	71,93	87,94	135,9
_	71,9	87,91	79,92	103,96	55,88	71,92	63,91	79,9	255,9	71,9	71,89	135,87
m	71,92	119,93	71,92	87,89	63,89	47,93	63,95	111,91	183,92	79,93	79,92	143,92
b	71,93	103,92	71,95	87,92	55,91	79,92	71,92	95,94	199,91	79,88	79,9	87,94
s	63,9	79,9	71,91	111,95	95,9	63,87	79,92	95,92	167,93	63,9	71,93	127,93

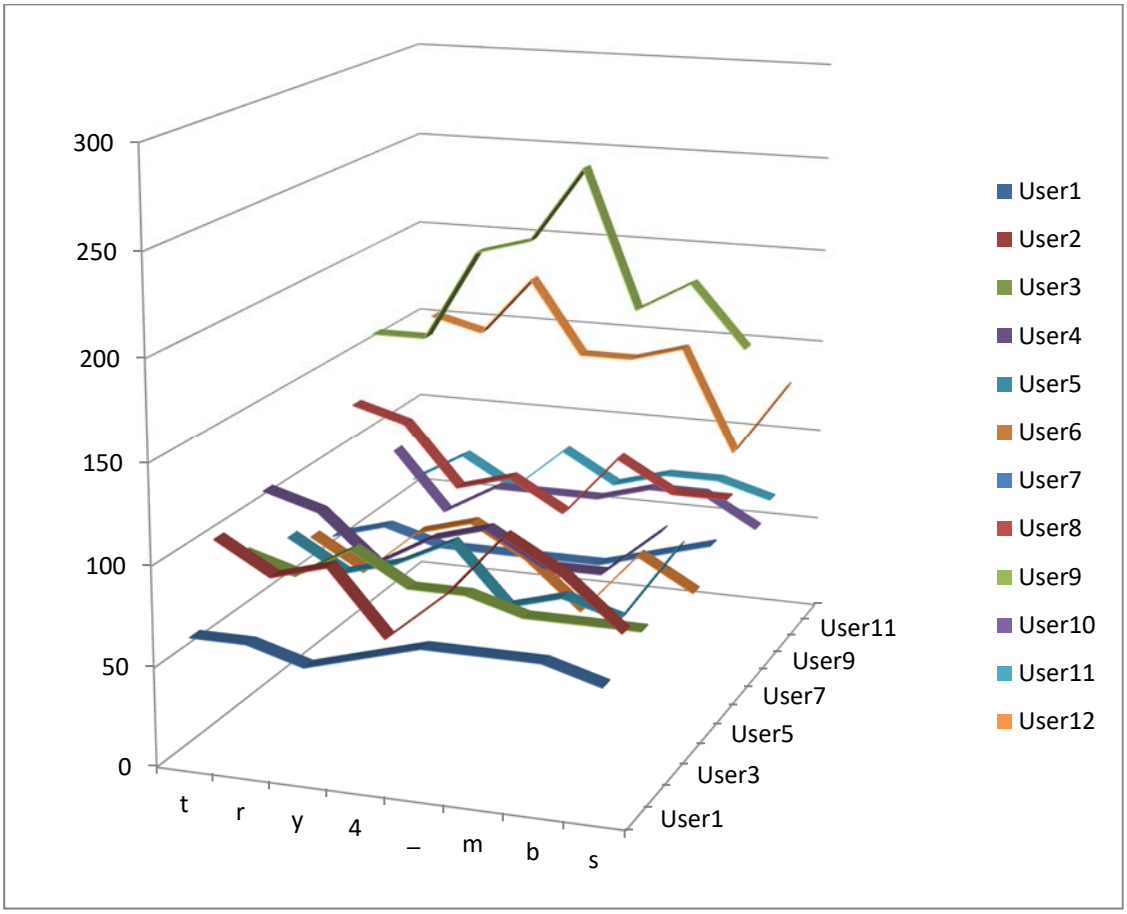
Πίνακας 1, χρόνοι μέσων όρων hold time των 12 χρηστών.

Το αντίστοιχο γράφημα απεικόνισης είναι το εξής



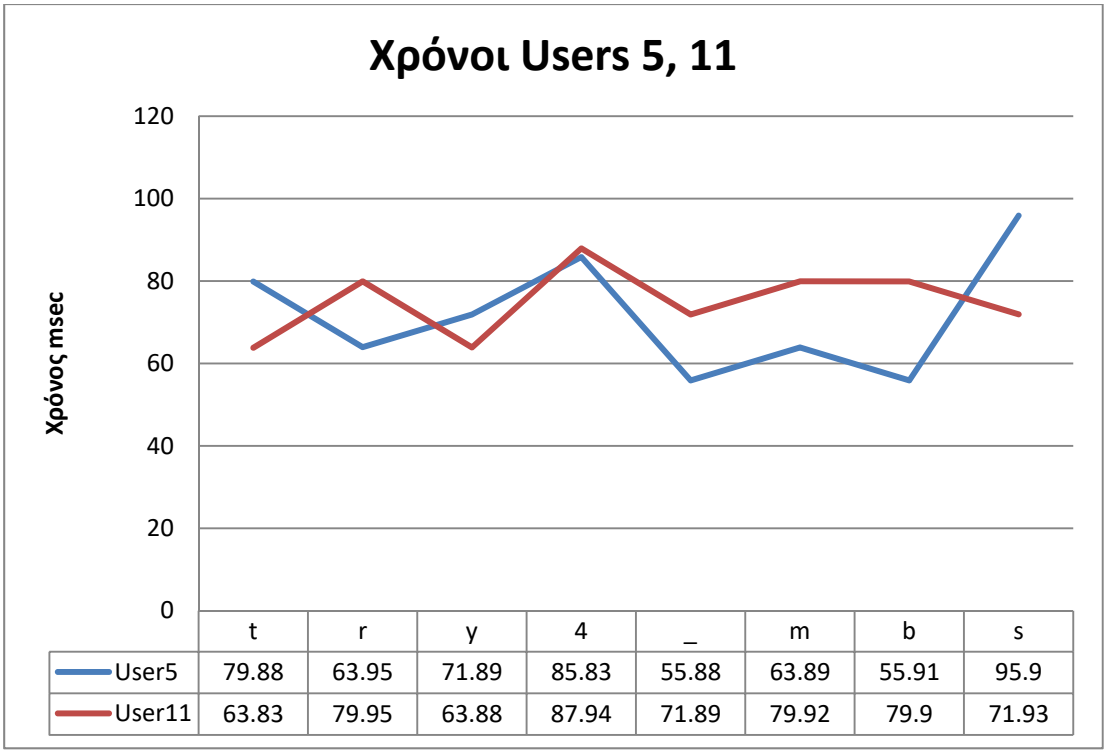
Γράφημα 1, μέσοι όροι των hold times των 12 χρηστών

Ας δούμε και το γράφημα σε τρισδιάστατη απεικόνιση σε άλλη προοπτική



Γράφημα 2, τρισδιάστατη απεικόνιση μέσων όρων των hold times των 12 χρηστών

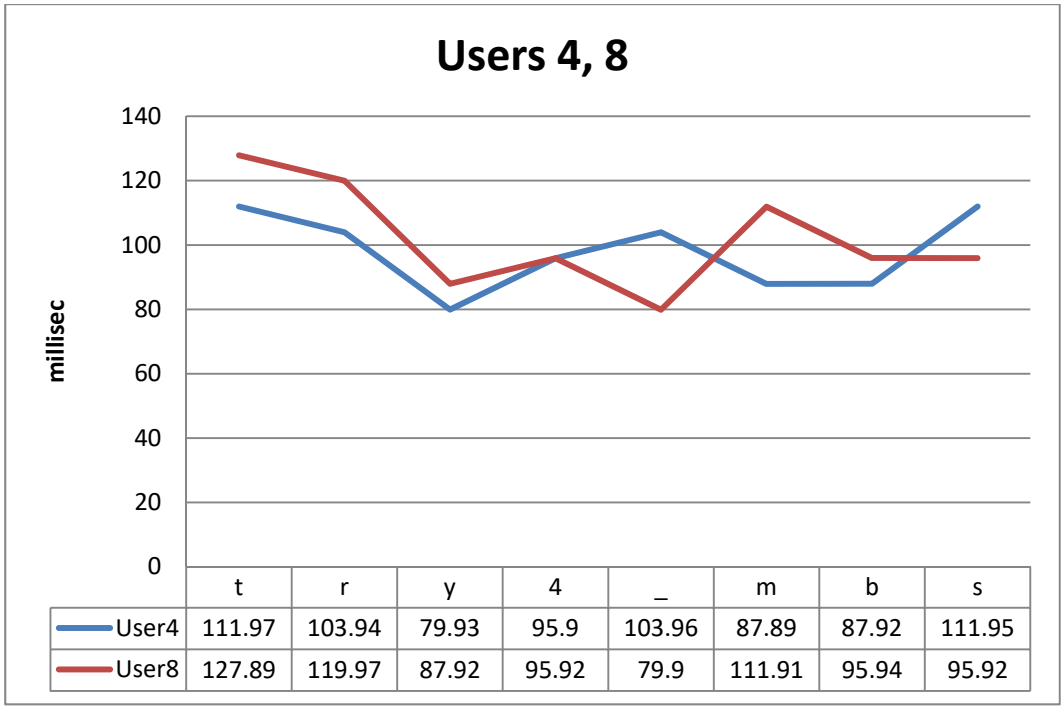
Ήδη βλέπουμε ότι κάθε χρήστης έχει το μοναδικό του τρόπο γραφής που φαίνεται όχι μόνο από το γράφημα του αλλά και σε απομονωμένα πλήκτρα ή σε συνδυασμούς. Όπου βλέπουμε σχεδόν ίδιο χρόνο σε δυο χρήστες, σε κάποια πλήκτρα βλέπουμε με ενδιαφέρον ότι αυτό δεν συνεχίζεται σε άλλα αλλά αποτελεί μοναδική παρατήρηση, κάνοντας κάθε ένα χρήστη μοναδικό από την πλευρά του τρόπου πληκτρολόγησης κάποιων πλήκτρων. Οι Users 9 και 12 είναι θα μπορούσαμε σε άλλη περίπτωση να τις πούμε ως ακραίες τιμές του γραφήματος αλλά εδώ σε αυτούς τους δυο, ο τρόπος πληκτρολόγησης είναι το δικό τους keystroke dynamic, το οποίο στη δική τους περίπτωση τους ξεχωρίζει μοναδικά. Ας δούμε ένα ζεύγος χρηστών που φαίνονται να έχουν το ίδιο γράφημα για να συγκρίνουμε δυο φαινομενικά ίδιους χρόνους πληκτρολόγησης. Επιλέγουμε τυχαία τους Users 5 και 11 για να δούμε κατά πόσο συμπίπτουν οι χρόνοι τους,



	t	r	y	4	_	m	b	s
User5	79.88	63.95	71.89	85.83	55.88	63.89	55.91	95.9
User11	63.83	79.95	63.88	87.94	71.89	79.92	79.9	71.93

Γράφημα 3, ενδεικτικοί μέσοι όροι hold times των χρηστών 5 και 11

Επιλέγουμε επίσης τυχαία το ζεύγος User 4,8 για να δούμε τους χρόνους τους,



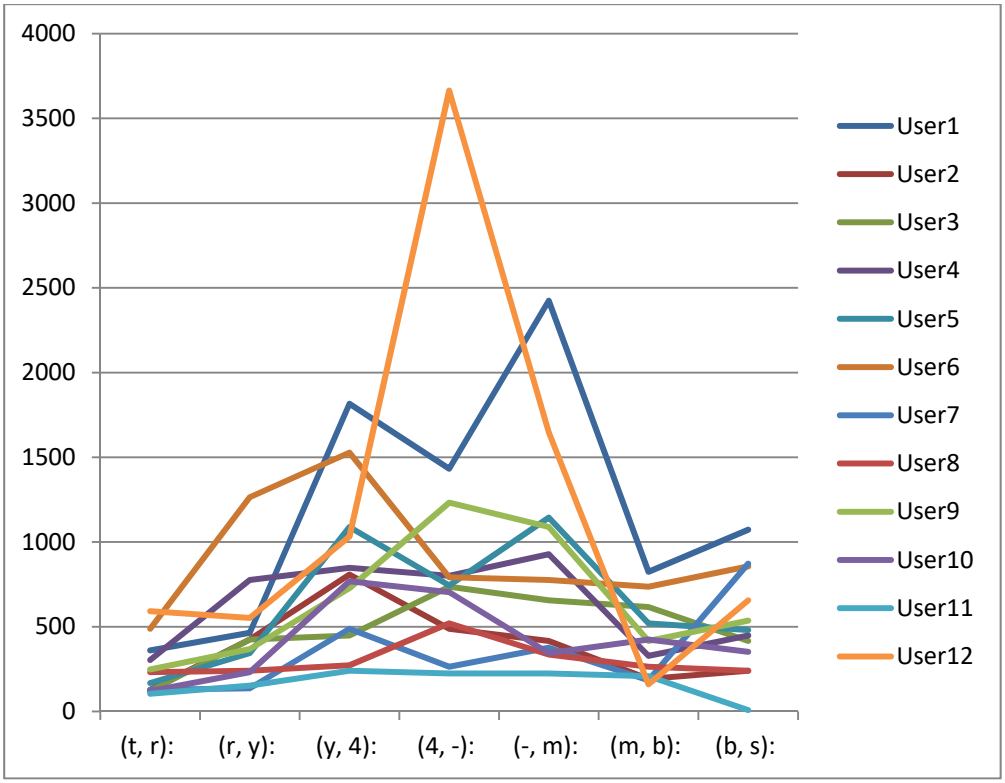
Γράφημα 3, ενδεικτικοί μέσοι όροι hold times των χρηστών 4 και 8

Βλέπουμε με ενδιαφέρον ότι όντως έχουμε διαφορετικούς χρόνους και σε όποιο γράμμα τείνουν να συμπέσουν είναι σχεδόν μόνο στους 2 από τους 8 χαρακτήρες.

