Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Πολυτεχνική Σχολή

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Εργαστήριο Επεξεργασίας Πληροφορίας και Υπολογισμών

Διπλωματική Εργασία

Συνεχής έμμεση αυθεντικοποίηση χρηστών κινητού τηλεφώνου με συνδυασμό των δεδομένων πλοήγησης και συμπεριφοράς

Χρήστος Εμμανουήλ
Αριθμός Μητρώου (ΑΕΜ): 8804

Επιβλέπων Καθηγητής: **Ανδρέας Συμεωνίδης**
Επιβλέπων Υποψήφιος Διδάκτωρ: **Θωμάς Καρανικιώτης**

Θεσσαλονίκη, Ιούλιος 2022

Περίληψη

Τα έξυπνα κινητά τηλέφωνα (smartphones) έχουν γίνει πλέον αναπόσπαστο κομμάτι της καθημερινότητας και οι πληροφορίες που αποθηκεύονται σε αυτά συνεχώς αυξάνονται. Προκύπτει λοιπόν το ζήτημα της ασφάλειας αυτών των συσκευών, που είναι κρίσιμο για την εξασφάλιση της προστασίας των δεδομένων του ιδιοκτήτη ενός smartphone από κακόβουλους χρήστες. Οι περισσότερες συσκευές πλέον προσφέρουν ένα επίπεδο ασφάλειας χρησιμοποιώντας διάφορους τρόπους αυθεντικοποίησης, που όμως έχουν χαρακτηριστεί ευάλωτοι και έτσι έχει δημιουργηθεί η ανάγκη για την υλοποίηση καινούργιων μεθοδολογιών. Λύση στο πρόβλημα έρχονται να δώσουν τεχνικές συνεχούς – έμμεσης αυθεντικοποίησης, δηλαδή συστήματα που εκτελούνται συνεχώς στο παρασκήνιο της συσκευής, χωρίς να χρειάζονται την εκτέλεση ενεργειών από την πλευρά του χρήστη. Τα συστήματα αυτά συνήθως χρησιμοποιούν διάφορα δεδομένα του κινητού τηλεφώνου ή άλλων συσκευών, μοντελοποιούν την συμπεριφορά του χρήστη και στην συνέχεια παρέχουν ένα μοναδικό ή συμπληρωματικό επίπεδο ασφαλείας, που εξετάζει αν η συμπεριφορά του χρήστη συμβαδίζει με αυτή του ιδιοκτήτη. Στη συγκεκριμένη εργασία, το σύστημα βασίζει τη λειτουργία του σε δεδομένα αισθητήρων που είναι ήδη εγκατεστημένοι στα περισσότερα smartphones, όπως το επιταχυνσιόμετρο, το γυροσκόπιο και η οθόνη αφής. Η συμπεριφορά του ιδιοκτήτη μοντελοποιείται με αυτά τα δεδομένα μέσω της χρήσης μοντέλων μηχανικής μάθησης που, στη συνέχεια, μπορούν να πάρουν κατάλληλες αποφάσεις. Αυτό που κάνει το εν λόγω σύστημα να ξεχωρίζει είναι η χρήση ενός συνόλου μοντέλων μηχανών διανυσμάτων υποστήριξης μίας κλάσης (One Class Support Vector Machines), με ένα εύρος τιμών για τις παραμέτρους, για κάθε τύπο δεδομένων, που παράγει την πιθανότητα μια συμπεριφορά να συμβαδίζει με αυτή του ιδιοκτήτη και στην συνέχεια καλεί ένα σύστημα εμπιστοσύνης να αποφασίσει αν θα πραγματοποιηθεί το κλείδωμα της συσκευής. Όπως αποδεικνύεται, ένα τέτοιο σύστημα είναι εύκολα υλοποιήσιμο, μπορεί να προσαρμόζεται στον τύπο δεδομένων που είναι διαθέσιμος κάθε στιγμή και έτσι μπορεί να επιφέρει σημαντικές βελτιώσεις στην αυθεντικοποίηση του χρήστη με έναν συνεχή αλλά και μη παρεμβατικό τρόπο.

Χρήστος Εμμανουήλ

Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Ελλάδα

Ιούνιος 2022

Abstract

Continuous implicit authentication of a smartphone user based on gesture and sensor data

Smartphones have become an important assistant to everyday life chores and the information stored in them is constantly increasing. This fact raises the issue of the security of data exchanged through these devices, which is crucial to ensure the protection of the owner from malicious users. These days, most devices offer a level of security using various authentication methods, which however have been identified as vulnerable and thus the need has arisen for the development of new, more secure, methodologies. Thus, a lot of recent approaches are targeted towards continuous – implicit authentication techniques, i.e., systems that run continuously in the background of the device, without the need to perform actions on the part of the user. These systems typically use various data from a mobile phone or other devices, model the behavior of the user and then provide a unique or complementary level of security, which examines whether the current user's behavior is in line with that of the owner. Within the context of this diploma thesis, the developed system relies on sensor data available on most smartphones, such as the accelerometer, gyroscope and touch screen. The behavior of the phone owner is modeled with these data through the use of machine learning models, which can then make appropriate decisions. The proposed system differentiates from similar approaches through the use of a set of One Class Support Vector Machines, with a range of values for the parameters for each data type, which produces the probability that a behavior is in line with that of the owner, which is then used by a confidence system to decide if the device will be locked. As it turns out, such a system is easy to develop, can be adapted to the type of data available at any time and thus can bring significant improvements in user authentication in a continuous but non-invasive way.

Christos Emmanouil

Department of Electrical and Computer Engineering

Aristotle University of Thessaloniki, Greece

June 2022

Ευχαριστίες

Η περάτωση της εργασίας αυτής σηματοδοτεί και την λήξη της πορείας μου ως προπτυχιακός φοιτητής. Για τον λόγο αυτό, θα ήθελα να εκφράσω τις ευχαριστίες μου σε όλους τους ανθρώπους που είχα την τιμή να συνεργαστώ και σε όλους αυτούς που είναι δίπλα μου όλα αυτά τα χρόνια. Ιδιαίτερα, θα ήθελα να ευχαριστήσω τον επιβλέποντα αναπληρωτή καθηγητή, κύριο Ανδρέα Συμεωνίδη, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτήν τη διπλωματική εργασία. Ειδικής μνείας αξίζει και ο συνεπιβλέπων της εργασίας μου και υποψήφιος διδάκτωρ, κύριος Θωμάς Καρανικιώτης, με τον οποίο είχαμε μια άριστη συνεργασία και ήταν δίπλα μου σε όποια απορία και προβληματισμό αντιμετώπισα. Η εργασία αυτή ήταν μια μοναδική εμπειρία, που μου έδωσε γνώσεις, εμπειρίες και με βοήθησε να εξερευνήσω περισσότερο τον κλάδο της μηχανικής μάθησης και των δεδομένων. Ελπίζω με την εργασία μου να συνείσφερα και εγώ στο πρόβλημα της συνεχούς και έμμεσης προστασίας των κινητών τηλεφώνων και ευελπιστώ η εργασία αυτή να βοηθήσει φοιτητές που θα επιλέξουν να ασχοληθούν με το συγκεκριμένο πρόβλημα.

Χρήστος Εμμανουήλ

Πίνακας Περιεχομένων

Λίστα Σχημάτων

Λίστα Πινάκων

1 Εισαγωγή

1.1 Κίνητρο & Περιγραφή Προβλήματος

Αυτή την στιγμή εκτιμάται ότι περίπου το 85% του παγκόσμιου πληθυσμού, δηλαδή 6,64 δισεκατομμύρια χρήστες, χρησιμοποιούν έξυπνα κινητά τηλέφωνα (smartphones). Ο αριθμός αυτός το 2016 ήταν μόλις 3,7 δισεκατομμύρια, ενώ αναμένεται να ξεπεράσει τα 7,6 δισεκατομμύρια μέχρι το 2027 [1]. Αποδεικνύεται λοιπόν, ότι η ανάπτυξη των συγκεκριμένων συσκευών είναι ραγδαία και πλέον αποτελούν αναπόσπαστο κομμάτι της καθημερινότητας. Συγκεκριμένα, όπως αναφέρεται σε έρευνα που πραγματοποιήθηκε στην Ισπανία το 2019, το 22,5% των χρηστών χρησιμοποιούν την συσκευή τους τουλάχιστον για 1-2 ώρες, ενώ το 17,7% ξεπερνά τις 4 ώρες [2] καθημερινά.

Αποτελέσματα της αλληλεπίδρασης με αυτές τις συσκευές είναι η δημιουργία και αποθήκευση δεδομένων. Αυτά μπορεί να είναι διάφορες προσωπικές και επαγγελματικές πληροφορίες, όπως μηνύματα, φωτογραφίες, έγγραφα, κωδικοί αλλά και μεταδεδομένα διάφορων εφαρμογών. Η διάθεση αυτών σε κάποιον κακόβουλο χρήστη μπορεί να αποβεί επικίνδυνη για τον κάτοχο, καθιστώντας έτσι μείζονος σημασίας την ασφάλεια αυτών των συσκευών.

Σήμερα, οι περισσότερες συσκευές στηρίζουν την ασφάλειας τους σε μεθόδους αυθεντικοποίησης που χρησιμοποιούν τα χαρακτηριστικά του δαχτυλικού αποτυπώματος, του προσώπου ή της φωνής, σε συνδυασμό με κάποιον κωδικό πρόσβασης (pin ή password) ή ένα μοτίβο (graphical password). Το μειονέκτημα αυτών των παραδοσιακών μεθοδολογιών οφείλεται στο γεγονός ότι αποτελούν το μοναδικό επίπεδο ασφάλειας (single point of entrance). Κάποιος χρήστης μπορεί να προσπεράσει την οθόνη κλειδώματος, εφαρμόζοντας τεχνικές υποκλοπής και στην συνέχεια να έχει πρόσβαση σε όλα τα δεδομένα της συσκευής. Επιπλέον, έρευνα του 2018 έδειξε ότι το 52% των χρηστών δεν χρησιμοποιεί κανέναν τρόπο ασφάλισης [3], υπογραμμίζοντας έτσι, ότι οι παραδοσιακές μεθοδολογίες αυθεντικοποίησης δυσχεραίνουν τους χρήστες και άρα πολλοί δεν τις χρησιμοποιούν.

Προκύπτει λοιπόν η ανάγκη για την ανάπτυξη ενός νέου συστήματος συνεχούς – έμμεσης αυθεντικοποίησης (Continuous Implicit Authentication – CIA), που θα παρέχει προστασία και μετά το ξεκλείδωμα της συσκευής, ενώ ταυτόχρονα θα εκτελείται στο παρασκήνιο με διαφανή τρόπο προς τον χρήστη, προσεγγίζοντας ισορροπημένα τις προδιαγραφές ασφάλειας και ευχρηστίας.

1.2 Στόχος Διπλωματικής Εργασίας

Σε ερευνητικό επίπεδο έχουν πραγματοποιηθεί αρκετές μελέτες για την ανάπτυξη CIA συστημάτων. Πολλές είναι όμως αυτές, που γεννούν ερωτήματα σχετικά με την αποτελεσματικότητα των προτεινόμενων συστημάτων σε πραγματικές συνθήκες αλλά και την λειτουργικότητα που προσφέρουν στον χρήστη.