Συνεχίζουμε με την παράθεση των πινάκων των διγραμμάτων (digraphs) με τους χρόνους τους, θυμίζουμε τη διάταξη ζευγών τα (t,r), (r,y) (y,4), (4, -), (-, m), (m,b), (b,s).

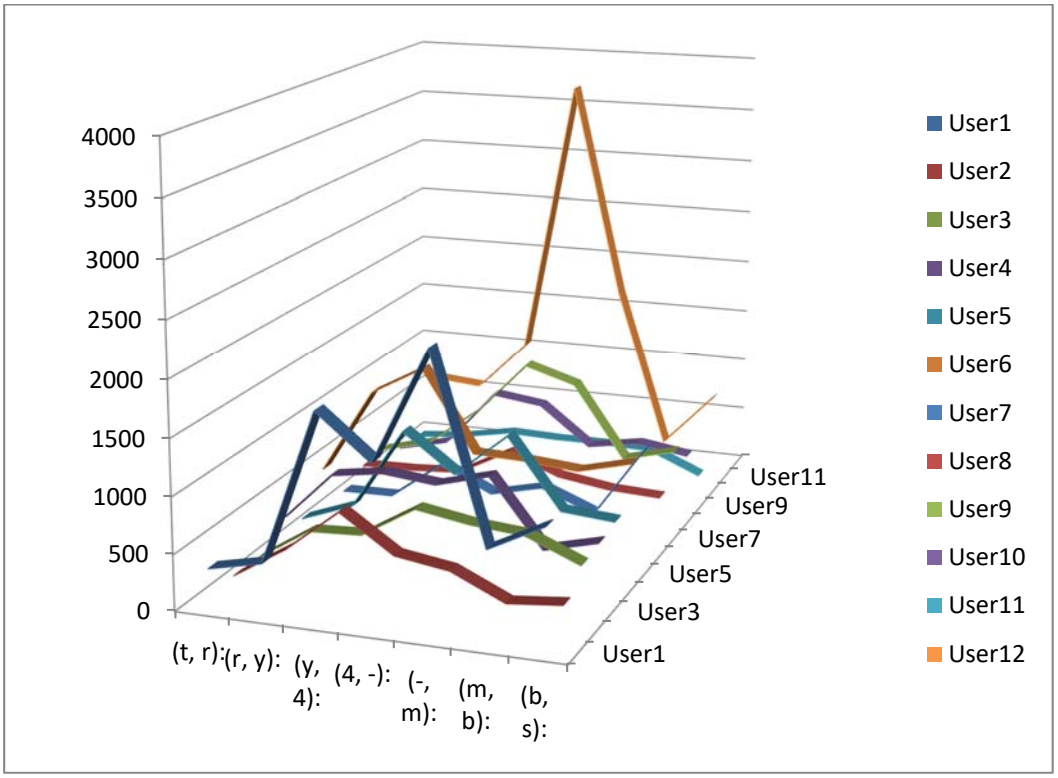
	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms
digraph	**User1**	**User2**	**User3**	**User4**	**User5**	**User6**	**User7**	**User8**	**User9**	**User10**	**User11**	**User12**
(t, r):	360,07	128,04	120,07	304,03	168,06	488,08	128,06	232,03	248,06	120,05	104,07	592,09
(r, y):	464,08	424,08	424,07	776,04	344,08	1264,08	136,08	240,07	368,09	232,09	152,08	552,14
(y, 4):	1816,07	808,08	448,07	848,12	1088,09	1528,08	488,1	272,08	728,07	768,07	240,08	1032,11
(4, -):	1432,07	488,1	736,1	800,07	744,11	792,07	264,08	520,1	1232,07	704,1	224,09	3664,09
(-, m):	2424,08	416,07	656,08	928,08	1144,1	776,07	376,1	336,09	1088,07	344,05	224,11	1648,09
(m, b):	824,09	192,06	616,05	328,05	520,09	736,06	184,05	264,07	416,07	424,12	208,08	160,04
(b, s):	1072,09	240,1	416,04	448,07	480,12	856,13	872,06	240,06	536,08	352,11	8,07	656,09

Πίνακας 2, χρόνοι διγραμμάτων (digraph) των δώδεκα χρηστών



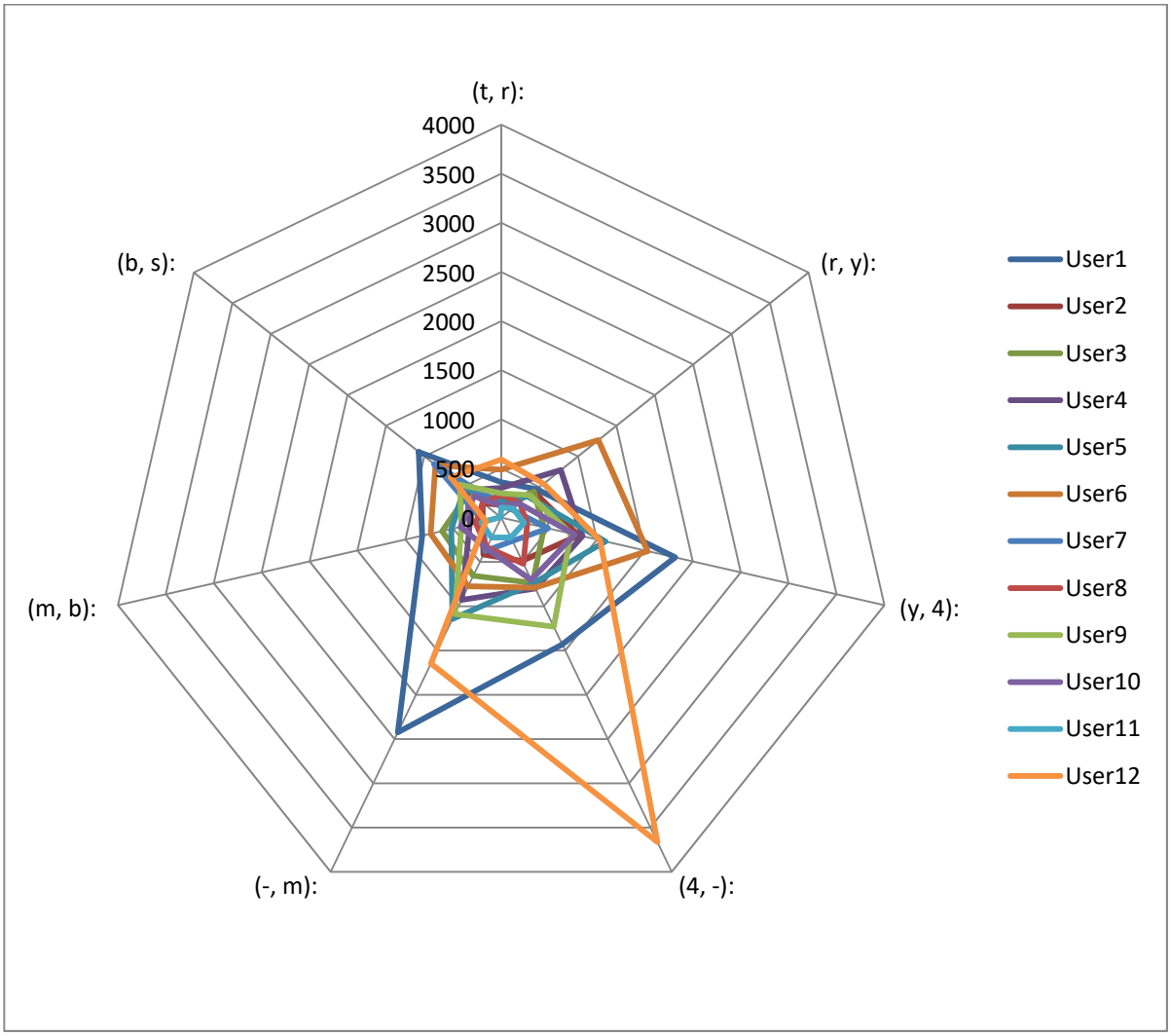
Γράφημα 4, μέσοι όροι των digraph των12 χρηστών

Διάγραμμα με τους χρόνους των διγραμμάτων των χρηστών και ακολουθεί το διάγραμμα με την τρισδιάστατη απεικόνιση των χρόνων των διγραμμάτων.



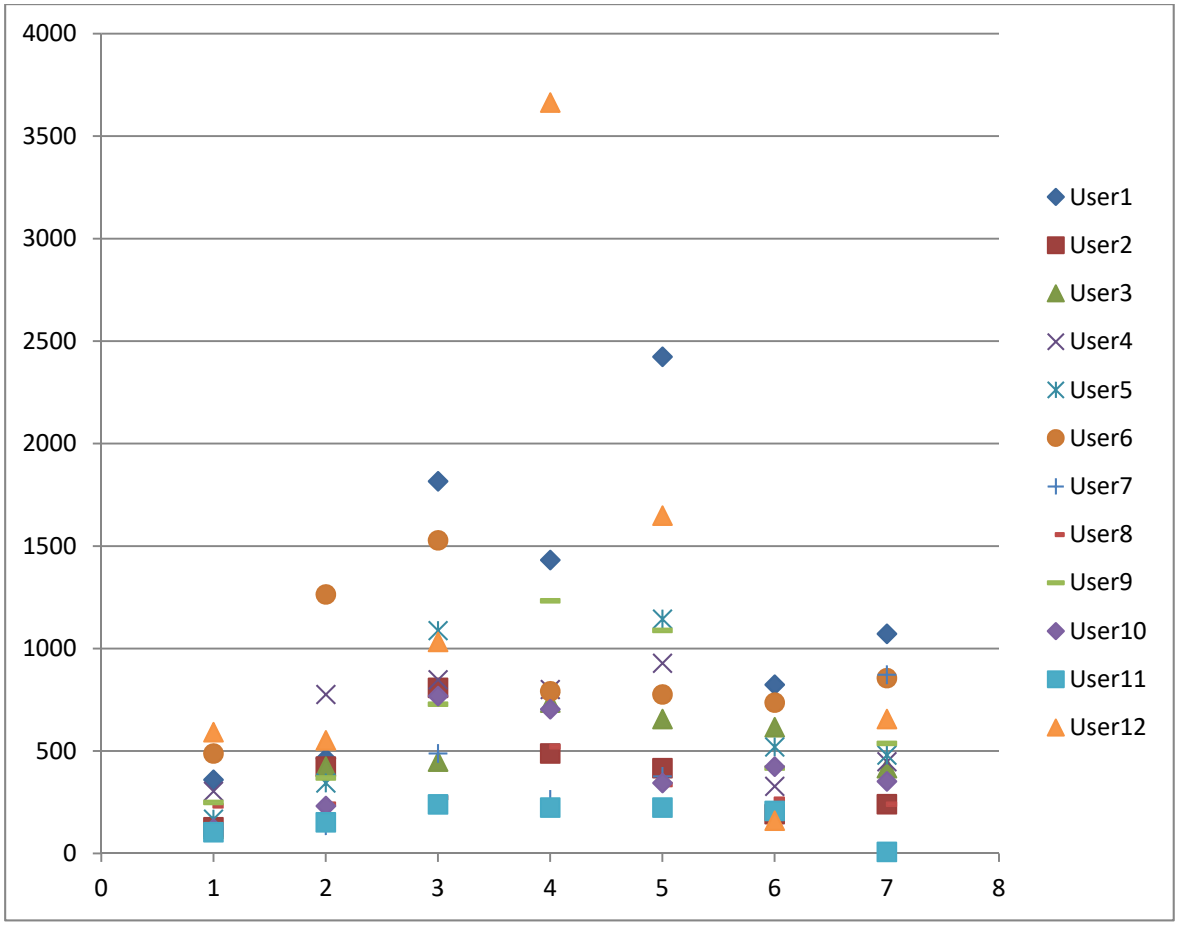
Γράφημα 5, τρισδιάστατη απεικόνιση των μέσων όρων των digraph των12 χρηστών

Βλέπουμε με ενδιαφέρον ότι απεικονίζεται πιο ξεκάθαρα ο ξεχωριστός τρόπος πληκτρολόγησης των χρηστών με την χρήση των διγραμμάτων. Ας δούμε σε αραχνοειδές διάγραμμα την συγκέντρωση των χρόνων του κάθε χρήστη για να δούμε πόσο διαφορετικός είναι όντως ο ρυθμός πληκτρολόγησης του καθενός.



Γράφημα 6, αραχνοειδές γράφημα των μέσων όρων των digraph των12 χρηστών

Ας δούμε και σε διάγραμμα διασποράς την διαφορά μεταξύ των χρόνων,



Γράφημα 6, πίνακας διασποράς των μέσων όρων των digraph των12 χρηστών

Θα δούμε στην ανάλυση των μετρήσεων τι ακριβώς συμπεράσματα μπορούν να εξαχθούν από αυτή τη διαδικασία. Βλέπουμε όμως ήδη ότι η συμπεριφορά της πληκτρολόγησης δηλαδή το βιομετρικό στοιχείο της δυναμικής της πληκτρολόγησης διαφέρει από άνθρωπο σε άνθρωπο.

5.3 Ανάλυση και ερμηνεία δεδομένων

Σε αυτή την ενότητα θα προσπαθήσουμε να παραθέσουμε και να αναλύσουμε τα στοιχεία που συγκεντρώσαμε στην έρευνα μας. Ξεκινώντας από το πρώτο κομμάτι της ερευνητικής διαδικασίας, από την δειγματοληπτική έρευνα με τη βοήθεια του ερωτηματολογίου μπορούμε να εξάγουμε χρήσιμα συμπεράσματα σχετικά με την γνώση των χρηστών πάνω στην ασφάλεια των υπολογιστών, τους κινδύνους που υπάρχουν, τα μέτρα προστασίας αλλά και τη γνώση και τις επιφυλάξεις πάνω στα βιομετρικά και ειδικότερα στα keystroke dynamics.

Ας δούμε λίγο πρώτα τα δημογραφικά του κοινού που απάντησε στο **ερωτηματολόγιο** αρχίζοντας από το φύλο όπου 54% ήταν οι άνδρες και το 46% οι γυναίκες. Στην ηλικία βλέπουμε ότι σε ποσοστό 96% είναι πάνω από 25 ετών άρα έχουν ήδη αρκετές προσλαμβάνουσες ως ώριμοι χρήστες του διαδικτύου. Στο εκπαιδευτικό επίπεδο βλέπουμε ένα σημαντικό 68% να είναι απόφοιτος τριτοβάθμιας εκπαίδευσης και το 84% χρησιμοποιεί καθημερινά το διαδίκτυο και τον ΗΥ, στατιστικό εύρημα που μας δίνει στοιχεία για την εμπειρία των χρηστών. Μπαίνοντας στα βιομετρικά βλέπουμε ότι 58% γνωρίζει τι είναι με βεβαιότητα ενώ το 30% έχει ακούσει αλλά δεν είναι σίγουρος τι είναι. Εδώ να υπενθυμίσουμε ότι από την ηλικία των 12 ο πολίτης πρέπει να εκδώσει δελτίο ταυτότητας που περιέχει τουλάχιστον δυο βιομετρικά, τα δακτυλικά αποτυπώματα και φωτογραφία με προδιαγραφές αναγνώρισης προσώπου, άρα εδώ βλέπουμε ότι ένα 42% δεν γνωρίζει ή δεν είναι σίγουρος για τα βιομετρικά.

Συνεχίζοντας για να ξεκαθαρίσουμε το παραπάνω εύρημα ρωτούμε και αναφέρουμε οκτώ τρόπους φυσιολογικής και συμπεριφορικής βιομετρικής αναγνώρισης και το ποιους από αυτούς γνωρίζουν. Εδώ ξεκαθαρίζει αφού οι κλασικοί μέθοδοι όπως τα δακτυλικά αποτυπώματα, το πρόσωπο, η ίριδα και τα υπόλοιπα, εκτός ενός, είναι γνωστά σε ποσοστό από 39% έως και 96%. Οι συμμετέχοντες γνωρίζουν αυτό το ένα βιομετρικό σε ποσοστό 16% και είναι το keystroke dynamics, εύρημα σημαντικό γιατί μας δείχνει το περιθώριο εξέλιξης που έχει και μάλιστα ως συμπεριφοράς και μη επεμβατικό βιομετρικό.

Βλέπουμε στην επόμενη ερώτηση ότι οι περισσότεροι γνωρίζουν σε ποσοστό 89% τα βιομετρικά ως μέθοδο ελέγχου της πρόσβασης αλλά το 31% δεν γνωρίζει ότι περιέχονται ήδη σε δημόσια έγγραφα όπως τα διαβατήρια, την άδεια οδήγησης και ακόμα και στην τράπεζα (η υπογραφή). Οι συμμετέχοντες αναγνωρίζουν σε ποσοστό 17% ότι μόνο ο κωδικός πρόσβασης δεν είναι ασφαλής τρόπος, το 51% δεν το θεωρεί ασφαλές, αλλά ένα σημαντικό ποσοστό 32% είναι στη μέση προφανώς γιατί δεν γνωρίζει ακριβώς τους κινδύνους παρά το ότι βλέπουμε σε επόμενη ερώτηση ότι γνωρίζουν σχετικά με ηλεκτρονικές απάτες σε ποσοστό 99%!

Σε ερώτηση για εισαγωγή στη σκέψη των συμμετεχόντων του two factor authentication βλέπουμε ότι το 63% πράγματι αντιλαμβάνεται την πρόσθετη ασφάλεια της αποστολής ενός SMS για την ολοκλήρωση ηλεκτρονικών πληρωμών αλλά υπάρχει περιθώριο βελτίωσης λόγω του υπόλοιπου 37% που δεν νιώθει περισσότερο ασφαλής ή δεν γνωρίζει τι είναι αυτό. Η επόμενη λοιπόν ερώτηση είναι πολύ χρήσιμη γιατί μας λέει πόσοι έχουν πέσει θύμα ηλεκτρονικής απάτης με ένα σημαντικό 25% να έχει πέσει ή να μην γνωρίζει με βεβαιότητα το γεγονός άρα θεωρούμε ότι λόγω μη γνώσης είναι πιθανό να έχει ή να πέσει στο μέλλον θύμα απάτης. Συνεχίζουμε με μια ερώτηση που καταδεικνύει τη γνώση των συμμετεχόντων από τον κίνδυνο που ελλοχεύει από τη χρήση πολλών συσκευών (tablet, laptop, PC, smartphone) για πρόσβαση στο διαδίκτυο και σε ευαίσθητες υπηρεσίες όπως το web-banking. Σε συντριπτικό ποσοστό 95% λοιπόν, οι συμμετέχοντες αναγνωρίζουν τον κίνδυνο πρόσβασης από πολλές συσκευές, κίνδυνος που μπορεί να οφείλεται από κλοπή συσκευής μέχρι κακόβουλο λογισμικό ή phishing.

Στη συνέχεια βλέπουμε με ενδιαφέρον ότι ένα 40% έχει διακόψει ηλεκτρονική υπηρεσία λόγω υποψίας ή γεγονότος παραβίασης ασφαλείας. Παρόλο το μεγάλο ποσοστό γνώσης με τους κινδύνους ένα 58% αλλάζει τον κωδικό πρόσβασης μόνο όταν προταθεί από την εκάστοτε ηλεκτρονική υπηρεσία ή ακόμα και ποτέ. Σαν φυσική συνέχεια των μέχρι τώρα απαντήσεων βλέπουμε ότι μόνο το 36% είναι σίγουρο ότι δεν έχει προσβληθεί από ιό ή άλλο κακόβουλο λογισμικό συσκευή τους ενώ το 57% είναι σίγουρο και το 7% δεν γνωρίζει καθόλου. Μετά από τις απαντήσεις στα προηγούμενα ερωτήματα οι συμμετέχοντες σε ποσοστό 78% συμφωνούν ότι θα προτιμούσαν ένα επιπλέον επίπεδο ασφάλειας πέρα από το κωδικό πρόσβασης και στην επόμενη το 73% πιστεύουν ότι τα βιομετρικά θα μπορούσε να είναι ένας τέτοιος τρόπος αφού πιστεύουν ότι το βελτιώνουν. Συνεχίζουμε ρωτώντας αν τα keystroke dynamics θα μπορούσαν να είναι ένας τέτοιος πρόσθετος τρόπος και εδώ έχουμε το ενδιαφέρον στοιχείο του να απαντούν θετικά το 35%, (θυμίζουμε ότι το γνώριζαν μόνο 16%), ενώ 46% δηλώνουν ότι δεν το γνωρίζουν ως βιομετρικό τρόπο και 19% δεν πιστεύουν ότι θα βελτίωνε ως μέτρο ασφάλειας. Συνεχίζοντας βλέπουμε ότι μόνο ένα 15% δεν είναι επιφυλακτικό απέναντι στη χρήση των βιομετρικών

κύρια λόγω ενδεχόμενης κακής χρήσης, στοιχείο σημαντικό που επηρεάζει ιδιαίτερα τα φυσιολογικά βιομετρικά ως μόνιμα. Ως φιλικότερο στη χρήση βλέπουμε τα δακτυλικά αποτυπώματα και αυτό μάλλον είναι λόγω της συνήθειας και της γνώσης του κόσμου σε αυτά αλλά και λόγω της υποσυνείδητης χρήσης τους από κρατικές αρχές με μεγάλο δείκτη αξιοπιστίας (αστυνομία). Βλέπουμε όμως με ενδιαφέρον μια τάση του κοινού προς τη φιλικότητα των συμπεριφορικών βιομετρικών σε αντίθεση με τα φυσιολογικά (υπογραφή 25%, keystroke 27%, φωνή 24%) που πάλι μας οδηγεί ότι με ενημέρωση του κοινού πάνω σε αυτές τις μεθόδους τα αποτελέσματα θα βελτιωθούν περαιτέρω. Στις επόμενες δυο ερωτήσεις θέλουμε να μάθουμε πόσο αποδοχή έχουν γενικά οι τεχνολογίες βιομετρικών στον έλεγχο πρόσβασης και βλέπουμε ότι υπάρχει μεγάλο περιθώριο από την αρχική δυσπιστία στην αρχή του ερωτηματολογίου αφού οι απαντήσεις είναι σχεδόν μοιρασμένες και όπως φαίνεται στην τελευταία τελικά μόνο το 30% πιστεύει ότι η έλευση νέων τεχνολογιών όπως τα βιομετρικά δεν θα βελτιώσει την ασφάλεια των ηλεκτρονικών υπηρεσιών.

Συνεχίζουμε την ανάλυση των ευρημάτων **στο πείραμα** όπου μετά από τη συλλογή των χρόνων **hold time** και **digraph** των 12 συμμετεχόντων μετά την εισαγωγή του κωδικού ‘try4-mbs’ αποθηκεύσαμε τις τρεις τελευταίες εγγραφές μετά την δοκιμαστική εισαγωγή εξοικείωσης που επαναλήφθηκε για 15 φορές αφού είδαμε ότι είχαμε μηδενικά σφάλματα εισαγωγής του κωδικού και άρα ήταν αρκετός ο αριθμός αυτών των επαναλήψεων. Σε αυτές τις τρεις μετρήσεις υπολογίστηκε ο μέσος όρος, και στις δυο παραμέτρους μετρήσεων και φτιάχτηκε πίνακας και διαγράμματα σύγκρισης. Ο μέσος όρος χρησιμοποιήθηκε και στην έρευνα που έγινε χρήση ο κωδικός που χρησιμοποιούμε και εμείς [Loy 2005] ως μέθοδος ταξινόμησης των αποτελεσμάτων μαζί με άλλα στατιστικά χαρακτηριστικά, αλλά το βασικότερο είναι πως θα μπορέσουμε να ορίσουμε το κατώφλι ή τα όρια που θα επιτρέπουμε στο νόμιμο χρήστη την είσοδο. Οι ερευνητές **[21], [23]** χρησιμοποίησαν τον ακόλουθο τύπο για αυτή τη σύγκριση,

$$\left|\frac{reference\ feature - test\ feature}{reference\ feature}\right| \times 100\% \leq threshold$$

Τύπος 7, τύπος σύγκρισης εισαγωγής για θετικό ή αρνητικό αποτέλεσμα [23]

Το κατώφλι ορίζεται ανάλογα με την περίσταση και την εφαρμογή και όπως είδαμε το υπολογίζουμε ανάλογα με το πόσο FAR και FRR απαιτούμε κατά περίσταση.