Βασικός στόχος της διπλωματικής εργασίας είναι η ανάπτυξη και ολοκληρωμένη αξιολόγηση ενός συστήματος συνεχούς – έμμεσης αυθεντικοποίησης, που θα λειτουργεί με δεδομένα που προέρχονται από το smartphone και θα μπορεί να ανταπεξέλθει αποδοτικά σε ποικιλία πραγματικών συνθηκών.

Πιο συγκεκριμένα, η έννοια της συνεχούς αυθεντικοποίησης αφορά το γεγονός ότι ο έλεγχος πρέπει να πραγματοποιείται όσο διάστημα ο χρήστης χρησιμοποιεί την συσκευή, εκτελώντας ελέγχους και μετά το ξεκλείδωμά της, ενώ η έμμεση αυθεντικοποίηση αναφέρεται στη διατήρηση της ευχρηστίας της συσκευής, χωρίς να χρειάζεται η εκτέλεση επιπρόσθετων ενεργειών από πλευράς χρήστη. Η μεθοδολογία στηρίζεται στην μοντελοποίηση του τρόπου που ο χρήστης αλληλεπιδρά με την συσκευή. Προς αυτή την κατεύθυνση, στην συγκεκριμένη εργασία, χρησιμοποιούνται δεδομένα δύο ειδών: αυτά του επιταχυνσιομέτρου (accelerometer) και του γυροσκοπίου (gyroscope) που περιγράφουν τον τρόπο που ο χρήστης κρατάει την συσκευή, αλλά και αυτά της οθόνη αφής που περιγράφουν τον τρόπο πλοήγησης. Αυτά τα δεδομένα παράγονται από τα περισσότερα smartphones και σε συνδυασμό με τεχνικές μηχανικής μάθησης (Machine Learning – ML), μπορούν να αποτελέσουν την βάση για ένα CIA σύστημα.

Η αξιολόγηση ενός τέτοιου συστήματος αφορά τόσο την προστασία από κακόβουλους χρήστες, όσο και την λειτουργικότητα προς τον κάτοχο. Ιδανικά, το σύστημα θα πρέπει να κλειδώνει την συσκευή σε μη εξουσιοδοτημένους χρήστες προτού προβούν σε οποιαδήποτε παράνομη πράξη, αλλά και να μην απορρίπτει τον ιδιοκτήτη την ώρα που διεκπεραιώνει σημαντικές διεργασίες. Ωστόσο, τα ζητούμενα αυτά είναι αντιστρόφως ανάλογα: η σχεδίαση αυστηρότερων συστημάτων μπορεί να οδηγήσει σε συχνά κλειδώματα του κατόχου, ενώ η σχεδίαση ελαστικότερων συστημάτων σε συχνή αποδοχή κακόβουλων χρηστών. Το παραπάνω γεγονός, σε συνδυασμό με την διαφορετικότητα της ανθρώπινης συμπεριφοράς και την ύπαρξη σφαλμάτων στα απαιτούμενα δεδομένα, θέτει την ταυτόχρονη επίτευξη χαμηλών ποσοστών αποδοχής μη εξουσιοδοτημένων χρηστών και χαμηλών ποσοστών απόρριψης του πραγματικού χρήστη ένα απαιτητικό πρόβλημα, που χρειάζεται μεγάλο πλήθος δεδομένων, διαφορετικών χρηστών, ώστε να μπορεί να γίνει η εξαγωγή συμπερασμάτων που ανταποκρίνονται στην πραγματικότητα.

1.3 Διάρθρωση Κειμένου

Το παρόν κείμενο αποτελεί την γραπτή αναφορά της διαδικασίας σχεδιασμού και υλοποίησης του συστήματος αυθεντικοποίησης αλλά και των πειραμάτων που εκτελέστηκαν. Το κίνητρο και οι στόχοι παρουσιάστηκαν σε αυτή την ενότητα. Στην επόμενη ενότητα γίνεται η περιγραφή των εννοιών της αυθεντικοποίησης και της μηχανικής μάθησης, αναλύεται ο τρόπος λειτουργίας των αισθητήρων που χρησιμοποιούνται και παρουσιάζονται χρήσιμοι αλγόριθμοι και μετρικές. Στην τρίτη ενότητα ερευνάται η επιστημονική περιοχή, καταγράφονται διάφορες έρευνες και υπογραμμίζεται ο ρόλος της προκείμενης εργασίας. Στην τέταρτη περιγράφεται λεπτομερώς η διαδικασία σχεδιασμού του τελικού συστήματος, παρουσιάζονται τα προβλήματα που αντιμετωπίστηκαν και αναλύονται τα κριτήρια επιλογής των διαφόρων παραμέτρων. Τέλος, στην ενότητα πέντε καταγράφονται τα αποτελέσματα, γίνονται συγκρίσεις με άλλες εργασίες και αναφέρονται τα συμπεράσματα, δίνοντας προτάσεις για μελλοντική έρευνα.

2 Θεωρητικό Υπόβαθρο

Για την κατανόηση του προβλήματος, του συστήματος που αναπτύχθηκε καθώς και της μεθοδολογίας που περιγράφεται σε επόμενη ενότητα, κρίνεται απαραίτητη η εξοικείωση του αναγνώστη με έννοιες και τεχνικές που εφαρμόστηκαν. Σε αυτό το κεφάλαιο λοιπόν, γίνεται η ανάλυση του θεωρητικού υποβάθρου.

2.1 Αυθεντικοποίηση

Αυθεντικοποίηση (authentication) είναι η διαδικασία κατά την οποία ο χρήστης παρέχει σε ένα πληροφοριακό σύστημα τα απαραίτητα στοιχεία, με σκοπό να εγκριθεί η πρόσβαση στα αντικείμενα που ορίστηκαν κατά την διαδικασία της *ταυτοποίησης (identification)*. Σημειώνεται ότι οι όροι αυθεντικοποίηση και ταυτοποίηση είναι διαφορετικοί και δεν πρέπει να συγχέονται. Για παράδειγμα, σε έναν ηλεκτρονικό υπολογιστή με την ταυτοποίηση ορίζεται ο ρόλος του χρήστη ως διαχειριστή ή επισκέπτη, ενώ με την αυθεντικοποίηση ελέγχεται η αντιστοίχιση στον ρόλο αυτό. Ωστόσο, τα κινητά τηλέφωνα είναι μια προσωπική συσκευή, ο χρήστης είναι μοναδικός και έτσι οι δύο όροι είναι ταυτόσημοι.

Η εξέλιξη της τεχνολογίας και των μεθοδολογιών έχει οδηγήσει στην διαμόρφωση διάφορων συστημάτων αυθεντικοποίησης. Μια κατηγοριοποίηση αυτών μπορεί να γίνει βάση της πληροφορίας που απαιτούν από τον χρήστη [4]. Οι κύριες αυτές κατηγορίες περιγράφονται παρακάτω (Σχήμα 1):

- *Κάτι που ξέρεις (Something You Know):* Ο χρήστης πρέπει να γνωρίζει κάτι για να αποκτήσει πρόσβαση. Αυτό θα μπορούσε να είναι ένας κωδικός, ένα μοτίβο ή μία ερώτηση ασφαλείας.

- *Κάτι που έχεις (Something You Have):* Ο χρήστης πρέπει να έχει κάτι στην κατοχή του. Τέτοια παραδείγματα είναι διακριτικά ασφαλείας, ειδικές συσκευές ή ταυτότητες.

- *Κάτι που είσαι (Something You Are):* Συστήματα τα οποία βασίζονται σε έμφυτα φυσικά (physical) ή συμπεριφορικά (behavioral) χαρακτηριστικά, γνωστά και ως βιομετρικά. Παραδείγματα αποτελούν το δαχτυλικό αποτύπωμα, το πρόσωπο, η φωνή [5] αλλά και ο γραφικός χαρακτήρας ή ο τρόπος πληκτρολόγησης [6].

Επιπλέον, ένας ακόμα διαχωρισμός γίνεται βάσει της διαφάνειας του συστήματος προς τον τελικό χρήστη. Έτσι ο έλεγχος μπορεί να είναι:

- *Ενεργός (Active – Explicitly):* Όπου το σύστημα απαιτεί την εισαγωγή δεδομένων από τον χρήστη, όπως την πληκτρολόγηση ενός κωδικού ή μίας απάντησης σε μία ερώτηση ασφαλείας.

- *Παθητικός (Passive – Implicitly):* Όταν εκτελείται στο παρασκήνιο, χωρίς να χρειάζεται ενέργεια από τον χρήστη. Συστήματα αυτής της κατηγορίας ξεχωρίζουν για την δυνατότητά τους να εκτελούνται συνεχώς χωρίς να επεμβαίνουν στην λειτουργικότητα της συσκευής.

Σχήμα 1: Κατηγορίες Συστημάτων Αυθεντικοποίησης

Πλέον, πολλές υπηρεσίες και εφαρμογές έχουν αρχίσει να χρησιμοποιούν συνδυασμούς τεχνικών αυθεντικοποίησης (Multi Factor Authentication – MFA). Η ανάληψη χρημάτων από το ATM με την χρήση κάρτας και την πληκτρολόγηση του PIN, αλλά και η σύνδεση σε λογαριασμούς ηλεκτρονικού ταχυδρομείου με τον κωδικό πρόσβασης και κάποιο συνθηματικό, είναι μερικά παραδείγματα τέτοιων συστημάτων. Όπως μάλιστα επιβεβαιώνουν οι Microsoft [7] και Google [8], τέτοια σύστημα αυξάνουν σημαντικά τα επίπεδα ασφαλείας, περιορίζοντας σημαντικά τις επιθέσεις από κακόβουλους χρήστες.

2.1.1 Συνεχής Έμμεση Αυθεντικοποίηση Συμπεριφορικών Χαρακτηριστικών

Οι άνθρωποι συχνά δημιουργούν διάφορες συνήθειες στην καθημερινότητά τους. Για παράδειγμα, η ώρα που κάποιος ξυπνάει και η συχνότητα που πλένει τα δόντια του είναι συνήθειες διαφορετικές για κάθε άνθρωπο και σε έναν βαθμό μπορούν να τον χαρακτηρίζουν. Έτσι λοιπόν, και ο τρόπος που κάποιος κρατάει το κινητό ή αλληλοεπιδρά με την οθόνη μπορεί να ορίσει μια συμπεριφορά και να αποτελέσει ένα βελτιωμένο μηχανισμό αυθεντικοποίησης, αποτελεσματικό στην καταπολέμηση της μη εξουσιοδοτημένης πρόσβασης.