Συνεχίζοντας να θυμηθούμε ότι ο μέσος όρος είναι το άθροισμα των μετρήσεων δια του πλήθους τους. Εδώ να πούμε ότι στόχος λόγω και των περιορισμών των συνθηκών αυτής της έρευνας είναι να διαφανεί η χρησιμότητα των keystroke dynamics δηλαδή **να αποδειχτεί** ότι όντως ο ρυθμός της πληκτρολόγησης είναι διαφορετικός ανά άνθρωπο τουλάχιστον στο αρχικό στάδιο χρήσης ενός νέου κωδικού. Ας δούμε το γράφημα με τους μέσους όρους των **hold time** των χαρακτήρων του κωδικού των 12 χρηστών λοιπόν,

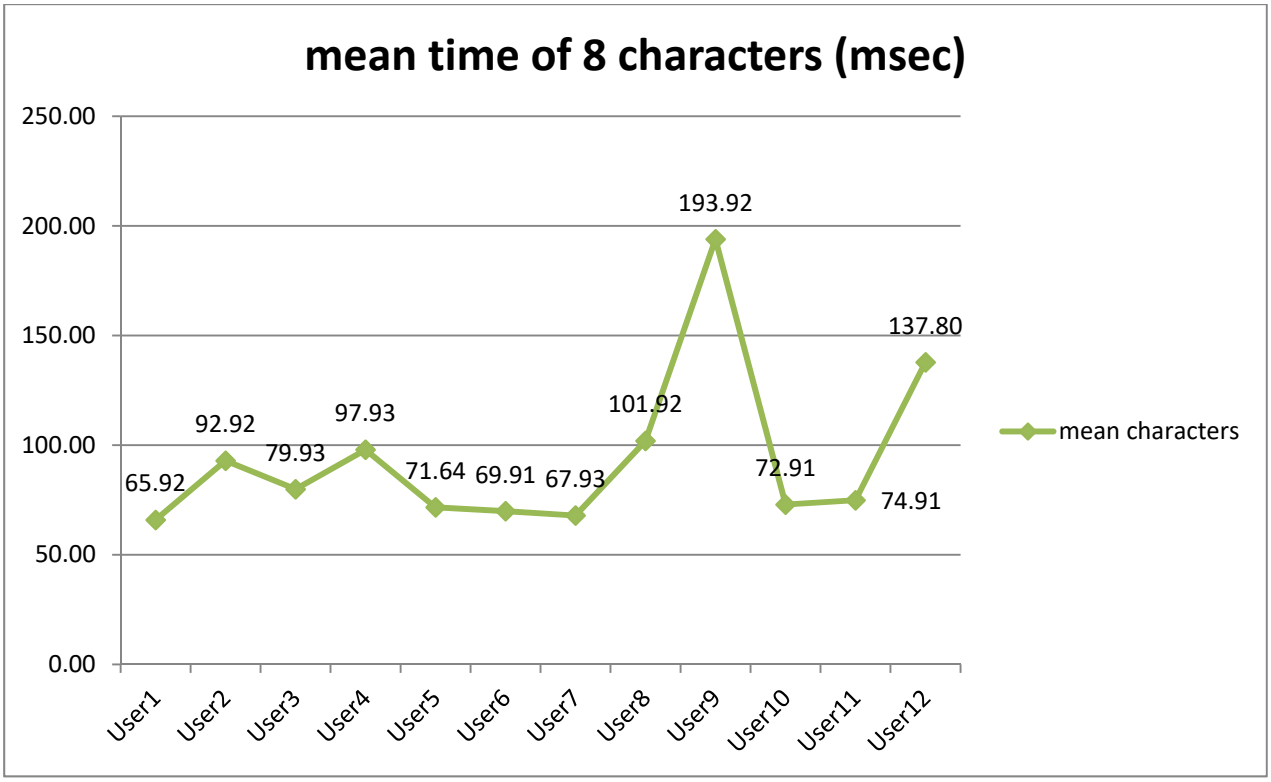
Χαρακτήρας	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms
	User1	**User2**	**User3**	**User4**	**User5**	**User6**	**User7**	**User8**	**User9**	**User10**	**User11**	**User12**
t	63,89	103,87	87,97	111,97	79,88	71,89	63,9	127,89	159,88	87,89	63,83	151,08
r	63,93	87,96	79,88	103,94	63,95	55,91	71,93	119,97	159,93	55,94	79,95	143,89
y	55,91	95,91	95,94	79,93	71,89	79,9	63,97	87,92	207,97	71,92	63,88	175,85
4	63,94	63,92	79,93	95,9	85,83	87,9	63,91	95,92	215,94	71,93	87,94	135,9
_	71,9	87,91	79,92	103,96	55,88	71,92	63,91	79,9	255,9	71,9	71,89	135,87
m	71,92	119,93	71,92	87,89	63,89	47,93	63,95	111,91	183,92	79,93	79,92	143,92
b	71,93	103,92	71,95	87,92	55,91	79,92	71,92	95,94	199,91	79,88	79,9	87,94
s	63,9	79,9	71,91	111,95	95,9	63,87	79,92	95,92	167,93	63,9	71,93	127,93

Πίνακας 3, μέσος όρος των χρόνων hold time των χρηστών

Και οι αντίστοιχοι μέσοι όροι ανά χρήστη,

User1	**User2**	**User3**	**User4**	**User5**	**User6**	**User7**	**User8**	**User9**	**User10**	**User11**	**User12**
65,92	92,92	79,93	97,93	71,64	69,91	67,93	101,92	193,92	72,91	74,91	137,80

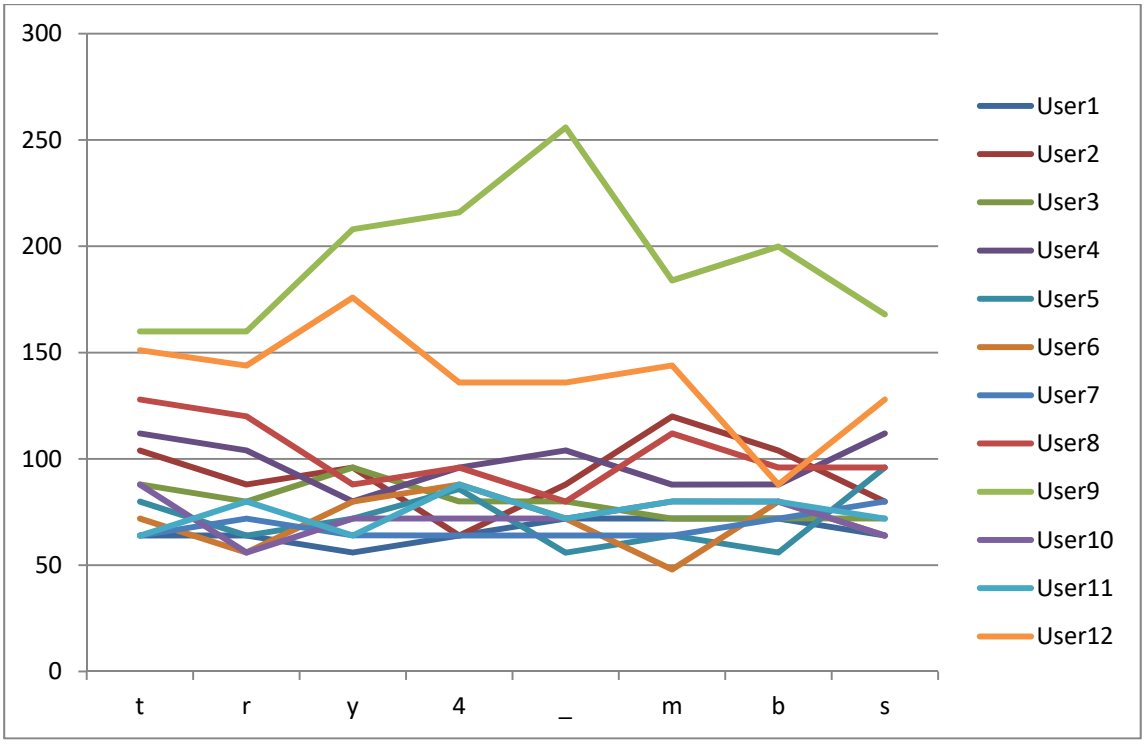
Το οποίο μας δίνει το εξής γράφημα με τους μέσους όρους των χαρακτήρων των 12 χρηστών,



Γράφημα 7, Ο μέσος όρος συνολικά των χαρακτήρων του κωδικού των12 χρηστών

Βλέπουμε με ενδιαφέρον ότι έχουμε διαφορές ανά χρήστη αλλά αν πάρουμε ένα εύρος τιμών από 67-72 msec βλέπουμε ότι οι χρήστες 5,6,7 έχουν κοντινές τιμές.

Ας θυμηθούμε τις διαφορές που είχαν μεταξύ τους ανά χαρακτήρα και όχι κατά τον μέσο όρο όλων των χαρακτήρων του κωδικού,



Γράφημα 8, μέσοι όροι των hold times των 12 χρηστών

Βλέπουμε ότι έχουμε συγκέντρωση των τιμών σε αρκετούς χρήστες που σημαίνει ότι πράγματι με τη χρήση του μέσου όρου του συνόλου χαρακτήρων ανά χρήστη έχουμε πιο ξεκάθαρη εικόνα όπως είδαμε παραπάνω.

Ας δούμε τώρα τις μέσες τιμές των digraph τους ανά χρήστη για να δούμε αν έχουμε κάποιο ενδιαφέρον εύρημα

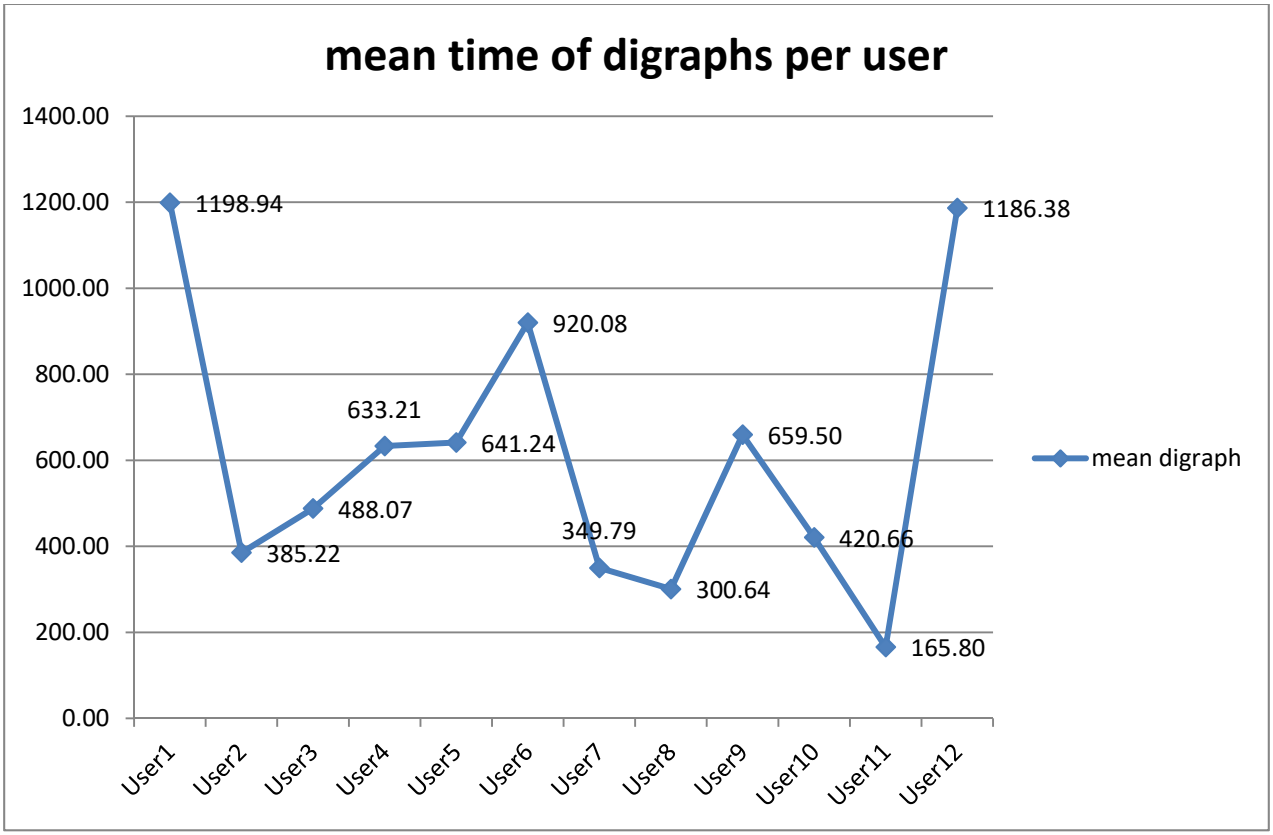
	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms	Χρόνος ms
digraph	**User1**	**User2**	**User3**	**User4**	**User5**	**User6**	**User7**	**User8**	**User9**	**User10**	**User11**	**User12**
(t, r):	360,07	128,04	120,07	304,03	168,06	488,08	128,06	232,03	248,06	120,05	104,07	592,09
(r, y):	464,08	424,08	424,07	776,04	344,08	1264,08	136,08	240,07	368,09	232,09	152,08	552,14
(y, 4):	1816,07	808,08	448,07	848,12	1088,09	1528,08	488,1	272,08	728,07	768,07	240,08	1032,11
(4, -):	1432,07	488,1	736,1	800,07	744,11	792,07	264,08	520,1	1232,07	704,1	224,09	3664,09
(-, m):	2424,08	416,07	656,08	928,08	1144,1	776,07	376,1	336,09	1088,07	344,05	224,11	1648,09
(m, b):	824,09	192,06	616,05	328,05	520,09	736,06	184,05	264,07	416,07	424,12	208,08	160,04
(b, s):	1072,09	240,1	416,04	448,07	480,12	856,13	872,06	240,06	536,08	352,11	8,07	656,09

Πίνακας 4, μέσος όρος των digraph ανά χρήστη

Και οι μέσοι όροι τους

User1	User2	User3	User4	User5	User6	User7	User8	User9	User10	User11	User12
1198,94	385,22	488,07	633,21	641,24	920,08	349,79	300,64	659,50	420,66	165,80	1186,38

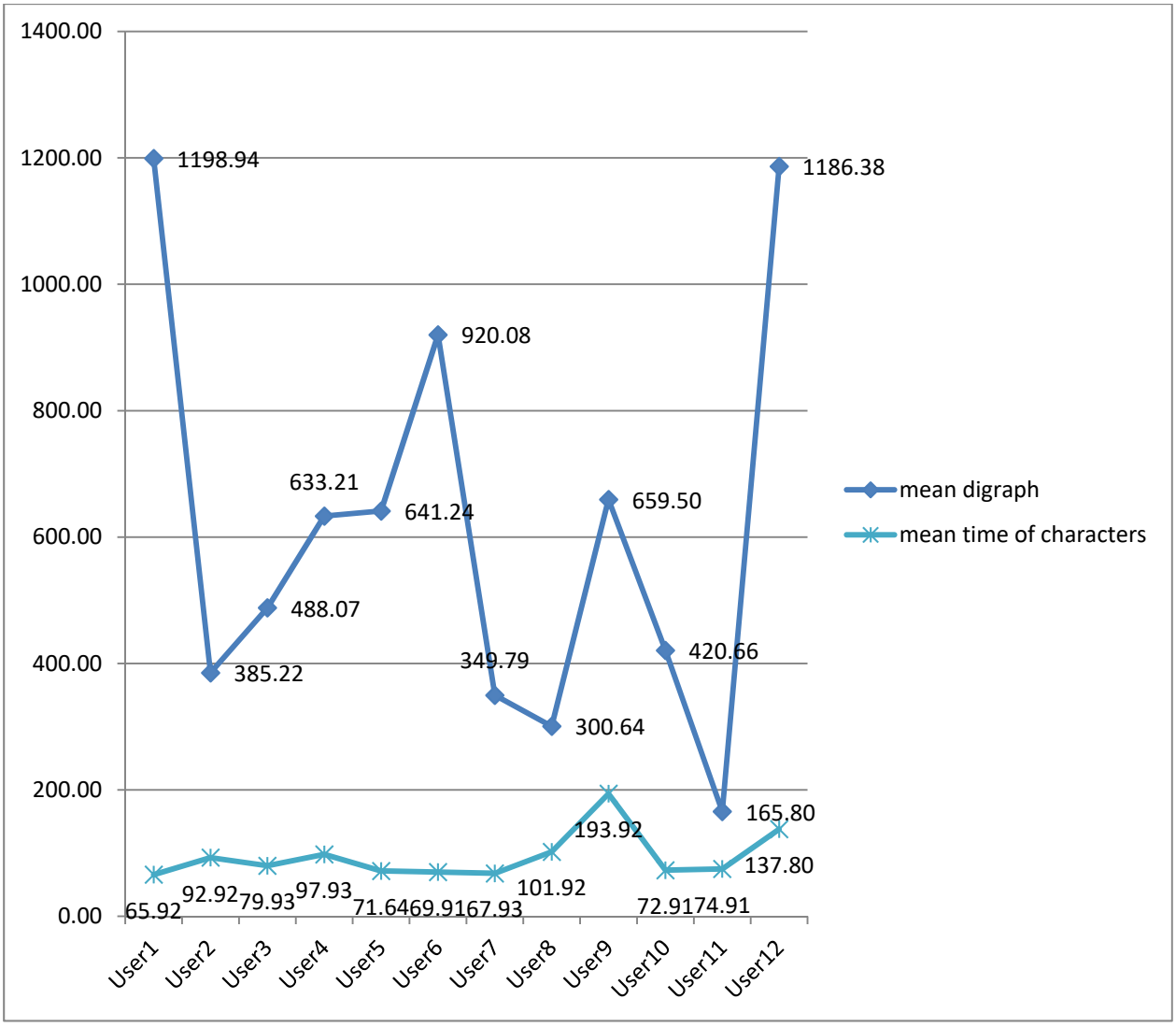
Και με το αντίστοιχο γράφημα με την απεικόνιση των τιμών αυτών των μέσων όρων των digraph ανά χρήστη,



Γράφημα 9, μέσοι όροι digraph ανά χρήστη

Εδώ πλέον ξεκαθαρίζει αρκετά το τοπίο δηλαδή μπορούμε να πούμε ότι με τον υπολογισμό των μέσων όρων των digraphs έχουμε συμπληρωματικό έλεγχο που σε συνδυασμό με το hold time μας ξεχωρίζει αρκετά τη συμπεριφορά του ρυθμού της πληκτρολόγησης ανά χρήστη.

Ας παραθέσουμε τα δυο γραφήματα μαζί των μέσων όρων hold time και digraph των πληκτρολογήσεων κάθε χρήστη,



Γράφημα 10, παράθεση των μέσων όρων hold time και digraph ανά χρήστη (Γραφήματα 7 και 9)

Βλέπουμε σε μεγαλύτερη κλίμακα πόσο σημαντικά ευρήματα έχουμε με την χρήση των digraphs. Πράγματι έχουμε ξεκάθαρες διαφοροποιήσεις ανά χρήστη, και βέβαια μπορούμε να χρησιμοποιήσουμε ταυτόχρονα δυο ή και περισσότερες παραμέτρους ελέγχου για να ταυτοποιήσουμε τον νόμιμο χρήστη. Υποθέτουμε ότι με χρήση ελέγχου παραπάνω συνδυασμών χαρακτήρων όπως trigraph ή και n-graph θα μας εμπλουτίζει και άλλο τη δεξαμενή ελέγχου. Για να συνοψίσουμε, έχουμε δει ότι με σύλληψη των χρόνων hold timeκαι digraph, έχουμε κάνει τις συγκρίσεις των μέσων όρων ανά χαρακτήρα του κάθε χρήστη αλλά και του digraph, και επίσης τώρα έχουμε κάνει σύγκριση των μέσων όρων των χρόνων όλων των χαρακτήρων και όλων των digraph ανά χρήστη, άρα έχουμε ήδη

τέσσερα στοιχεία σύγκρισης που μας έχουν δείξει την ουσιαστική διαφοροποίηση των χρόνων του ρυθμού της πληκτρολόγησης ανά χρήστη.

Είδαμε ήδη τα δυο rates το FAR και το FRR και συγκεκριμένα ότι ανάλογα με την περίσταση που θα χρησιμοποιήσουμε το σύστημα αναγνώρισης keystroke dynamic ότι γενικά υψηλότερες τιμές FAR είναι αποδεκτές σε εφαρμογές με όχι υψηλά επίπεδα ασφάλειας ενώ αντίθετα απαιτούμε υψηλό βαθμό FRR σε ευαίσθητες και κρίσιμες εφαρμογές και συστήματα. Είδαμε ήδη μεθόδους διαχωρισμού μέσω των μετρήσεων των μέσον όρων των χαρακτήρων και των διγραμμάτων, αλλά και τον μέσο όρο αυτών ανά χρήστη. Σε περίπτωση εφαρμογής που αποδεχόμαστε το υψηλό FAR μπορούμε να σταματήσουμε με αυτές τις μετρήσεις. Αν όμως έχουμε μια κρίσιμη εφαρμογή και φτάνουμε σε βαθμό ακρίβειας που αποδεχόμαστε υψηλό βαθμό FRR μπορούμε να χρησιμοποιήσουμε και την Ευκλείδεια απόσταση μεταξύ κοντινών μετρήσεων χρηστών για μεγαλύτερο φιλτράρισμα αποτελεσμάτων.

Κεφάλαιο 6

Βιομετρικά και προσωπικά δεδομένα

Τα βιομετρικά δεδομένα των ανθρώπων, η συλλογή, η αποθήκευση και η επεξεργασία τους αποτελεί το κατεξοχήν παράδειγμα της ορθής χρήσης των προσωπικών δεδομένων τους. Από την παγκόσμια διακήρυξη προστασίας των ανθρώπινων δικαιωμάτων του ΟΗΕ προβλέπεται η προστασία των προσωπικών δεδομένων και της προστασίας της ιδιωτικότητας (privacy) του ατόμου. Στην Ευρωπαϊκή Ένωση έχουν δημοσιευτεί δεκάδες Οδηγίες, Νόμοι και Κανονισμοί πάνω σε αυτό το τομέα οι οποίοι ερμηνεύονταν και εφαρμόζονταν με διαφορετικό τρόπο σε κάθε κράτος μέλος. Αυτό οδήγησε στη δημιουργία ενός βελτιωμένου πλαισίου το οποίο έγινε υποχρεωτικό σε όλα τα κράτη μέλη από το Μάιο του 2018, με την ονομασία Γενικός Κανονισμός Προσωπικών Δεδομένων (ΓΚΠΔ) ή στα αγγλικά GDPR. Από εκείνη την ημερομηνία όλη η έρευνα και η εργασία πάνω στα βιομετρικά δεδομένα πρέπει να συμμορφώνεται με το νέο κανονισμό.

6.1 Ο ΓΚΠΔ (GDPR)

Ο ΓΚΠΔ (ΕΕ 2016/679) άρχισε να ισχύει από την 25η Μαΐου του 2018 και αντίθετα με τις Ευρωπαϊκές οδηγίες δεν χρειάζεται ιδιαίτερη νομοθεσία σε κάθε μια χώρα ξεχωριστά αλλά από εκείνη την ημερομηνία έχει τεθεί αυτόματα σε ισχύ **[50].** Το ενδιαφέρον είναι ότι δεν περιορίζεται μόνο σε οργανισμούς εντός της ΕΕ αλλά εφαρμόζεται και σε αυτούς εκτός της ΕΕ, εφόσον παρέχουν ή προσφέρουν αγαθά ή υπηρεσίες σε πολίτες της ΕΕ. Ουσιαστικά εφαρμόζεται σε όλες τις επιχειρήσεις ή ινστιτούτα που κατέχουν ή επεξεργάζονται προσωπικά δεδομένα των πολιτών που διαμένουν στην ΕΕ. Ο ΓΚΠΔ εφαρμόζεται πάνω στα προσωπικά δεδομένα που είναι κάθε είδους πληροφορία ή δεδομένο που

σχετίζεται ή μπορεί να συνδεθεί με κάποιο άτομο και που τον χαρακτηρίζει όπως το ονοματεπώνυμο, η διεύθυνση, το τηλέφωνο, οι φωτογραφίες αλλά και οι ιδέες και οι απόψεις που έχει. Επιπλέον κάποια δεδομένα θεωρούνται ως ευαίσθητα όπως οι θρησκευτικές, πολιτικές πεποιθήσεις ή οι πληροφορίες σχετικά με την κατάσταση της υγείας του ατόμου.

Γύρω από αυτές τις πληροφορίες και δεδομένα που φανταζόμαστε σε τι βάθος υπάρχουν σε εταιρείες, οργανισμούς και διαδικτυακές υπηρεσίες ο ευρωπαίος πολίτης έχει μέσα από τον ΓΚΠΔ συγκεκριμένα δικαιώματα όπως το δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα του, το δικαίωμα αλλαγής και διόρθωσης λανθασμένων δεδομένων, το δικαίωμα περιορισμού της επεξεργασίας των δεδομένων που τον αφορούν, το δικαίωμα εναντίωσης στην επεξεργασία των δεδομένων του, το δικαίωμα στη λήθη δηλαδή το δικαίωμα της διαγραφής των δεδομένων που τον αφορούν και τέλος το δικαίωμα στη φορητότητα των δεδομένων δηλαδή τη δυνατότητα της παροχής των δεδομένων σε αναγνώσιμη μορφή. Επίσης πλέον είναι απαραίτητη από την αρχή η ρητή συγκατάθεση (*consent*) του ατόμου για την συλλογή και επεξεργασία των δεδομένων του παρέχοντας του κάθε δυνατή ενημέρωση και επεξήγηση όπου χρειάζεται ενισχύοντας τη διαφάνεια.

Κάθε οργανισμός που τηρεί αρχείο με προσωπικά δεδομένα είναι υποχρεωμένος να έχει ορίσει υπεύθυνο επεξεργασίας γνωστό με τον όρο Data Protection Officer (DPO) που έχει συγκεκριμένες υποχρεώσεις με γνώμονα την διαφάνεια στη μέθοδο συλλογής των προσωπικών δεδομένων, της επεξεργασίας και της αποθήκευσης τους. Ο DPO είναι υπεύθυνος για την ασφάλεια και την προστασία των δεδομένων, καθώς και για την γνωστοποίηση τυχόν παραβιάσεων. Η εποπτική Αρχή για τον ΓΚΠΔ στην Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

6.2 Βιομετρικά και ΓΚΠΔ

Ας δούμε τώρα τι γίνεται με τα βιομετρικά, την διαχείριση τους και τις αλλαγές μετά την ενεργοποίηση του ΓΚΠΔ. Τα προσωπικά δεδομένα μπορούν να χωριστούν σε κατηγορίες ανάλογα με την σοβαρότητα που απαιτεί η προστασία

τους **[50].** Έχουμε λοιπόν τις πολιτικές απόψεις, τις θρησκευτικές πεποιθήσεις και τις απόψεις σχετικά με τη φυλή, τον σεξουαλικό προσανατολισμό, την ηλικία και άλλα τέτοιου τύπου.

Ειδική κατηγορία είναι όλα τα ιατρικά δεδομένα και άλλη κατηγορία τα διοικητικής φύσης που περιλαμβάνει αριθμούς ταυτότητας, διευθύνσεις, αριθμούς τραπεζικών λογαριασμών. Τα βιομετρικά σύμφωνα με τον GDPR αναγράφονται ως "*special category of personal data*" ειδικής κατηγορίας προσωπικά δεδομένα που απαιτούν ειδική μεταχείριση σύμφωνα με το Άρθρο 9 του κανονισμού. Είδαμε ότι οι μεγάλες αλλαγές που έρχονται με τον νέο κανονισμό είναι το γεγονός ότι αφορά οποιονδήποτε συλλέγει και επεξεργάζεται δεδομένα Ευρωπαίων πολιτών. Με αυτό το κανονισμό δημιουργούνται νέες κατηγορίες προσωπικών δεδομένων. Τα βιομετρικά είναι μια τέτοια ειδική κατηγορία και ως ευαίσθητα προσωπικά δεδομένα πρέπει να διαχειρίζονται με απόλυτα ασφαλές και συγκεκριμένο τρόπο.