Τα φυσιολογικά χαρακτηριστικά συνήθως χρησιμοποιούνται για στιγμιαίο έλεγχο ταυτότητας, ενώ τα συμπεριφορικά χαρακτηριστικά μπορούν να εφαρμοστούν με παθητικό τρόπο, δίνοντας την δυνατότητα για συνεχή έλεγχο [9]. Ένα σύστημα ελέγχου που εκτελείται με συνεχή και έμμεσο τρόπο μπορεί να εφαρμοστεί ως μοναδικός τρόπος αυθεντικοποίησης, απαλλάσσοντάς τον χρήστη από την διαδικασία εισαγωγής κωδικού, αλλά και ως ένα επιπλέον επίπεδο αυθεντικοποίησης, υποβοηθώντας τους κοινούς τρόπους ασφάλειας. Για παράδειγμα, μετά το ξεκλείδωμα της συσκευής, αν η αλληλεπίδραση που παρατηρείται αποκλίνει από την συμπεριφορά του κατόχου, σημαίνει ότι η πιθανότητα να χειρίζεται ο κάτοχος την συσκευή μειώνεται, αν σημειωθούν αρκετές αποκλίνουσες συμπεριφορές, η συσκευή κλειδώνει και ζητά την εισαγωγή κωδικού [10].

Ωστόσο, ακολουθώντας μια τέτοια λογική, προκύπτουν τα εξής ερωτήματα:

- Πόσο ενοχλητικός είναι ένας τέτοιος μηχανισμός για τον ιδιοκτήτη;

- Πώς επηρεάζεται η απόδοση της συσκευής;

Μέσω όμως προσεκτικής σχεδίασης, καθώς και με την χρήση δεδομένων που έτσι και αλλιώς παράγονται συνεχώς από μια συσκευή, μπορούν να αναπτυχθούν μηχανισμοί που εξασφαλίζουν:

- Καλύτερη εμπειρία χρήστη, καθώς δεν απαιτούνται ενέργειες από αυτόν.

- Ενισχυμένο σύστημα ασφάλειας, λόγω διαφάνειας αλλά και ύπαρξης πολλαπλών επιπέδων αυθεντικοποίησης.

- Εύκολη προσαρμογή σε μεγάλο πλήθος χρηστών, καθώς το σύστημα μαθαίνει από τα δεδομένα του κάθε χρήστη.

- Προοπτικές εξέλιξης, καθώς η ανάπτυξη τέτοιων συστημάτων γίνεται σε επίπεδο λογισμικού, που μπορεί να βελτιωθεί με σχετική ευκολία.

- Χαμηλό κόστος ανάπτυξης, καθώς τα περισσότερα smartphones διαθέτουν το απαραίτητο υλικό (hardware).

Συνοπτικά, η χρήση βιομετρικών στοιχείων συμπεριφοράς είναι μη παρεμβατική στην εμπειρία του χρήστη, ενώ ταυτόχρονα παρέχει ακριβείς πληροφορίες για τον προσδιορισμό της ταυτότητας και έτσι καθίσταται ιδιαίτερα εύχρηστη και ασφαλή τεχνική [11].

2.2 Δεδομένα Κινητού Τηλεφώνου

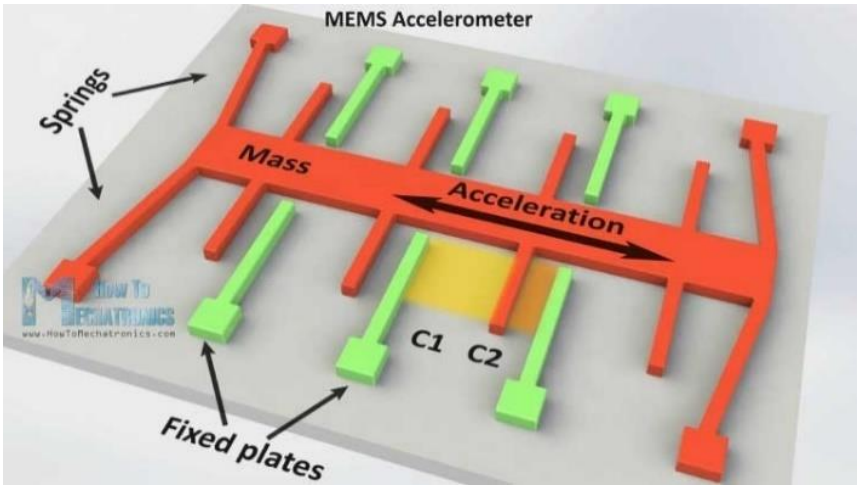
Όπως αναφέρθηκε και στο πρώτο κεφάλαιο, τα smartphones κατά την λειτουργία τους παράγουν και αποθηκεύουν μεγάλο πλήθος δεδομένων. Μέρος αυτών προέρχεται από ένα πλήθος αισθητήρων που χρησιμοποιούνται από το λειτουργικό σύστημα και διάφορες εφαρμογές.

Εξ ορισμού, ένας αισθητήρας είναι μια συσκευή η οποία μετράει μια φυσική ποσότητα και την μετατρέπει σε ηλεκτρικό σήμα. Δηλαδή είναι ένας μετατροπέας ερεθισμάτων σε αναλογικό ή ψηφιακό σήμα. Η ποιότητα και ακρίβεια των μετρήσεων συνήθως μεταβάλλεται ανάλογα με την ποιότητα κατασκευής και το κόστος. Συνεπώς, μεταξύ αισθητήρων ίδιας λειτουργίας, αλλά διαφορετικών κινητών τηλεφώνων μπορεί να υπάρξουν διαφοροποιήσεις στα δεδομένα. Τα smartphones διαθέτουν πολλούς αισθητήρες, όπως αυτός της κάμερας ή του μικροφώνου. Ωστόσο, για τις ανάγκες της εργασίας, θα δοθεί έμφαση στον τρόπο λειτουργίας του επιταχυνσιομέτρου, του γυροσκοπίου και της οθόνης αφής.

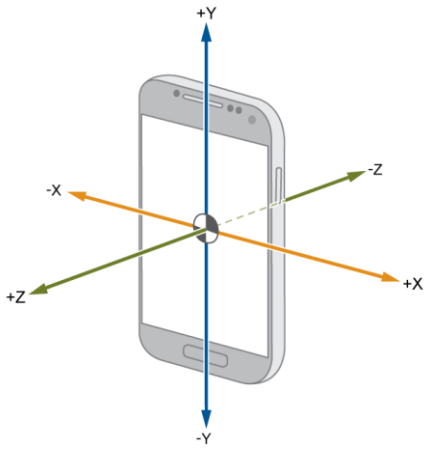
2.2.1 Επιταχυνσιόμετρο

Το *επιταχυνσιόμετρο (accelerometer)* ανήκει στην κατηγορία των αισθητήρων κίνησης και μπορεί να μετράει την μεταβολή της επιτάχυνσης. Χρησιμοποιείται για την ανίχνευση κινήσεων αλλά και τον προσδιορισμό του προσανατολισμού μιας συσκευής. Υπάρχουν διαφορετικοί τύποι, αλλά η αρχή λειτουργίας είναι ίδια. Αυτό που κάνει είναι να μετατρέπει μηχανικές δυνάμεις σε ηλεκτρικό σήμα, βάσει της μεταβολής μίας αντίστασης ή μιας χωρητικότητας. Στις ηλεκτρονικές συσκευές συνήθως συναντάται ο τύπος των μικροηλεκτρομηχανικών συστημάτων (Microelectromechanical Systems – MEMS) (Σχήμα 2) [12]. Στα κινητά τηλέφωνα, χρησιμοποιούνται αισθητήρες τέτοιου τύπου, που όμως μπορούν να αντιληφθούν τις συνιστώσες της επιτάχυνσης στους τρεις άξονες x, y και z (Σχήμα 3).

Οι μετρήσεις από ένα επιταχυνσιόμετρο λαμβάνονται βάσει μίας προκαθορισμένης συχνότητας δειγματοληψίας και οποιαδήποτε στιγμή μπορούν να χρησιμοποιηθούν για την διεκπεραίωση χρήσιμων λειτουργιών. Μερικές από αυτές είναι η περιστροφή της οθόνης, η διατήρηση σωστού προσανατολισμού στις φωτογραφίες, καθώς και ο υπολογισμός της ταχύτητας του χρήστη.



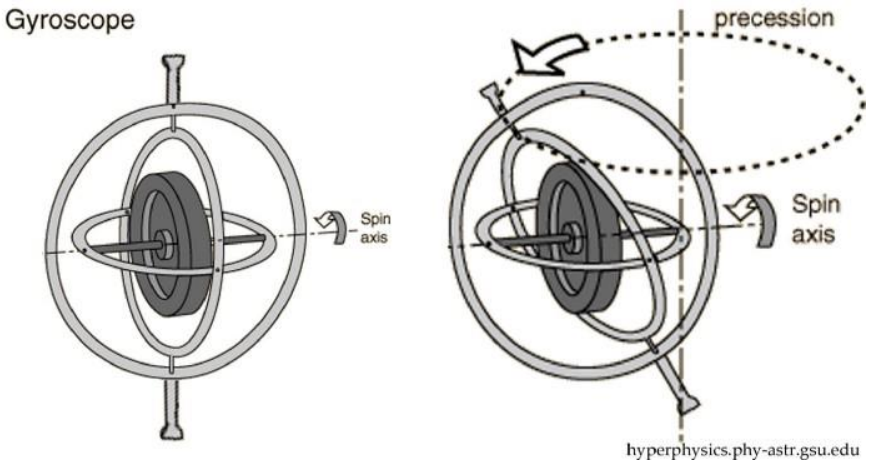
Σχήμα 2: Μικροηλεκτρομηχανικό Επιταχυνσιόμετρο



Σχήμα 3: Επιταχυνσιόμετρο Τριών Αξόνων

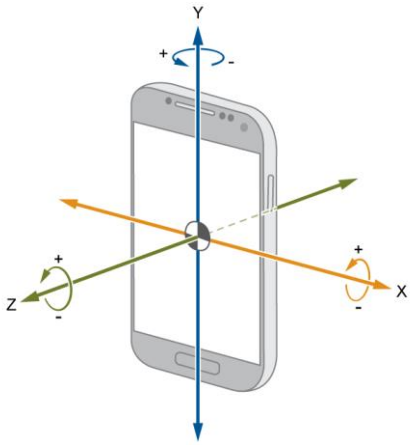
2.2.2 Γυροσκόπιο

Το *γυροσκόπιο (gyroscope)* ανήκει και αυτό στην κατηγορία των αισθητήρων κίνησης. Είναι ένας πολύ απλός μηχανισμός, ιδιαίτερα χρήσιμος σε πολλές εφαρμογές χάρη στην ικανότητά του να παρέχει ακριβείς μετρήσεις προσανατολισμού και περιστροφής. Αντιστέκεται στις εξωτερικές αλλαγές, διορθώνοντας οποιαδήποτε γωνιακή μετατόπιση, παρέχοντας έτσι σταθερότητα και ισορροπία. Στην απλή μορφή του είναι ένας ρότορας σε έναν άξονα περιστροφής, που περικλείεται από ένα πλαίσιο (Σχήμα 4) [13] και η λειτουργία του βασίζεται στην αρχή διατήρηση της στροφορμής.