Προτάσεις προστασίας είναι η δημιουργία μιας ακόμα μεθόδου προστασίας της ταυτότητας του πολίτη με την χρήση ψευδωνύμου ως αναγνωριστικό. Αυτό είναι ένα ενδιάμεσο μέσο μεταξύ της πραγματικής ταυτότητας του χρήστη των βιομετρικών και της πλήρους ανωνυμίας του. Καθορίζει βασικές αρχές όπως την διαφάνεια των δεδομένων , την αρχική ευθύνη και τον σχεδιασμό πολιτικών σχεδίασης προστασίας των δεδομένων. Εισάγει την υποχρέωση του υπεύθυνου επεξεργασίας προσωπικών δεδομένων ο οποίος είναι και ο υπεύθυνος κατά τον Νόμο. Σε κάθε υπόνοια διαρροής δεδομένων πρέπει να δηλώνεται αμέσως στην Αρχή και στα άτομα που αφορά η διαρροή. Πρέπει να υπάρχει ξεκάθαρη επισήμανση και ενημέρωση των πολιτών για την χρήση, την επεξεργασία, τον τρόπο και τον χρόνο αποθήκευσης των βιομετρικών δεδομένων τους και ξεκάθαρη αποδοχή του πολίτη. Η δυνατότητα ο πολίτης να μπορεί να μάθει τι, πόσα και από ποιους χρησιμοποιούνται τα βιομετρικά του και να μπορεί να ζητά την διακοπή της χρήσης και την καταστροφή των αρχείων με αυτά. Βλέπουμε ότι πλέον υπάρχει αυστηροποίηση του πλαισίου προστασίας του πολίτη από κακή χρήση των προσωπικών δεδομένων του, όπως τα βιομετρικά δεδομένα του.

Καταλαβαίνουμε ήδη από τα προηγούμενα ότι ο τρόπος που ο χρήστης πληκτρολογεί ή αλληλεπιδρά με τον ΗΥ, το ξεκλείδωμα που κάνει στο κινητό

του με τα δακτυλικά αποτυπώματα ή με το πρόσωπο του, δημιουργεί πιθανά κενά από τον όγκο των δεδομένων που συγκεντρώνονται από τις εταιρείες, ή τους οργανισμούς, φτιάχνοντας ένα μοναδικό προφίλ του κατόχου από πολλαπλές πλευρές, όπως τι υπηρεσία χρησιμοποιεί, πως τι χρησιμοποιεί, πότε και γιατί. Επαναλαμβάνουμε ότι ως ειδικής κατηγορίας ο κανονισμός επιτρέπει σε κάθε κράτος μέλος της ΕΕ να επιβάλει επιπρόσθετα μέτρα και περιορισμούς, πράγμα που σημαίνει ότι πρέπει να υπάρχει σφαιρική ενημέρωση γύρω από την νομοθεσία σε επίπεδο κράτους ώστε να αποφευχθούν παραβιάσεις. Τα βιομετρικά συμπεριφοράς είναι στο μικροσκόπιο της ΕΕ για να μελετήσουν κατά πόσο τα πλεονεκτήματα τους είναι σημαντικά περισσότερα από τον κίνδυνο παραβίασης της ιδιωτικότητας και της κακής χρήσης τους όχι μόνο από κακόβουλα λογισμικά και χάκερ αλλά και μεγάλες και γνωστές εταιρείες.

6.3 Ηθικά και νομικά ζητήματα, αντίκτυπος των βιομετρικών

Πέρα από τους κανονισμό ΓΚΠΔ που θέτει περιορισμούς και υποχρεώσεις υπάρχουν και άλλα νομικά αλλά και ηθικά ζητήματα που έχουν συγκεκριμένο αντίκτυπο και στη χρήση των βιομετρικών αλλά και στους ανθρώπους που τα χρησιμοποιούν ή τα διαχειρίζονται. Κλασικό παράδειγμα τη τελευταία δεκαετία που έχουμε την ανάπτυξη των εργαλείων του διαδικτύου με σκοπό την καταγραφή των συνηθειών των χρηστών για να υπάρξει στοχευμένη διαφήμιση ώστε οι εταιρείες να έχουν το ανταγωνιστικό πλεονέκτημα σε σχέση με τους ανταγωνιστές τους. Με την ολοένα μεγαλύτερη εφαρμογή αυτών των πρακτικών η προστασία της ιδιωτικότητας γίνεται ακόμα πιο μεγάλης σημασίας. Πολύ περισσότερο αν αρχίσουν να χρησιμοποιούνται ως μέθοδοι ανίχνευσης και ανάλυσης και τα βιομετρικά στοιχεία μας.

Υπάρχουν συγκεκριμένα ερωτήματα που εγείρονται όπως ποιος συλλέγει τα βιομετρικά στοιχεία μας και συγκεκριμένα το βιομετρικό συμπεριφοράς του ρυθμού της πληκτρολόγησης, και αν αυτός που τα συλλέγει τα διαμοιράζεται με

τρίτες εταιρείες για εμπορική ή άλλη χρήση χωρίς τη συγκατάθεση του ατόμου. Μπορούμε να συνοψίσουμε τους προβληματισμούς των ανθρώπων σχετικά με τα βιομετρικά τους στο ποιος τα συλλέγει, πως τα αποθηκεύει και τα προστατεύει, πως αποτρέπει τη μη εξουσιοδοτημένη χρήση, για πόσο χρόνο τα έχει στη κατοχή του και αν έχει το μηχανισμό που επιβάλει ο ΓΚΠΔ για το δικαίωμα στη λήθη δηλαδή να μπορεί να διαγραφεί εντελώς κάθε βιομετρική πληροφορία μετά από αίτημα του ατόμου. Πρέπει λοιπόν να υπάρχουν ξεκάθαρα οι όροι και οι προϋποθέσεις των συστημάτων βιομετρικών δεδομένων και να υπάρχει απόλυτη εναρμόνιση όχι μόνο με τον ΓΚΠΔ αλλά και με όλες τις κατευθύνσεις και οδηγίες που προτείνονται από τις αρμόδιες αρχές όπως στην Ελλάδα η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Ο αντίκτυπος των βιομετρικών είναι και οικονομικός από την πλευρά των μέτρων ασφαλείας, τα συστήματα συλλογής και η ποιότητα τους αλλά και το επίπεδο διαλειτουργικότητας που έχουν με άλλα συστήματα (πχ αναγνώριση προσώπου με ΑΤΜ τράπεζας). Επίσης η διαμόρφωση καθορισμένων προτύπων (standards) με την εξέλιξη των βιομετρικών όπως το ISO/IEC JTC 1/SC 37 παρέχει και ένα πρόσθετο μέτρο όχι μόνο ασφάλειας αλλά και αύξησης της εμπιστοσύνης των πολιτών. Πάνω από όλα όμως πρέπει να υπάρχει πολύ προσεκτική εφαρμογή των βιομετρικών και για αυτό το λόγο η ΑΠΔΠΧ με τις αποφάσεις της ορίζει κατά πόσο είναι νόμιμη η χρήση των βιομετρικών με βάση την κρισιμότητα της εφαρμογής (πχ εφαρμογή ποιου είδους βιομετρικού σε εγκατάσταση κρίσιμη και ευαίσθητη από πλευρά της ασφάλειας όπως τα αεροδρόμια) και ποια από τα βιομετρικά επιτρέπονται για κάθε χρήση ώστε να υπάρχει η προστασία αυτού του είδους των ευαίσθητων προσωπικών δεδομένων.

Κεφάλαιο 7

Επίλογος

7.1 Αποτίμηση τεχνολογίας keystroke dynamics

Στην παρούσα μεταπτυχιακή εργασία ασχοληθήκαμε με τα βιομετρικά συστήματα ελέγχου πρόσβασης, και ειδικότερα με το βιομετρικό συμπεριφοράς του ρυθμού της πληκτρολόγησης, keystroke dynamics. Σκοπός ήταν να μάθουμε σχετικά με την τεχνολογία αυτού του βιομετρικού, και να δούμε πως μπορεί να λειτουργήσει συνδυαστικά με τους ήδη χρησιμοποιούμενους τρόπους πρόσβασης (username/ password) και να αυξήσει το επίπεδο ασφάλειας αλλά και ποια η γνώση του κοινού πάνω σε αυτό το βιομετρικό συμπεριφοράς. Εδώ να σημειώσουμε πάλι ότι με τη χρήση αυτού του βιομετρικού ουσιαστικά προστατευόμαστε από επιθέσεις brute force, dictionary και rainbow αφού δεν απαιτείται πλέον μόνο η εύρεση του κωδικού αλλά πρέπει να συνδυάζεται και με το σωστό χρονικό παράθυρο των hold times και digraphs για να επιτραπεί η είσοδος στην υπηρεσία.

Επιπρόσθετα έγινε λήψη απαντήσεων σε ερωτηματολόγιο από 100 συμμετέχοντες σχετικά με τα βιομετρικά, τα keystroke dynamics αλλά και ερωτήσεις σχετικά με τη γνώση του κοινού πάνω στην ασφάλεια υπολογιστών και δικτύων. Επίσης πραγματοποιήθηκε πείραμα εισαγωγής κωδικού μέσω ΗΥ από 12 συμμετέχοντες ώστε να διαπιστώσουμε με εργαστηριακό τρόπο την διαφορά των χρόνων hold time και digraph στο αρχικό διάστημα χρήσης ενός νέου κωδικού μήκους 8 χαρακτήρων. Αυτός ο κωδικός έχει ήδη ευρέως χρησιμοποιηθεί από άλλους ερευνητές **[23], [25], [26]** και μπορεί να μας δώσει και συγκριτικά στοιχεία αν και ήταν διαφορετικά τα μεγέθη των συμμετεχόντων, των συνθηκών και των παραμέτρων.

Αυτή η εργασία είναι ένα μέσο πληροφόρησης για τα βιομετρικά ως μέθοδος πρόσβασης και ειδικότερα των keystroke dynamics. Αυτό το βιομετρικό συμπεριφοράς αποτελεί μια λύση με πολύ σοβαρά πλεονεκτήματα όπως την πολύ γρήγορη χρήση συστημάτων two factor authentication, που μπορούν σε ευαίσθητες υπηρεσίες να είναι και σε δυναμική μορφή ώστε να υπάρχει επιπρόσθετη ασφάλεια, χωρίς να απαιτεί ειδικό εξοπλισμό σύλληψης αυτού του βιομετρικού πέρα από ένα κοινό πληκτρολόγιο και χωρίς ακριβά συστήματα που απαιτούν ισχυρή επεξεργαστική ισχύ.

Στο ερωτηματολόγιο λοιπόν φάνηκε ότι παρά το γεγονός ότι το κοινό δεν γνωρίζει σχετικά με το keystroke dynamics (μόνο το 16% το γνώριζε), θα το χρησιμοποιούσε σε μεγάλο βαθμό λόγω της μη επεμβατικότητας (non-intrusive) στην ιδιωτικότητα του και ως πιο φιλικό στη χρήση σε ποσοστό 28% αναδεικνύοντας το δεύτερο μετά από τα δακτυλικά αποτυπώματα σε σύνολο οκτώ διαφορετικών βιομετρικών μεθόδων αναγνώρισης, πράγμα που σημαίνει ότι έχει μεγάλες πιθανότητες και περιθώρια χρήσης ως μέθοδος αναγνώρισης στο μέλλον. Συγκεκριμένα διαφαίνεται όπως ήδη αναφέραμε, άμεσα η εξασφάλιση από επιθέσεις τύπου brute force αλλά και dictionary όπως και rainbow μια που δεν θα απαιτείται μόνο η ανεύρεση των κωδικών αλλά και το χρονικό παράθυρο του keystroke dynamic του συγκεκριμένου χρήστη, πράγμα που κάνει πλέον αυτού του τύπου επιθέσεις πραγματικά ανίσχυρες μια που το όπλο τους είναι η δοκιμή εκατομμύρια διαφορετικών κωδικών το δευτερόλεπτο. Επίσης το keystroke dynamic έχει τη δυνατότητα της συνεχούς ‘εκπαίδευσης’ μέσω της μάθησης του συστήματος πάνω στο τρόπο εισαγωγής του κωδικού του χρήστη στο χρόνο. Άλλο χρόνο έχει τις πρώτες δέκα φορές και άλλες μετά από χίλιες, το οποίο αυτό θα αλλάζει δυναμικά αφαιρώντας την πιο παλαιά με την πιο καινούργια μέτρηση στην βάση δεδομένων του συστήματος του ελέγχου πρόσβασης επικαιροποιώντας την, με τους νέους χρόνους.