Σχήμα 4: Γυροσκόπιο

Όπως και στο επιταχυνσιόμετρο, υπάρχουν διαφορετικοί τύποι, ενώ στα smartphones προτιμάται ο τύπος MEMS. Συνήθως χρησιμοποιείται για την μέτρηση των γωνιών περιστροφής στους τρεις άξονες (Σχήμα 5) και για την βελτίωση των μετρήσεων του επιταχυνσιομέτρου. Η μορφή τους διαφέρει από αυτή της προηγούμενης εικόνας, ωστόσο η βασική αρχή λειτουργίας παραμένει ίδια. Σημαντικές δυνατότητες που προσφέρει το γυροσκόπιο στις κινητές συσκευές είναι η σταθεροποίηση των εικόνων, ο καθαρισμός εικόνων πανοράματος, η υποστήριξη του συστήματος πλοήγησης (Global Positioning System – GPS) όταν χάνεται το σήμα, αλλά και η ανίχνευση κινήσεων του χρήστη σε διάφορα παιχνίδια και εφαρμογές.



Σχήμα 5: Γυροσκόπιο Κινητού Τηλεφώνου

2.2.3 Οθόνη Αφής

Μια *οθόνη αφής (touchscreen)* είναι μια συσκευή εισόδου/εξόδου. Προβάλει πληροφορίες στον χρήστη, ενώ ταυτόχρονα δέχεται ερεθίσματα από αυτόν. Η υλοποίηση του πρώτου λειτουργικού touchscreen έγινε το 1973, ενώ, από τότε μέχρι σήμερα έχει γίνει ένας από τους πιο διαδεδομένους τρόπους αλληλεπίδρασης σε πάρα πολλά συστήματα [14].

Η λειτουργία του βασίζεται στα τρία παρακάτω βασικά στοιχεία [15]:

- *Αισθητήρας Αφής (Touch Sensor):* Επιφάνεια η οποία μπορεί να αντιληφθεί άγγιγμα. Υπάρχουν διαφορετικοί τύποι. Στα κινητά τηλέφωνα συνήθως συναντάται ο *χωρητικός (capacitive).* Πρόκειται για μια επιφάνεια επικαλυμμένη με ένα ηλεκτρικά φορτισμένο υλικό. Το άγγιγμά της προκαλεί αλλαγή στην χωρητικότητα, υποδεικνύοντας έτσι την περιοχή αλληλεπίδρασης. Χαρακτηριστικά του συγκεκριμένου τύπου είναι η ανθεκτικότητα, η μεγάλη ακρίβεια και το γεγονός ότι λειτουργεί αποκλειστικά με άγγιγμα δαχτύλου [16].

- *Ελεγκτής (Controller):* Το hardware που μετατρέπει τις αλλαγές τάσης του αισθητήρα αφής σε σήματα που μπορούν να λάβουν οι ηλεκτρονικές συσκευές.

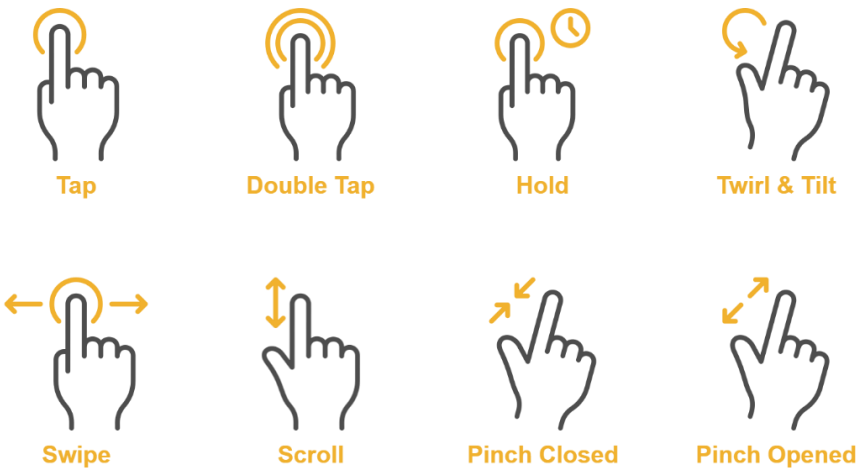
- *Λογισμικό (Software):* Λαμβάνει το σήμα από τον ελεγκτή και ενημερώνει την συσκευή για την τοποθεσία και το είδος του σήματος, κάνοντας στην ουσία την συσκευή να αντιδρά ανάλογα.

Στα smartphones όλες οι λειτουργίες γίνονται μέσω της οθόνης αφής. Ο χρήστης αλληλεπιδρά με το κινητό τηλέφωνο επιλέγοντας το εικονίδιο ή το αντικείμενο που επιθυμεί. Επίσης, έχει τη δυνατότητα να ενεργοποιήσει λειτουργίες με συντομεύσεις που ορίζονται από διάφορες *χειρονομίες (gestures).* Συνήθως, οι χειρονομίες είναι παρόμοιες μεταξύ διαφορετικών συσκευών, ωστόσο μπορεί να είναι διαφορετικές οι λειτουργίες τους. Παρακάτω φαίνονται μερικές από τις πιο συνηθισμένες (Σχήμα 6).

Στην εργασία χρησιμοποιούνται οι:

- *Tap*: Η πιο βασική χειρονομία που πραγματοποιείται με ελαφριά αφή με το δάχτυλο του χρήστη. Χρησιμοποιείται αντί για τη χρήση κουμπιών ή το πάτημα πλήκτρων του πληκτρολογίου.

- *Swipe, Scroll*: Χρήσιμες χειρονομίες που πραγματοποιούνε με το οριζόντιο ή κατακόρυφο σύρσιμο του δακτύλου στην οθόνη. Σημειώνεται ότι τα scrolls αναφέρονται και ως κατακόρυφα swipes. Είναι γενικά γρήγορες κινήσεις στην οθόνη, παρόμοιες με τις κινήσεις που θα κάνει ο χρήστης για να γυρίσει μια σελίδα σε ένα βιβλίο. Ο χρήστης μπορεί να εναλλάσσεται μεταξύ των αρχικών οθονών ή να κάνει κύλιση σε μία ιστοσελίδα ή έγγραφο.



Σχήμα 6: Χειρονομίες Οθόνης Αφής

2.3 Τεχνητή Νοημοσύνη

Στο πρώτο μισό του 20ου αιώνα (1938 - 1946), η επιστημονική φαντασία άρχισε να εξοικειώνει τον κόσμο με την έννοια των ρομπότ. Την δεκαετία του 1950 ένα ρεύμα επιστημόνων άρχισε να ερευνά το μαθηματικό ενδεχόμενο της *τεχνητής νοημοσύνης (Artificial Intelligence – AI),* δηλαδή συστημάτων που μιμούνται στοιχεία της ανθρώπινης συμπεριφοράς και υπονοούν κάποια στοιχειώδη ευφυΐα. Το 1956 όπως πολλοί θεωρούν, οι Allen Newell, Cliff Shaw και Herbert Simon παρουσίασαν το πρώτο πρόγραμμα που σχεδιάστηκε για να μιμείται τις δεξιότητες επίλυσης προβλημάτων ενός ανθρώπου (Logic Theorist). Από τότε και μέχρι τα τέλη του αιώνα γίνονται σημαντικές προσπάθειες εξέλιξης του κλάδου. Χαρακτηριστικό παράδειγμα αποτελεί η ήττα του παγκόσμιου πρωταθλητή σκακιού Gary Kasparov το 1997 από το Deep Blue της IBM [17].

Σήμερα η τεχνολογική ανάπτυξη είναι τεράστια, οι υπολογιστές είναι προσιτοί στο ευρύ κοινό, μπορούν να αποθηκεύσουν τεράστιο όγκο πληροφοριών και να εκτελέσουν πράξεις πάρα πολύ γρήγορα. Το γεγονός αυτό επιτρέπει την ενσωμάτωση AI συστημάτων σε κάθε τομέα

και πρόβλημα. Στις διάφορες μηχανές αναζήτησης και συστήματα προτάσεων (Netflix Recommendation Engine), στους έξυπνους βοηθούς (Google Assistant, Alexa, Siri) και αυτοκίνητα αλλά και σε τραπεζικά συστήματα και συστήματα υγείας, υπάρχει ένα μικρό ή μεγάλο κομμάτι τεχνητής νοημοσύνης.

2.4 Μηχανική Μάθηση

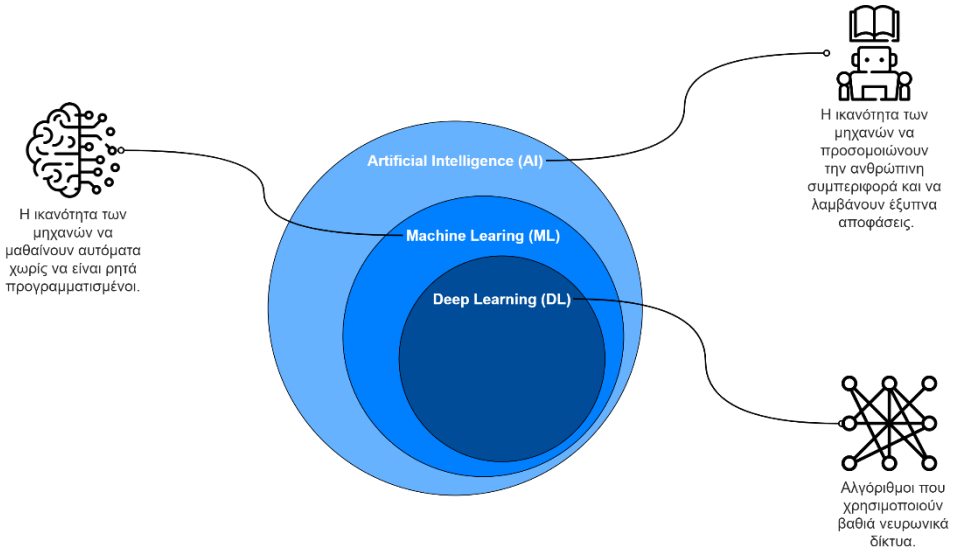
Η *μηχανική μάθηση (Machine Learning – ML)* είναι κλάδος του AI (Σχήμα 7). Βασίζεται στην ιδέα ότι τα συστήματα μπορούν να χρησιμοποιούν δεδομένα και αλγορίθμους για να βελτιώνουν την αποτελεσματικότητά τους χωρίς να προγραμματίζονται ρητά.

Είναι μία διαδικασία, στον πυρήνα της οποίας βρίσκεται ένας έξυπνος αλγόριθμος που όπως αναφέρει ο Michael Tamir [18], αποτελείται από τρία βασικά στοιχεία:

1. *Διαδικασία Απόφασης (Decision Process):* Μια ακολουθία υπολογισμών ή άλλων βημάτων που λαμβάνει δεδομένα και επιστρέφει μια εικασία για το είδος τους ή την απάντηση που ψάχνει να βρει ο αλγόριθμος.

2. *Συνάρτηση Σφάλματος (Error Function):* Μια μέθοδος αξιολόγησης της εικασίας συγκρίνοντάς την με γνωστά παραδείγματα (όταν είναι διαθέσιμα).

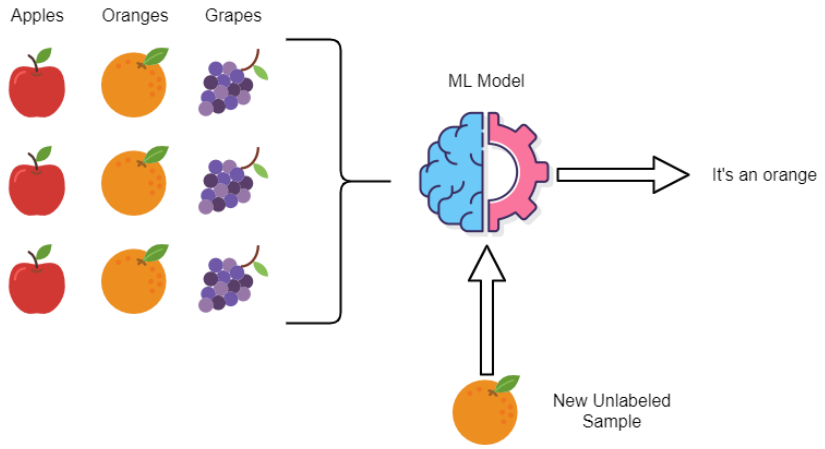
3. *Διαδικασία Βελτιστοποίησης (Optimization Process):* Εξετάζει την αστοχία και στη συνέχεια ενημερώνει την διαδικασία απόφασης έτσι ώστε την επόμενη φορά το σφάλμα να είναι μικρότερο.



Σχήμα 7: Σχέσεις Τεχνίτης Νοημοσύνης, Μηχανικής Μάθησης & Βαθιάς Μάθησης

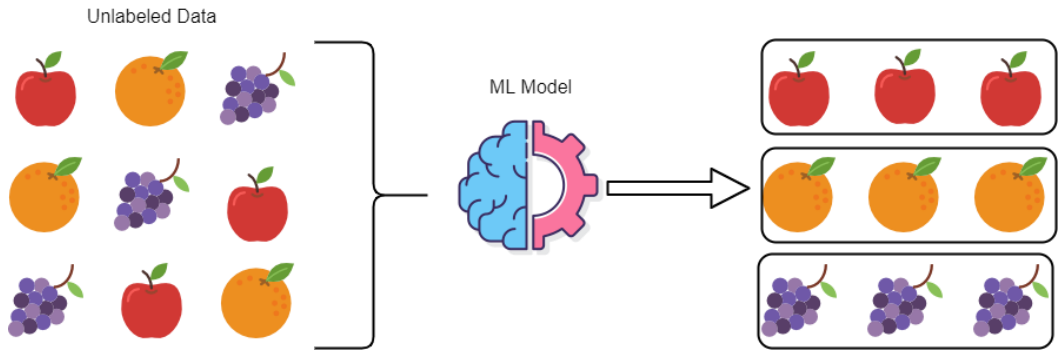
Η επιλογή και η εκπαίδευση του αλγορίθμου, ώστε να δίνει επιθυμητές απαντήσεις, είναι ενέργειες που ένας επιστήμονας κάνει βάσει του είδους των διαθέσιμων δεδομένων και το ερευνητικό ερώτημα. Ο τρόπος εκπαίδευσης μπορεί να διαχωριστεί σε τέσσερις βασικές προσεγγίσεις [19]:

- *Εποπτευόμενη Μάθηση (Supervised Learning):* Ο αλγόριθμος μαθαίνει σε ένα επισημασμένο (labelled) σύνολο δεδομένων (Σχήμα 8). Κάθε δείγμα στο σύνολο εκπαίδευσης επισημαίνεται με την απάντηση που ψάχνει να βρει ο αλγόριθμος. Ο αλγόριθμος μπορεί να χρησιμοποιήσει την απάντηση αυτή για να αξιολογήσει την ακρίβειά του και να βελτιώνεται. Η εποπτευόμενη μάθηση είναι χρήσιμη σε προβλήματα ταξινόμησης (classification) και παλινδρόμησης (regression).



Σχήμα 8: Εποπτευόμενη Μάθηση

- *Μη Εποπτευόμενη Μάθηση (Unsupervised Learning):* Τα καθαρά, τέλεια επισημασμένα σύνολα δεδομένων δεν είναι πάντα εύκολο να βρεθούν και μερικές φορές τα ερωτήματα δεν έχουν ξεκάθαρη απάντηση. Σε αυτές τις περιπτώσεις χρησιμοποιείται η μάθηση χωρίς επίβλεψη (Σχήμα 9). Στη μη εποπτευόμενη μάθηση ένας αλγόριθμος λαμβάνει ένα σύνολο δεδομένων χωρίς ρητές οδηγίες σχετικά με το τι πρέπει να γίνει, τα δείγματα δεν έχουν συγκεκριμένο επιθυμητό αποτέλεσμα και ο αλγόριθμός επιχειρεί να βρει μοτίβα, εξάγοντας χρήσιμα χαρακτηριστικά και αναλύοντας την δομή τους. Η μάθηση χωρίς επίβλεψη είναι ιδιαίτερα χρήσιμη σε προβλήματα ομαδοποίησης (clustering), ανάλυσης συσχετίσεων (association analysis) και μείωσης διαστάσεων (dimensionality reduction).



Σχήμα 9: Μη Εποπτευόμενη Μάθηση

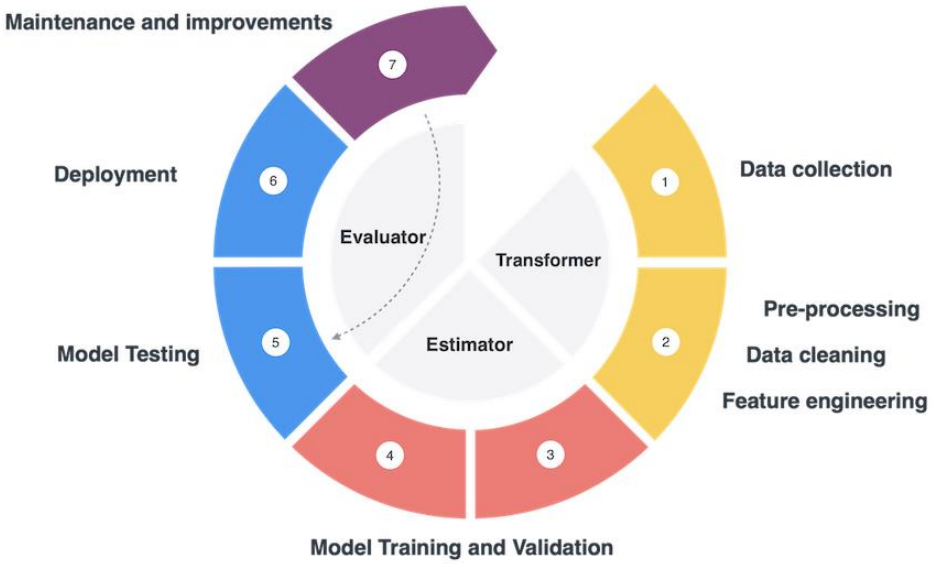
- *Ημιεποπτευόμενη Μάθηση (Semi-Supervised Learning):* Όταν η εξαγωγή σχετικών χαρακτηριστικών από τα δεδομένα είναι δύσκολη και η επισήμανση παραδειγμάτων χρονοβόρα, τότε η ημιεποπτευόμενη μάθηση αποδεικνύεται ιδιαίτερα χρήσιμη. Το σύνολο εκπαίδευσης περιέχει δείγματα που μπορεί να έχουν ή να μην έχουν ετικέτα, όπως για παράδειγμα στον εντοπισμό ενός όγκου ή μίας ασθένειας σε ιατρικές εικόνες αξονικής ή μαγνητικής τομογραφίας, ένας ακτινολόγος μπορεί να επισημάνει ένα μικρό υποσύνολο σαρώσεων και οι αλγόριθμοι ημιεποπτευόμενης μάθησης μπορούν να επωφεληθούν από αυτό το σχετικά μικρό ποσοστό επισημασμένων δειγμάτων και να βελτιώσουν την ακρίβειά τους.

- *Ενισχυτική Μάθηση (Reinforcement Learning):* Η ενισχυτική μάθηση προσεγγίζει περισσότερο τον τρόπο που οι άνθρωποι μαθαίνουν. Ο αλγόριθμός ή πράκτορας, όπως ονομάζεται, προσπαθεί να βρει τον βέλτιστο τρόπο για να επιτύχει έναν συγκεκριμένο στόχο και για κάθε ενέργεια που κάνει λαμβάνει μια θετική ή αρνητική ανταμοιβή. Μέσω της ανατροφοδότησης ο αλγόριθμός μαθαίνει και βελτιώνει την απόδοσή του, κάθε καινούργια επιλογή που κάνει βασίζεται τόσο στις ανταμοιβές προηγούμενων προσπαθειών, όσο και στην εξερεύνηση νέων τακτικών που μπορεί να έχουν καλύτερη απόδοση. Είναι ιδιαίτερα χρήσιμη μέθοδος για την εκπαίδευση ρομπότ και για την λήψη αποφάσεων σε πραγματικό χρόνο. Χαρακτηριστικό παραδείγματα αποτελεί η χρήση τους στο σχεδιασμό βιντεοπαιχνιδιών.

Κάθε μία από τις παραπάνω μεθοδολογίες συνοδεύεται και από ένα σύνολο αλγορίθμων (Linear Regression, Random Forest, KNN, DBSCAN, Support Vector Machine, Markov Decision Process, κλπ.). Αναφέρεται ότι το υποσύνολο των αλγορίθμων που στηρίζουν την λειτουργία τους σε νευρωνικά δίκτυα πολλών επιπέδων, είναι ευρέως γνωστό ως βαθιά

μάθηση (Deep Learning – DL). Η περιγραφή τέτοιων αλγορίθμων ξεφεύγει από το πλαίσιο της εργασίας, υπογραμμίζεται όμως ότι ο κλάδος DL αποτελεί υποσύνολο του ML (Σχήμα 7).

Αναπόσπαστο κομμάτι της μηχανικής μάθησης είναι ο σχεδιασμός ενός τρόπου κωδικοποίησης και αυτοματοποίησης της διαδικασίας εκπαίδευσης και βελτιστοποίησης των αλγορίθμων. Αυτό το κομμάτι συνήθως ονομάζεται αγωγός (pipeline) και ενσωματώνει όλες τις πρακτικές για την παραγωγή του μοντέλου, επιτρέπει την εφαρμογή πραγματικών σεναρίων χρήσης και συνήθως περιλαμβάνει εργασίες, που αφορούν: τη συλλογή και προεπεξεργασία δεδομένων, την εξαγωγή χαρακτηριστικών, την εκπαίδευση, αξιολόγηση και βελτιστοποίηση του μοντέλου (Σχήμα 10).