Τέλος να πούμε το ιδιαίτερο πλεονέκτημα των βιομετρικών συμπεριφοράς σε σχέση με τα φυσιολογικά, είναι το γεγονός, ότι τα δεύτερα σε περίπτωση κλοπής δεν μπορούν να αλλάξουν και πλέον είναι επισφαλής η χρήση τους και άρα **αχρηστεύονται**, σε αντίθεση με τα συμπεριφορικά τα οποία όπως είδαμε στο πείραμα, αν κλαπούν οι χρόνοι θα πρέπει να αντιγράφεται σε μεγάλη ακρίβεια ο

τρόπος πληκτρολόγησης του νόμιμου από τον κακόβουλο για να μπορέσουν να χρησιμοποιηθούν και όχι απλά από ένα μηχάνημα όπως ΗΥ. Ο λόγος είναι στο δεύτερο στοιχείο που είδαμε τα διγράμματα (digraphs) τα χρονικά διαστήματα είναι διαφορετικά σε σχέση με το πάτημα ενός πλήκτρου σε χρόνο. Εκεί ο ερευνητής μπορεί να προσθέσει ακόμα ένα ώστε να έχουμε χρόνους των τριγραμμάτων (trigraph) ή και άλλους συνδυασμούς σε κομμάτια του κωδικού (πχ στο δικό μας κωδικό `'try4-mbs'` να υπολόγιζε επιπρόσθετα το ρυθμό στο κομμάτι `'4-mb'`). Και βέβαια τελειώνοντας αφήνουμε την πολύ απλή λύση αντίδρασης σε ενδεχόμενο κινδύνου, την αλλαγή του κωδικού που πλέον θα συνοδεύεται με νέο pattern του ρυθμού πληκτρολόγησης και εντελώς άλλο keystroke dynamic βιομετρικό κάνοντας τον νέο κωδικό πάλι πολύ ισχυρό σε επιθέσεις των τύπων που γνωρίζουμε.

7.2 Ανοικτά ερευνητικά ερωτήματα και θέματα

Είδαμε σε αυτή την εργασία πληροφορίες και θεωρία σχετικά με το βιομετρικό συμπεριφοράς του ρυθμού της πληκτρολόγησης (keystroke dynamics). Ταυτόχρονα εκτελέσαμε πείραμα ώστε να διαφανεί η χρησιμότητα και η αξιοπιστία του ως τεχνικής two factor authentication για έλεγχο της πρόσβασης με το ελάχιστο κόστος από πλευράς εξοπλισμού αφού το μόνο που απαιτείται είναι ένα πληκτρολόγιο. Αυτό συνδυάστηκε με τις απαντήσεις 100 ατόμων από διαδικτυακό ερωτηματολόγιο ώστε να εξετάσουμε κατά πόσο είναι αποδεκτό το βιομετρικό της συμπεριφοράς keystroke dynamics από τους χρήστες ευρύτερου εκπαιδευτικού και ηλικιακού εύρους. Ταυτόχρονα όμως ανοίχτηκαν και κάποια νέα θέματα αλλά και ερευνητικά ερωτήματα. Ένα σημαντικό θέμα προς περαιτέρω έρευνα είναι η χρήση όχι μόνο ενός βιομετρικού κατά τον χρόνο εισόδου αλλά δυο ή και περισσότερα ανάλογα με την σπουδαιότητα και κρισιμότητα της εφαρμογής, τα λεγόμενα **multimodal biometrics**. Με αυτή τη μέθοδο σε περίπτωση που έχουμε κάνει είσοδο σε web banking και πέρα από το κωδικό και το βιομετρικό συμπεριφοράς για την περιήγηση σε περίπτωση που θέλουμε να εκτελέσουμε μια πληρωμή θα απαιτεί για παράδειγμα και ένα βιομετρικό φυσιολογικό όπως τα δακτυλικά αποτυπώματα για να ολοκληρώσει

μια κρίσιμη λειτουργία. Σε τι μας βοηθάει αυτό; Σε περίπτωση που δεν έχουμε διαθέσιμο το κινητό μας για αποστολή του κωδικού επιβεβαίωσης sms μπορούμε να προχωρήσουμε κανονικά.

Ένα ακόμα πεδίο εξαιρετικά ενδιαφέρον **[8]** είναι η χρήση όχι μόνο του στατικού (static) βιομετρικού δηλαδή μόνο κατά την εισαγωγή του κωδικού αλλά και δυναμικά (dynamic) δηλαδή τον συνεχή εντοπισμό του ρυθμού πληκτρολόγησης πάνω στο hold time των πλήκτρων αλλά και των digraphs ώστε να έχουμε δυναμική παρακολούθηση του ατόμου που εκτελεί την λειτουργία σε όλη τη διάρκεια αυτής. Απόρροια αυτού του χαρακτηριστικού της δυναμικής παρακολούθησης του keystroke dynamics είναι το πολύ σημαντικό πεδίο της καταγραφής της ιατρικής κατάστασης ενός ηλικιωμένου με μόνο στοιχείο την συγγραφή ενός μηνύματος ηλεκτρονικού ταχυδρομείου. Θα μπορεί δηλαδή να αντιλαμβάνεται πιθανά το σύστημα την νοητική ή τη σωματική κατάσταση του ατόμου από τον τρόπο και τον ρυθμό που επικοινωνεί με τα παιδιά του στέλνοντας μόνο τα στατιστικά και όχι το περιεχόμενο του μηνύματος στον γιατρό του για έλεγχο ή αντιπαραβολή με τα συνήθη στατιστικά. Δηλαδή μπορούμε να πούμε ότι με την μέθοδο του **liveness detection** θα μπορούμε να παρακολουθούμε και να εντοπίζουμε περιπτώσεις άνοιας αλλά και μαθησιακών δυσκολιών.

Τέλος ένα πολύ σημαντικό πεδίο έρευνας πάνω στα keystroke dynamics είναι η δίγλωσση γραφή, δηλαδή η καταγραφή όχι μόνο στα αγγλικά αλλά και στο ρυθμό της πληκτρολόγησης σε ελληνικά όπου εκεί υπάρχει κενό στη βιβλιογραφία.

Βιβλιογραφία

[1] N. Ahmad, A. Szymkowiak, and P. A. Campbell, "Keystroke dynamics in the pre-touchscreen era," *Frontiers in Human Neuroscience*, vol. 7, 2013.

[2] I. Alsaadi, "Physiological Biometric Authentication Systems, Advantages, Disadvantages and Future Development: A Review," *IJSTR*, vol. 4, no. 12, 2015.

[3] Ananya and S. Singh, "Keystroke Dynamics for Continuous Authentication," in *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2018, pp. 205–208.

[4] M. Antal, L. Z. Szabó, and I. László, "Keystroke Dynamics on Android Platform," *Procedia Technology*, vol. 19, pp. 820–826, 2015.

[5] T. Anusas-amornkul and K. Wangsuk, "A comparison of keystroke dynamics techniques for user authentication," in *2015 International Computer Science and Engineering Conference (ICSEC)*, Chiang Mai, Thailand, 2015, pp. 1–5.

[6] K. O. Bailey, J. S. Okolica, and G. L. Peterson, "User identification and authentication using multi-modal behavioral biometrics," *Computers & Security*, vol. 43, pp. 77–89, Jun. 2014.

[7] D. Bala, "Biometrics and information security," in *Proceedings of the 5th annual conference on Information security curriculum development - InfoSecCD '08*, Kennesaw, Georgia, 2008, p. 64.

[8] S. P. Banerjee and D. Woodard, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey," *Journal of Pattern Recognition Research*, vol. 7, no. 1, pp. 116–139, 2012.

[9] D. Benini, "Improving Biometric Search Performance with Intramodal Fusion," Available at https://www.aware.com/blog-improving-biometric-search-performance-intramodal-fusion/ *Aware*.

[10] S. Bhatt and T. Santhanam, "Keystroke dynamics for biometric authentication; A survey," in *2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering*, Salem, 2013, pp. 17–23.

[11] D. Bhattacharyya, R. Ranjan, P. Das, T. Kim, and S. K. Bandyopadhyay, "Biometric Authentication Techniques and its Future Possibilities," in *2009*

Second International Conference on Computer and Electrical Engineering, Dubai, UAE, 2009, pp. 652–655.

[12] Y. S. Can and F. Alagoz, "User identification using Keystroke Dynamics," in *2014 22nd Signal Processing and Communications Applications Conference (SIU)*, Trabzon, Turkey, 2014, pp. 1083–1085.

[13] J. W. Creswell and C. N. Poth, *Qualitative inquiry & research design: choosing among five approaches*, Fourth edition. Los Angeles: SAGE, 2018.

[14] U.S. DHS, "Biometrics." *US Department of Homeland Security,* nd. Available at https://www.dhs.gov/biometrics/

[15] R. Giot, B. Dorizzi, and C. Rosenberger, "A review on the public benchmark databases for static keystroke dynamics," *Computers & Security*, vol. 55, pp. 46–61, Nov. 2015.

[16] O. HENNIGER, *Encyclopedia of Biometrics: I - Z, Signature Recognition*, vol. 2.

[17] R. Joshi, "Adaptive Fingerprint Image Enhancement for Low-Quality of Images by Learning from the Images and Features Extraction," *IJSHRE*, vol. 2, no. 5, pp. 139–143, 2014.

[18] M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Applied Soft Computing*, vol. 11, no. 2, pp. 1565–1573, Mar. 2011.

[19] S. K. Katsikas, D. A. Gkritzalēs, and S. Gkritzalēs, *Ασφάλεια πληροφοριακών συστημάτων*. Athēna: Ekdoseis Neōn Technologiōn, 2004.

[20] K. S. Killourhy and R. A. Maxion, "Comparing anomaly-detection algorithms for keystroke dynamics," in *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, Lisbon, Portugal, 2009, pp. 125–134.

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

[22] E. A. Kochegurova, E. S. Gorokhova, and A. I. Mozgaleva, "Development of the Keystroke Dynamics Recognition System," *Journal of Physics: Conference Series*, vol. 803, p. 012073, Jan. 2017.

[23] C. C. Loy, "Pressure-Based Typing Biometrics User Authentication Using the Fuzzy ARTMAP Neural Network.," presented at the International

Conference on Neural Information Processing (ICONIP), 2005.

[24] V. Matyáš and Z. Říha, "Biometric Authentication — Security and Usability," in *Advanced Communications and Multimedia Security*, vol. 100, B. Jerman-Blažič and T. Klobučar, Eds. Boston, MA: Springer US, 2002, pp. 227–239.

[25] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Generation Computer Systems*, vol. 16, no. 4, pp. 351–359, Feb. 2000.

[26] J. Montalvão, E. O. Freire, M. A. Bezerra Jr., and R. Garcia, "Contributions to empirical analysis of keystroke dynamics in passwords," *Pattern Recognition Letters*, vol. 52, pp. 80–86, Jan. 2015.

[27] A. F. M. N. H. Nahin, J. M. Alam, H. Mahmud, and K. Hasan, "Identifying emotion by keystroke dynamics and text pattern analysis," *Behaviour & Information Technology*, vol. 33, no. 9, pp. 987–996, Sep. 2014.

[28] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[29] A. Peacock, Xian Ke, and M. Wilkerson, "Typing patterns: a key to user identification," *IEEE Security & Privacy Magazine*, vol. 2, no. 5, pp. 40–47, Sep. 2004.

[30] J. Pfost, "The science behind keystroke dynamics" *Biometric Technology Today*, vol. 15, no. 2, p. 7, Feb. 2007.

[31] P. H. Pisani and A. C. Lorena, "Emphasizing typing signature in keystroke dynamics using immune algorithms," *Applied Soft Computing*, vol. 34, pp. 178–193, Sep. 2015.

[32] Qinghan Xiao, "Security issues in biometric authentication," in *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005.*, West Point, NY, USA, 2005, pp. 8–13.

[33] C. Roberts, "Biometric attack vectors and defences," *Computers & Security*, vol. 26, no. 1, pp. 14–25, Feb. 2007.

[34] R. Roštár and J. Olejár, "Keystroke Dynamics Based User Authentication Using Neural Networks," in *Artificial Neural Nets and Genetic Algorithms*, Vienna: Springer Vienna, 1995, pp. 194–197.

[35] R. Saini and N. Rana, "Comparison of various biometric methods" in

International Journal of Advances in Science and Technology, 2014, vol. 2.

[36] C. Senk and F. Dotzler, "Biometric authentication as a service for enterprise identity management deployment: a data protection perspective," in *2011 Sixth International Conference on Availability, Reliability and Security*, Vienna, 2011, pp. 43–50.

[37] D. Shanmugapriya and G. Padmavathi}, "A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges," *CoRR*, vol. abs/0910.0817, 2009.

[38] D. P. Sidlauskas and S. Tamer, "Hand Geometry Recognition," in *Handbook of Biometrics*, A. K. Jain, P. Flynn, and A. A. Ross, Eds. Boston, MA: Springer US, 2008, pp. 91–107.

[39] R. SINGEL, "Hey, don't tampa with my privacy," *Wired*, 28-Jan-2010.

[40] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and P. Bours, "Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords," *Computers & Security*, vol. 45, pp. 147–155, Sep. 2014.

[41] P. S. Teh, A. B. J. Teoh, C. Tee, and T. S. Ong, "Keystroke dynamics in password authentication enhancement," *Expert Systems with Applications*, vol. 37, no. 12, pp. 8618–8627, Dec. 2010.

[42] H. C. A. van Tilborg and S. Jajodia, Eds., *Encyclopedia of cryptography and security*, 2nd ed. New York: Springer, 2011.