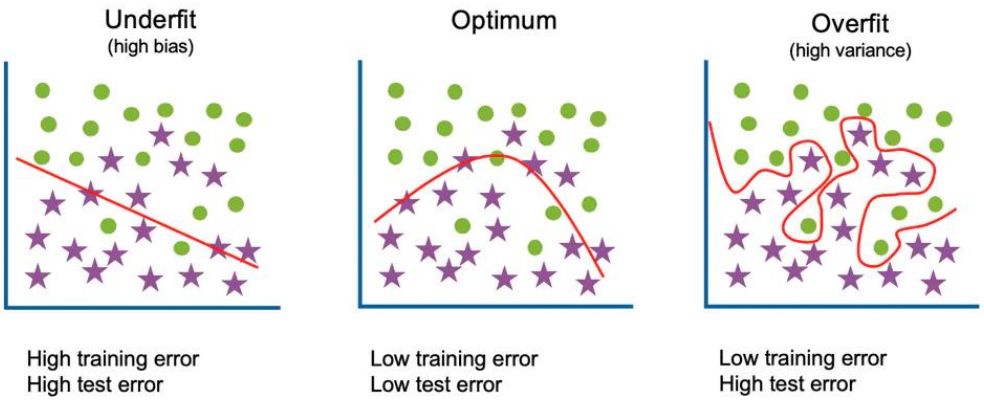


Σχήμα 10: Αγωγός Μηχανικής Μάθησης

Τέλος, σημειώνεται ότι σημαντικός στόχος των μοντέλων μηχανικής μάθησης είναι η γενίκευσή τους με σωστό τρόπο. Δηλαδή, η ικανότητά τους να προσαρμοστούν σε καινούργια δεδομένα [20]. Συχνά προβλήματα που παρουσιάζονται ως προς αυτή την κατεύθυνση και χρίζουν προσοχής είναι (Σχήμα 11):

- *Η υπερεκπαίδευση (Overfitting):* Όταν ένα μοντέλο κατά την διάρκεια της εκπαίδευσης θεωρεί εσφαλμένα δείγματα ή θόρυβο ως έγκυρες παρατηρήσεις. Έτσι, το μοντέλο μοντελοποιεί υπερβολικά καλά τα δεδομένα εκπαίδευσης, μη μπορώντας να ανταπεξέλθει σε καινούργια δείγματα.

- *Η υποεκπαίδευση (Underfitting):* Η έλλειψη επαρκούς αριθμού δειγμάτων ή η επιλογή λανθασμένου αλγορίθμου μπορεί να οδηγήσει στην δημιουργία μοντέλων που αδυνατούν να εντοπίσουν σημαντικές συσχετίσεις. Τα μοντέλα δεν μπορούν να βρουν τα χαρακτηριστικά εκείνα που θα βοηθήσουν στην επίλυση του προβλήματος και έτσι δυσκολεύονται να ανταπεξέλθουν τόσο στα δεδομένα εκπαίδευσης, όσο και σε καινούργια δεδομένα.



Σχήμα 11: Υπερεκπαίδευση & Υποεκπαίδευση

2.5 Ανίχνευση Ανωμαλιών

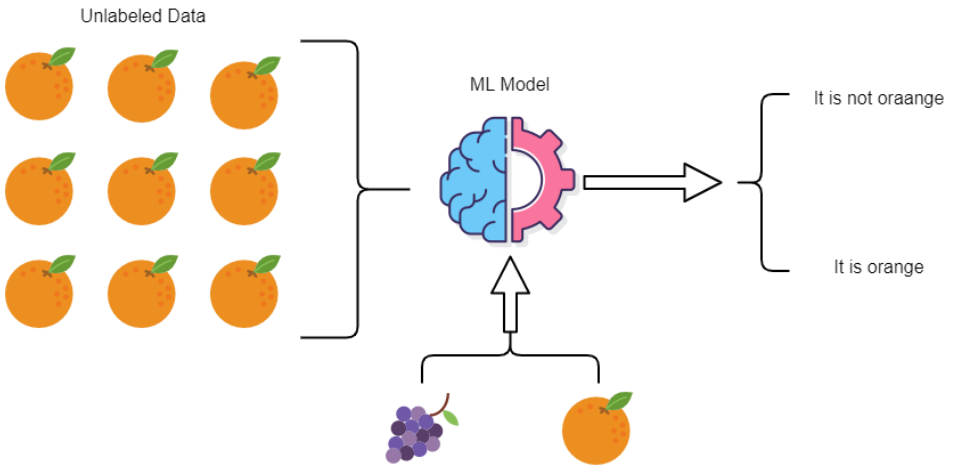
Ο όρος *ανίχνευση ανωμαλιών (anomaly detection)* αναφέρεται στις εφαρμογές που εξετάζουν εάν μια παρατήρηση ανήκει στο σύνολο κάποιων αρχικών παρατηρήσεων. Πολλές φορές συσχετίζεται με προβλήματα αυθεντικοποίησης και ασφάλειας, όπως για παράδειγμα την αντιμετώπιση οικονομικών απατών και την διάγνωση ασθενειών. Συχνά οι σχετικοί αλγόριθμοί αναφέρονται και ως ταξινομητές μίας κλάσης (One Class Classifiers) [21]. Ένας κλασικός ταξινομητής πολλών κλάσεων χρησιμοποιεί επισημασμένα δεδομένα εκπαίδευσης (supervised learning), με σκοπό να παράξει ένα μοντέλο που θα μπορεί να διακρίνει την κλάση μιας νέας παρατήρησης. Στην ανίχνευση ανωμαλιών θεωρείται ότι τα δεδομένα εκπαίδευσης ανήκουν σε μία μοναδική κλάση και το παραγόμενο μοντέλο πρέπει να είναι σε θέση να ξεχωρίσει αν μια νέα παρατήρηση ανήκει σε αυτήν ή όχι (Σχήμα 12).

Η ανίχνευση ανωμαλιών μπορεί να διαχωριστεί στις δύο παρακάτω υποκατηγορίες [22]:

- *Ανίχνευση Ακραίων Δειγμάτων (Outlier Detection):* Συχνά αναφέρεται και ως ανίχνευση ανωμαλιών χωρίς επίβλεψη (unsupervised), τονίζοντας ότι οι αντίστοιχοι

αλγόριθμοι διαχειρίζονται ένα μη επισημασμένο σύνολο δεδομένων. Όταν τα δεδομένα εκπαίδευσης περιέχουν ακραία δείγματα που απέχουν πολύ από τα υπόλοιπα, οι αλγόριθμοι ανίχνευσης ακραίων τιμών προσπαθούν να ανιχνεύσουν τις περιοχές μεγάλης πυκνότητας παρατηρήσεων και στην συνέχεια να αποκλείσουν τα δείγματα που δεν βρίσκονται σε αυτές. Κοινό πρόβλημα αποτελεί η αποθορυβοποίηση συνόλων δεδομένων, με σκοπό την παραγωγή αποτελεσματικότερων μοντέλων. Οι αλγόριθμοι που συχνά χρησιμοποιούνται είναι: το δάσος απομόνωσης (isolation forest), ο τοπικός παράγοντας ακραίας τιμής (local outlier factor – LOF) και η υπερβάλλουσα καμπύλη (elliptic envelope).

- *Ανίχνευση Ασυνήθιστων Δειγμάτων (Novelty Detection):* Σκοπός των αλγορίθμων αυτών είναι να αναγνωρίσουν εάν μία νέα παρατήρηση ανήκει στο σύνολο εκπαίδευσης ή όχι. Προσπαθούν να οριοθετήσουν μια περιοχή βάση του συνόλου εκπαίδευσης και στη συνέχεια εξετάζουν την σχέση της περιοχής με κάθε καινούρια παρατήρηση. Μόνο όταν το δείγμα βρίσκεται εντός της περιοχής, θεωρείται ότι ανήκει στο σύνολο των αρχικών παρατηρήσεων. Οι αλγόριθμοι αυτοί, αναφέρονται και ως αλγόριθμοι ανίχνευσης ανωμαλιών ημιεποπτευόμενης επίβλεψης (semi-supervised), καθώς τα δείγματα του συνόλου εκπαίδευσης είναι μη επισημασμένα. Σε τέτοια προβλήματα, η καθαρότητα του συνόλου εκπαίδευσης παίζει καθοριστικό ρόλο στην αποτελεσματικότητα του τελικού μοντέλου, η ύπαρξη λοιπόν καθόλου ή ελάχιστου θορύβου είναι αρκετά σημαντική. Οι πιο συχνοί μηχανισμοί που καλούνται να λύσουν τέτοια προβλήματα, είναι τα διανύσματα υποστήριξης μίας κλάσης (One Class Support Vector Machine – OCSVM). Κοινά προβλήματα αποτελούν η αυθεντικοποίηση χρηστών, όπου η συλλογή δεδομένων από κάθε πιθανό παραβάτη είναι αδύνατη.

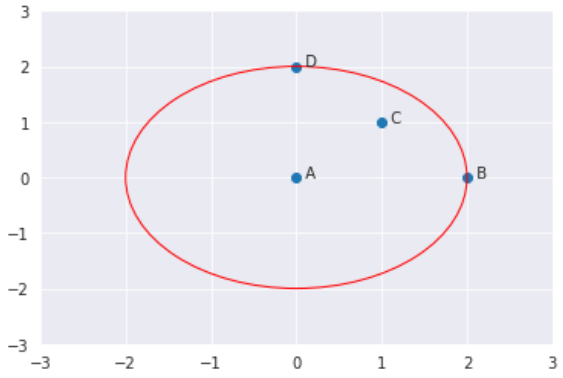


Σχήμα 12: Ταξινομητής Μίας Κλάσης

2.5.1 Local Outlier Factor – LOF

Ο τοπικός συντελεστής ακραίων τιμών (Local Outlier Factor - LOF) είναι ένας αλγόριθμος, που συνήθως χρησιμοποιείται για outlier detection σε σύνολα δεδομένων [23]. Ο αλγόριθμος αυτός χαρακτηρίζει ένα δείγμα ως ακραίο λαμβάνοντας υπόψη την πυκνότητα της γειτονιάς του και συνεπώς αποδίδει καλά, όταν η πυκνότητα των παρατηρήσεων δεν είναι η ίδια σε όλο το σύνολο δεδομένων. Για να γίνει κατανοητός ο τρόπος λειτουργίας του, πρέπει να αποσαφηνιστούν οι έννοιες:

- *k-Απόσταση & k-Γείτονες (k-Distance & k-Neighbors):* Η k-απόσταση είναι η απόσταση (Ευκλείδεια, Μανχάταν, κ.λπ.) μεταξύ του σημείου και του πλησιέστερου k-γείτονα. Οι k-γείτονες συμβολίζονται με N_k και είναι το σύνολο σημείων που βρίσκονται μέσα ή πάνω στον κύκλο με ακτίνα ίση με την k-απόσταση. Για παράδειγμα, τέσσερα σημεία A, B, C και D (Σχήμα 13). Αν k=2, οι k-γείτονες του A θα είναι C, B και D, δηλαδή $||N_2(A)||=3$.



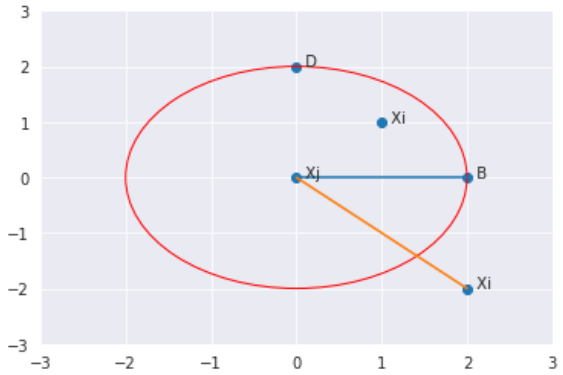
Σχήμα 13: k-Απόσταση & k-Γείτονες (k=2)

- *Απόσταση Προσβασιμότητας (Reachability Distance – RD):* Απόσταση προσβασιμότητας του Xj από το Xi, ορίζεται ως το μέγιστο της k-απόστασης του Xj και της απόστασης των δύο σημείων (Εξ. 1).

$$RD(Xi, Xj) = max(kDistance(Xj), Distance(Xi, Xj)) \quad (Εξ.\ 1)$$

Σε απλούς όρους, εάν ένα σημείο Xi βρίσκεται εντός των k-γειτόνων του Xj, η απόσταση προσβασιμότητας θα είναι η k-απόσταση του Xj (μπλε γραμμή),

διαφορετικά η απόσταση προσβασιμότητας θα είναι η απόσταση μεταξύ Xi και Xj (πορτοκαλί γραμμή) (Σχήμα 14).



Σχήμα 14: Απόσταση Προσβασιμότητας

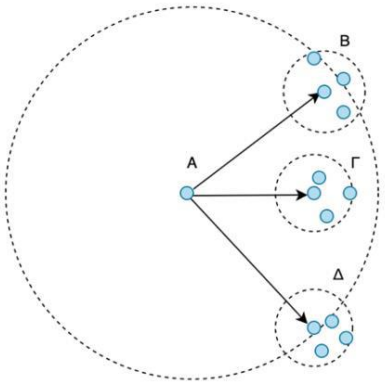
- *Τοπική Πυκνότητα Προσβασιμότητας (Local Reachability Density – LRD):* Ορίζεται ως το αντίστροφο της μέσης απόστασης προσβασιμότητας του A από τους γείτονές του (Εξ. 2). Σύμφωνα με τον τύπο, όσο μεγαλύτερη είναι η μέση απόσταση προσβασιμότητας, τόσο μικρότερη η πυκνότητα των σημείων γύρω από ένα συγκεκριμένο σημείο. Άρα, μια μικρή τιμή LDR δείχνει ότι οι γείτονες του σημείου βρίσκονται μακριά.

$$LDR_k(A) = \frac{1}{\sum_{Xj \in N_k(A)} \frac{RD(A,Xj)}{||\mathrm{N_k(A)}||}} \quad \textit{(Εξ. 2)}$$

Κατανοώντας τις παραπάνω έννοιες, ως LOF ορίζεται ο λόγος του μέσου όρου LRD των k-γειτόνων του A προς το LRD του A (Εξ. 3). Εάν το σημείο δεν είναι ακραίο (inlier), ο μέσος όρος LRD των k-γειτόνων είναι περίπου ίσος με το LRD του σημείου και το LOF είναι σχεδόν ίσο με 1. Από την άλλη πλευρά, εάν το σημείο είναι ακραίο (outlier), το LRD ενός σημείου είναι μικρότερο από το μέσο LRD των k-γειτόνων και συνεπώς η τιμή LOF θα είναι υψηλή. Γενικά, εάν LOF>1, το σημείο θεωρείται ακραίο, ωστόσο μερικές φορές χρειάζεται να γίνει σύγκριση της LOF τιμής του, με την μέγιστη τιμή LOF όλων των σημείων.

$$LOF_k(A) = \frac{\sum_{Xj \in N_k(A)} LRD_k(Xj)}{||\mathrm{N_k(A)}||} \times \frac{1}{LRD_k(A)} \quad \textit{(Εξ. 3)}$$

Σημαντικό πλεονέκτημα είναι η ικανότητα προσδιορισμού τοπικών ακραίων τιμών. Μπορεί να ανιχνεύσει outliers που βρίσκονται σε πολύ μικρή απόσταση από κάποιο σύμπλεγμα σημείων, όταν άλλες προσεγγίσεις αποτυγχάνουν.



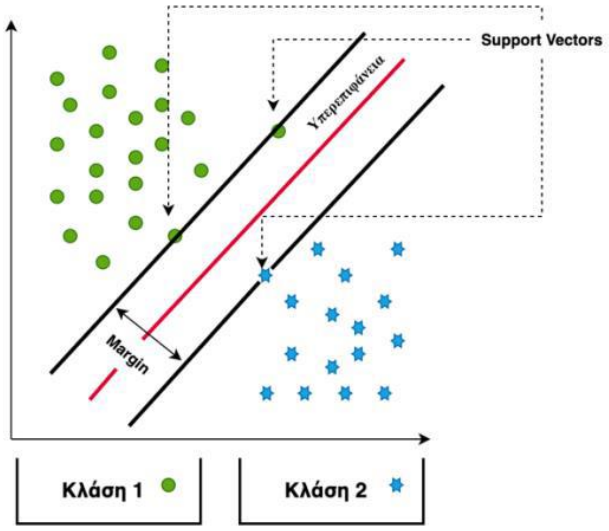
Σχήμα 15: Local Outlier Factor – LOF

2.5.2 Support Vector Machine – SVM

Μια βασική διανυσματική μηχανή υποστήριξης χρησιμοποιείται κυρίως για προβλήματα ταξινόμησης [24]. Για παράδειγμα, σε ένα πρόβλημα ταξινόμησης δύο κλάσεων, ο στόχος του SVM είναι η εύρεση ενός γραμμικού υπερεπιπέδου, το οποίο θα διαχωρίζει τις παρατηρήσεις των δύο κλάσεων. Τα υπερεπίπεδα που ικανοποιούν αυτή την συνθήκη θεωρητικά είναι άπειρα, ωστόσο ο SVM φροντίζει να επιλέγει εκείνο το υπερεπίπεδο που διαχωρίζει τα δεδομένα με βέλτιστο τρόπο (Σχήμα 16). Αναλυτικότερα ο αλγόριθμος προσπαθεί να βρει ένα υπερεπίπεδο διαχωρισμού το οποίο:

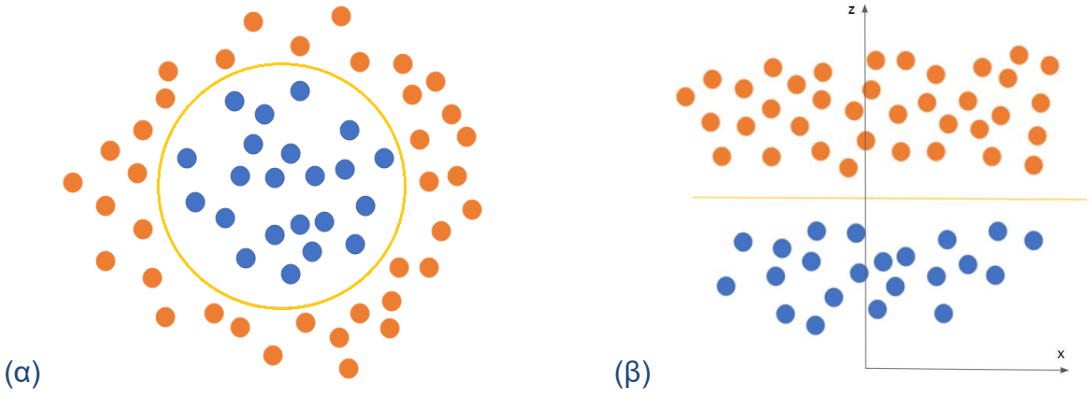
1. Ισαπέχει από τα πλησιέστερα διανύσματα των δύο κλάσεων, γνωστά ως διανύσματα υποστήριξης (support vectors).

2. Μεγιστοποιεί την απόσταση των διανυσμάτων υποστήριξης, γνωστή ως περιθώριο (margin).



Σχήμα 16: Support Vector Machine 2 Κλάσεων

Ωστόσο, στην πραγματικότητα τα περισσότερα προβλήματα δεν είναι γραμμικά αλλά τα SVMs έχουν την δυνατότητα να δημιουργούν μη γραμμικά όρια απόφασης, προβάλλοντας τα δεδομένα σε μεγαλύτερες διαστάσεις. Πιο συγκεκριμένα, χρησιμοποιείται μια συνάρτηση πυρήνα (kernel), για να προβάλλει τις παρατηρήσεις σε έναν χώρο μεγαλύτερων διαστάσεων που μπορεί να πραγματοποιηθεί γραμμικός διαχωρισμός (Σχήμα 17).



(α) (β)

Σχήμα 17: Μη γραμμική ταξινόμηση, (α) Χώρος παρατηρήσεων, (β) Χώρος διαχωρισμού

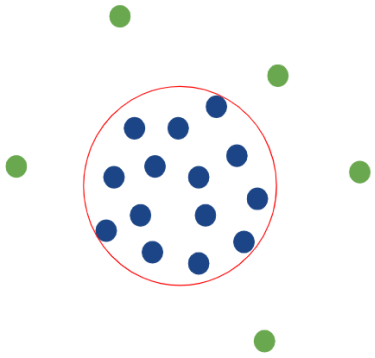
2.5.2.1 One Class Support Vector Machine – OCSVM

Αν και η παραπάνω λογική αποδεικνύεται αποτελεσματική σε προβλήματα κλασικής ταξινόμησης, χρειάζεται να υπάρξουν αλλαγές για να είναι δυνατή η εφαρμογή της σε προβλήματα novelty detection. Υπάρχουν αρκετές εναλλακτικές για την υλοποίηση του

αλγορίθμου στην πράξη [25], ωστόσο οι επικρατέστερες προσεγγίσεις αναφέρονται παρακάτω:

- Σύμφωνα με τους Schölkopf κ.ά. [26]: Όπως και στα κλασσικά SVMs, γίνεται η απεικόνιση των παρατηρήσεων σε χώρο περισσότερων διαστάσεων με σκοπό όμως τον διαχωρισμό περιοχών χαμηλής και υψηλής πυκνότητας. Η μέθοδος υλοποιείται με την κατασκευή ενός υπερεπιπέδου σε μέγιστη απόσταση από την αρχή των αξόνων του χώρου, που μπορεί να διαχωρίσει τις περιοχές που δεν περιέχουν δεδομένα. Τα δείγματα που βρίσκονται κοντά στην αρχή των αξόνων και κάτω από το υπερεπίπεδο ανήκουν σε περιοχές χαμηλότερης πυκνότητας και συνεπώς θεωρούνται ακραία (outliers), ενώ τα υπόλοιπα ανήκουν στην κλάση ενδιαφέροντος (inliers). Σημαντική παράμετρος της μεθόδου είναι η μεταβλητή *nu*, η οποία ορίζει το ποσοστό ακραίων τιμών στα δεδομένα και συνεπώς την σκληρότητα ή την απαλότητα του υπερεπιπέδου γύρω από τα δεδομένα.