[43] I. Tsimperidis, A. Arampatzis, and A. Karakos, "Keystroke dynamics features for gender recognition," *Digital Investigation*, vol. 24, pp. 4–10, Mar. 2018.

[44] Y. Wang, *Statistical techniques for network security: modern statistically-based intrusion detection and protection*. Hershey: Information Science Reference, 2009.

[45] Wikipedia, "*Biometrics*," 2019, [Online] Available: https://en.wikipedia.org/wiki/Biometrics [Accessed: Jan. 12, 2019].

[46] Wikipedia, "*Fingerprint*," 2019, [Online] Available: https://en.wikipedia.org/wiki/Fingerprint [Accessed: Jan. 15, 2019].

[47] R. V. Yampolskiy, "Mimicry Attack on Strategy-Based Behavioral Biometric," in *Fifth International Conference on Information Technology: New Generations (itng 2008)*, Las Vegas, NV, USA, 2008, pp. 916–921.

[48] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and

classification," *International Journal of Biometrics*, vol. 1, no. 1, p. 81, 2008.

[49] Ztackoverflow, "*Can I get the amount of time for which a key is pressed on a keyboard*", 2010, [Online], Available at: https://stackanswers.net/questions/can-i-get-the-amount-of-time-for-which-a-key-is-pressed-on-a-keyboard [Accessed: Dec. 5, 2018].

[50] R. Zanchez-Reillo, I. Ortega-Fernandez, W. Ponce-Hernandez, and H. C. Quiros-Sandoval, "How to implement EU data protection regulation for R&D in biometrics," *Computer Standards & Interfaces*, vol. 61, pp. 89–96, Jan. 2019.

[51] R. Zewail, A. Elsafi, M. Saeb, and N. Hamdy, "Soft and hard biometrics fusion for improved identity verification," in *The 2004 47th Midwest Symposium on Circuits and Systems, 2004. MWSCAS '04.*, Hiroshima, Japan, 2004, vol. 1, pp. 1_225-1_228.

Παράρτημα Α

Κώδικας πειράματος σε Python 2.7

```
import sys
from collections import defaultdict
import pygame
from pygame.key import name as keyname
from pygame.locals import *
from time import time
from datetime import datetime
datetime.now()
datetime(2009, 1, 6, 15, 8, 24, 78915)
print(datetime.now()) #edo mpainei to timestamp
print ('USER_A,B,C,D') # edo vazo to onoma tou xristi prin to peirama

dwell = defaultdict(list)
digramma = defaultdict(list)
anamoni = {}
last_key = None
typed_text = [[]]
def xronoi():
    all_text = [k for line in typed_text for k in line]
    print "dwell:"
    for key in all_text:
        print "%s: %.5f" % (key, dwell[key].pop(0))
    print "digramma:"
    for key1, key2 in zip(all_text, all_text[1:]):
        print "(%s, %s): %.5f" % (key1, key2,
                                  digramma[(key1, key2)].pop(0))
def xronoi_dwell(events):
    global last_key
    for event in events:
        if event.type == KEYDOWN:
            if event.key == K_ESCAPE:
                xronoi()
                sys.exit(0)
            t = anamoni[event.key] = time()
            if last_key is not None:
                if event.key != K_RETURN:
                    digramma[(last_key[0], keyname(event.key))].append(t
- last_key[1])
                last_key = None
        elif event.type == KEYUP:
            if event.key == K_RETURN:
                refresh_othonis()
                typed_text.append([])
                anamoni.pop(event.key)
                last_key = None
            else:
                t = time()
                dwell[keyname(event.key)].append(t -
anamoni.pop(event.key))
                last_key = [keyname(event.key), t]
                typed_text[-1].append(keyname(event.key))
def refresh_othonis():
    global screen
    screen.fill((255, 255, 255))
```

```
    header_font = pygame.font.Font(None, 22)
    header = header_font.render("Tora pliktrologiste ton kodiko 'try4-
mbs' , kai patiste ENTER gia na ton deite", True, (0, 0, 0))
    header_rect = header.get_rect()
    header_rect.centerx = screen.get_rect().centerx
    header_rect.centery = screen.get_rect().centery - 100

    text_font = pygame.font.Font(None, 32)
    user_text = text_font.render("".join(typed_text[-1]) if typed_text[-
1] else "...",
                                 True, (0, 0, 255))
    text_rect = user_text.get_rect()
    text_rect.centerx = screen.get_rect().centerx
    text_rect.centery = screen.get_rect().centery

    screen.blit(header, header_rect)
    screen.blit(user_text, text_rect)

    pygame.display.update()
if __name__ == '__main__':
    pygame.init()
    window = pygame.display.set_mode((1024, 768))
    screen = pygame.display.get_surface()
    refresh_othonis()
    while True:
        xronoi_dwell(pygame.event.get())
```

Παράρτημα Β

Ερωτηματολόγιο έρευνας

ΤΙΤΛΟΣ Ερωτηματολογίου
Εξελίξεις στις τεχνολογίες βιομετρικών , μελέτη και αξιολόγηση ελέγχου πρόσβασης με χρήση behavioral biometrics

Αγαπητοί/ές συμμετέχοντες/ουσες,

Το παρόν ερωτηματολόγιο αποτελεί μέρος μεταπτυχιακής εργασίας με θέμα: " Εξελίξεις στις τεχνολογίες βιομετρικών , μελέτη και αξιολόγηση ελέγχου πρόσβασης με χρήση behavioral biometrics, μελέτη περίπτωσης πάνω στα keystroke dynamics " του μεταπτυχιακού προγράμματος σπουδών 'Ασφάλεια Υπολογιστών και Δικτύων' του ΑΠΚΥ και έχει θέμα τη χρήση του ρυθμού της πληκτρολόγησης ως βιομετρικού συμπεριφοράς για τον έλεγχο πρόσβασης σε ηλεκτρονικές υπηρεσίες.

Πριν από τη συμπλήρωση του ερωτηματολογίου είναι σημαντικό να γνωρίζετε τα παρακάτω:

Α) Η συμπλήρωση του ερωτηματολογίου είναι προαιρετική και ανώνυμη.
Β) Οι πληροφορίες που θα δώσετε είναι αυστηρά εμπιστευτικές και διαθέσιμες αποκλειστικά και μόνο στον φοιτητή που υλοποιεί την έρευνα.
Γ) Δεν λαμβάνεται απολύτως κανένα στοιχείο που να σας ταυτοποιεί.
Δ) Οι πληροφορίες που θα δώσετε θα χρησιμοποιηθούν αυστηρά και μόνο για τους σκοπούς της έρευνας.

Για τη συμπλήρωση του ερωτηματολογίου απαιτούνται περίπου 5 λεπτά. Προσκαλείστε λοιπόν, να συμβάλετε σε αυτή την προσπάθεια με τη συμμετοχή σας στην παρούσα μελέτη. Σας ευχαριστώ εκ των προτέρων για το χρόνο σας. Παναγιώτης Κυριακίδης

Σε ποια ηλικιακή ομάδα ανήκετε; *

18-25, 26-39, 40-54, 55+

Ποιο είναι το φύλο σας;*

Άνδρας, Γυναίκα

Ποιο είναι το εκπαιδευτικό επίπεδό σας; *

Δευτεροβάθμια εκπαίδευση, Τριτοβάθμια (ΑΕΙ/ΤΕΙ), Μεταπτυχιακό, Διδακτορικό

Χρησιμοποιείτε συχνά ηλεκτρονικό υπολογιστή και το διαδίκτυο; *

Καθημερινά, Τουλάχιστον 3 φορές την εβδομάδα, Τουλάχιστον 1 φορά κάθε εβδομάδα, Μερικές φορές το μήνα

Γνωρίζετε τι είναι τα βιομετρικά? *

Ναι, γνωρίζω Όχι δεν γνωρίζω, Έχω ακούσει αλλά δεν είμαι σίγουρος/η

Ποιους από τους ακόλουθους τρόπους βιομετρικής αναγνώρισης έχετε ακούσει;*

Δακτυλικά αποτυπώματα (fingerprint)
Ίριδα του ματιού (iris)
Αναγνώριση προσώπου (face)
Αναγνώριση υπογραφής (signature)
DNA
Αναγνώριση αμφιβληστροειδούς (retina)
Αναγνώριση φωνής (voice)
Αναγνώριση ρυθμού πληκτρολόγησης (keystroke dynamics)

Ξέρετε ότι τα βιομετρικά χρησιμοποιούνται για τον έλεγχο της πρόσβασης; *

ΝΑΙ, ΟΧΙ

Γνωρίζετε ότι βιομετρικά στοιχεία σας περιέχονται ήδη στα δελτία ταυτότητας, διαβατήρια, άδεια οδήγησης, στη τράπεζα σας και αλλού; *

ΝΑΙ, ΟΧΙ

Πιστεύετε ότι μόνο η χρήση κωδικού (password) είναι αρκετά ασφαλής τρόπος πρόσβασης σε ηλεκτρονικές υπηρεσίες; *

Λιγότερο ασφαλής τρόπος 1, 2, 3, 4, 5 Πολύ ασφαλής τρόπος

Νιώθετε περισσότερη ασφάλεια με την αποστολή SMS για τη ολοκλήρωση ηλεκτρονικών πληρωμών; *

ΝΑΙ, ΟΧΙ, Δεν ξέρω

Έχετε ακούσει σχετικά με τις ηλεκτρονικές απάτες*

ΝΑΙ, ΟΧΙ

Έχετε πέσει θύμα ηλεκτρονικής απάτης; *

ΝΑΙ, ΟΧΙ, Δεν ξέρω

Πιστεύετε ότι με τη χρήση ΗΥ, λάπτοπ, smartphone, για πρόσβαση σε ηλεκτρονικές υπηρεσίες όπως τα social media (facebook, twitter, instagram), ηλεκτρονική τραπεζική και ηλεκτρονικό ταχυδρομείο, ο κίνδυνος από απειλές είναι αυξημένος; *

Πολύ αυξημένος, Σχετικά αυξημένος, Στα ίδια επίπεδα με παλαιότερα, Δεν γνωρίζω

Έχετε διακόψει τη χρήση υπηρεσιών λόγω υποψίας ή γεγονότων παραβίασης ασφαλείας;*

ΝΑΙ, ΟΧΙ

Πόσο συχνά αλλάζετε κωδικό (password) στις κύριες ηλεκτρονικές υπηρεσίες (mail, social, e-banking); *

Κάθε 3 μήνες ή λιγότερο, Κάθε εξάμηνο, Μια φορά το χρόνο, Όποτε μου προταθεί από το σύστημα, Ποτέ

Έχει προσβληθεί από ιό ή άλλο κακόβουλο λογισμικό ο υπολογιστής ή άλλη συσκευή σας; *

ΝΑΙ, ΟΧΙ, Δεν γνωρίζω

Θα προτιμούσατε ένα επιπλέον επίπεδο ασφάλειας πέρα από το password;*

ΝΑΙ, ΟΧΙ, Δεν γνωρίζω

Πιστεύετε ότι τα βιομετρικά βελτιώνουν το επίπεδο ασφαλείας σε ηλεκτρονικές υπηρεσίες; *

ΝΑΙ, ΟΧΙ, Δεν γνωρίζω

Πιστεύετε ότι το βιομετρικό συμπεριφοράς του ρυθμού της πληκτρολόγησης σας θα βοηθούσε ως ένα επιπλέον μέτρο ασφάλειας;*

ΝΑΙ, ΟΧΙ, Δεν γνωρίζω αυτό το βιομετρικό συμπεριφοράς

Για ποιο λόγο είστε περισσότερο επιφυλακτικοί σχετικά με τη χρήση των βιομετρικών σας;*

Διαρροή προσωπικών δεδομένων
Ασφάλεια αποθήκευσης των βιομετρικών στοιχείων
Ενδεχόμενη κακή χρήση των βιομετρικών από τρίτους (ασφαλιστικές, κρατικές αρχές)

Δεν είμαι επιφυλακτικός-ή
Άλλος λόγος

Ποιο βιομετρικό θα προτιμούσατε ως πιο φιλικό στη χρήση αλλά και θα θεωρούσατε λιγότερο επεμβατικό στη προσωπικότητα σας και στα προσωπικά σας δεδομένα:*

Δακτυλικά αποτυπώματα (fingerprint)
Ίριδα του ματιού μας (iris)
Αναγνώριση του προσώπου σας (face)
Αναγνώριση της υπογραφής σας (signature)
Χρήση του DNA σας
Αναγνώριση του αμφιβληστροειδούς (retina)
Αναγνώριση της φωνής (voice)
Αναγνώριση του ρυθμού της πληκτρολόγησης (keystroke dynamics)

Προκειμένου να εξυπηρετηθείτε καλύτερα, θα επιλέγατε να χρησιμοποιηθεί κάποιο βιομετρικό στοιχείο σας από διαδικτυακή υπηρεσία;*

Δεν θα επέλεγα σίγουρα 1,2,3,4,5 Σίγουρα θα επέλεγα

Η έλευση νέων τεχνολογιών όπως η τεχνητή νοημοσύνη και τα βιομετρικά στοιχεία θα βελτιώσουν την ασφάλεια των διαδικτυακών υπηρεσιών;*

Διαφωνώ πλήρως 1,2,3,4,5 Συμφωνώ απόλυτα