- Σύμφωνα με τους Tax κ.ά. [27]: Σε αυτή την προσέγγιση, αντί για υπερεπίπεδο, κατασκευάζεται μια υπερσφαίρα που περικλείει σχεδόν όλα τα δεδομένα της θετικής κλάσης. Στόχο είναι η ελαχιστοποίηση του τετραγώνου της ακτίνα της υπερσφαίρας, μεγιστοποιώντας έτσι το όριο μεταξύ της κλάσης και των υπόλοιπων περιπτώσεων. Αυτή η μέθοδος ονομάζεται περιγραφή διανυσματικών δεδομένων υποστήριξης (*Support Vector Data Description – SVDD*) και θεωρεί ένα δείγμα ως ακραίο εάν βρίσκεται εκτός της υπερσφαίρας (Σχήμα 18).



Σχήμα 18: Support Vector Data Description

Συνεπώς, η ελαχιστοποίηση της ακτίνας ενός SVDD μπορεί να οδηγήσει στην απόρριψη ενός μέρους των θετικά επισημασμένων δεδομένων. Η χρήση kernel διαφορετικού τύπου και μεγέθους κάνει πιο ευέλικτο ένα τέτοιο σύστημα. Αδυναμία

παρουσιάζεται όταν σε σύνολα μεγάλων διαστάσεων υπάρχουν δεδομένα με μεγάλη διακύμανση πυκνότητας.

Από τα παραπάνω προκύπτει πως το είδος συνάρτησης πυρήνα είναι σημαντικό για την αποτελεσματικότητα και των δύο μεθοδολογιών. Ένας kernel μπορεί να είναι γραμμικός, πολυωνυμικός, σιγμοειδής ή Γκαουσιανός (Gaussian) αλλιώς, ακτινωτής βάσης (Radial Basis Function – RBF). Και στις δύο μεθόδους αποδεικνύεται ότι ο RBF αποδίδει καλύτερα σε μεγαλύτερο πλήθος προβλημάτων, καθώς φαίνεται να προσαρμόζεται ικανοποιητικά σε δεδομένα, τα όρια των οποίων δεν είναι γραμμικά. Σημειώνεται ότι κατά την εκπαίδευση RBF-SVM πρέπει να δίνεται προσοχή στην παράμετρο *gamma*. Η παράμετρος gamma καθορίζει την επιρροή που έχει ένα δείγμα εκπαίδευσης στη συνάρτηση διαχωρισμού. Εάν το gamma είναι μεγάλο μπορεί να δημιουργηθούν προβλήματα overfitting, ενώ αν είναι μικρό τότε η επιρροή των παρατηρήσεων είναι μικρή και το μοντέλο συμπεριφέρεται παρόμοια με ένα γραμμικό μοντέλο, αποτελούμενο από υπερεπίπεδα που διαχωρίζουν περιοχές υψηλής πυκνότητας [28].

2.6 Μετρικές Αξιολόγησης Αυθεντικοποίησης

Αναπόσπαστο βήμα της ανάπτυξης ενός συστήματος είναι η αξιολόγησή του. Αναμφισβήτητα, ο τελικός χρήστης κρίνει το σύστημα, ωστόσο τις περισσότερες φορές είναι αναγκαίο να πραγματοποιηθεί μια πρώτη εκτίμηση της απόδοσης, πριν το σύστημα ολοκληρωθεί. Συνήθως αυτό επιτυγχάνεται με την χρήση μετρικών, δηλαδή τιμών που βασίζονται σε κάποιο μαθηματικό τύπο ή διαδικασία και ποσοτικοποιούν την ικανότητα του συστήματος να εκτελεί σωστά το έργο του. Στα μαθηματικά, στην στατιστική και στην μηχανική μάθηση υπάρχει μια τεράστια γκάμα μετρικών που χρησιμοποιείται σε διαφορετικά προβλήματα. Η επιλογή μετρικών που δίνουν μια σχετική με το πρόβλημα απάντηση, καθώς και ο ορισμός ενός αποδεκτού εύρους τιμών για αυτές είναι ιδιαίτερα σημαντικά για την σωστή αξιολόγηση και βελτιστοποίηση του τελικού συστήματος.

Στα συστήματα έμμεσης αυθεντικοποίησης τα βασικά ζητούμενα είναι η ασφάλεια και ευχρηστία. Ένα CIA σύστημα για smartphones θα πρέπει να είναι σε θέση να εντοπίζει άμεσα οποιαδήποτε παραβατική ενέργεια και να κλειδώνει την συσκευή, αλλά ταυτόχρονα να μην εμποδίζει τον πραγματικό χρήστη όταν διεκπεραιώνει διάφορες διεργασίες. Ως προς αυτή την κατεύθυνση, οι δύο παρακάτω μετρικές είναι από τις σημαντικότερες για την αξιολόγηση τέτοιων συστημάτων:

- *Ποσοστό Λανθασμένης Αποδοχής (False Acceptance Rate – FAR):* Το ποσοστό των φορών που το σύστημα παρείχε πρόσβαση σε μη εξουσιοδοτημένο άτομο ((Εξ. 4).

$$FAR = \frac{Αριθμός\ αποδεκτών\ ενεργείων\ κακόβουλου\ χρήστη}{Συνολικός\ αριθμός\ ενεργειών\ κακόβουλου\ χρήστη} \quad (Εξ.\ 4)$$

- *Ποσοστό Λανθασμένης Απόρριψης (False Rejection Rate – FRR):* Το ποσοστό των φορών που το σύστημα δεν παρείχε πρόσβαση σε εξουσιοδοτημένο άτομο ((Εξ. 5).

$$FRR = \frac{Αριθμός\ μη\ αποδεκτών\ ενεργείων\ πραγματικού\ χρήστη}{Συνολικός\ αριθμός\ ενεργειών\ πραγματικού\ χρήστη} \quad (Εξ.\ 5)$$

Ιδανική λύση στο πρόβλημα της αυθεντικοποίησης θα ήταν ο ταυτόχρονος μηδενισμός αυτών των δύο μετρικών. Ωστόσο, η ποιότητα δεδομένων αλλά και φύση του προβλήματος κάνουν κάτι τέτοιο μη εφικτό. Όπως θα φανεί και από τα πειράματα, αυτές οι μετρικές είναι αντιστρόφως ανάλογες και η μείωση της μίας οδηγεί στην αύξηση της άλλης. Επομένως, όπως είδη αναφέρθηκε, το πρόβλημα της αυθεντικοποίησης ανάγεται στην ταυτόχρονη επίτευξη ποσοστών FAR και FRR όσο πιο κοντά στο μηδέν γίνεται.

3 Επισκόπηση Ερευνητικής Περιοχής

Το τελευταίο διάστημα, η συνεχής – έμμεση αυθεντικοποίηση έχει αποκτήσει αυξημένο ενδιαφέρον. Πολυάριθμες μελέτες έχουν εξερευνήσει διαφορετικές μεθοδολογίες και τεχνολογίες για τη μοντελοποίηση της συμπεριφοράς των χρηστών. Με την ανάπτυξη των μέσων αποθήκευσης και υπολογισμών, καθώς και με τη συχνότερη ενσωμάτωση αισθητήρων στα smartphones, ο έλεγχος ταυτότητας με συμπεριφορικά χαρακτηριστικά έχει γίνει ιδιαίτερα αποτελεσματικός.

Η εξερεύνηση επιστημονικών δημοσιεύσεων είναι απαραίτητη για την υιοθέτηση μεθοδολογίας αλλά και την εξοικείωση με έννοιες και τεχνικές. Επιπλέον, οι υπάρχουσες έρευνες προσφέρουν χρήσιμες πληροφορίες για πιθανά προβλήματα που μπορεί να παρουσιαστούν και διαμορφώνουν ένα επίπεδο αντικειμενικής αξιολόγησης. Στην ενότητα αυτή παρουσιάζονται κάποιες από τις μελέτες που αποτέλεσαν βάση για την προκείμενη εργασία. Για τον σκοπό αυτό και παρόμοια με το [29], οι έρευνες διαχωρίζονται σε 4 κατηγορίες βάσει των δεδομένων που χρησιμοποιούν για να πραγματοποιήσουν τον έλεγχο. Τα δεδομένα αυτά είναι:

- Δεδομένα Κίνησης (Motion): Η κατηγορία αυτή περιλαμβάνει μεθοδολογίες που προϋποθέτουν την συλλογή δεδομένων από αισθητήρες κίνησης (επιταχυνσιόμετρο, γυροσκόπιο, κλπ.) και ο έλεγχος βασίζεται στην μοντελοποίηση των κινήσεων του χρήστη κατά την αλληλεπίδραση με το smartphone.

  Προς αυτή την κατεύθυνση, οι Amini κ.ά. [30] παρουσίασαν το DeepAuth, στο οποίο εξέτασαν την απόδοση Long Short Term Memory (LSTM) δικτύων σε δεδομένα 47 χρηστών που συλλέχθηκαν με ελεγχόμενο τρόπο. Τα πειράματα έδειξαν ότι σε χρονικό περιθώριο 20 δευτερολέπτων το σύστημα πετυχαίνει ακρίβεια 96,7%. Οι Lee κ.ά. [31] δημιουργώντας ένα σύστημα βασισμένο σε SVM, απέδειξαν ότι ο συνδυασμός δεδομένων από περισσότερους αισθητήρες μπορεί να βελτιώσει τα αποτελέσματα. Ομοίως, οι Li κ.ά. χρησιμοποιώντας ταυτόχρονα δεδομένα γυροσκοπίου και επιταχυνσιομέτρου, δημιουργήσαν τα συστήματα SensorAuth [32] και SCANet [33]. Τα δεδομένα τους αποκτήθηκαν με ελεγχόμενο τρόπο, ωστόσο και οι δύο μελέτες ερευνούν σε βάθος παραμέτρους που επηρεάζουν την αποτελεσματικότητα. Το πρώτο σύστημα βασισμένο σε SVM πέτυχε Equal Error Rate (EER) 4,66% σε παράθυρο 5 δευτερολέπτων, ενώ το δεύτερο με Νευρωνικό Δίκτυο (Neural Network – NN) ακρίβεια 90,04% και ERR 5,14% σε παράθυρο 3 δευτερολέπτων. Ιδιαίτερη προσοχή δόθηκε και στην έρευνα της Τσίντζηρα [34], όπου χρησιμοποιώντας ταυτόχρονα δεδομένα γυροσκοπίου και επιταχυνσιομέτρου αλλά και μελετώντας την

αποτελεσματικότητα διάφορων αλγορίθμων, κατάφερε να πετύχει μέσο FRR 5,38% και 6,74% και μέσο FAR 4,34% και 2,02% με OCSVM και LOF αντίστοιχα. Τα αποτελέσματα αυτά είναι πολύ σημαντικά και αξιόπιστα, καθώς τα δεδομένα προέρχονται από το σύνολο δεδομένων του BrainRun [35] και είναι αρκετά κοντά σε δεδομένα πραγματικών συνθηκών.

- Δεδομένα Βαδίσματος (Gait): Σε αυτή την κατηγορία περιλαμβάνονται συστήματα ελέγχου που βασίζονται στην αναγνώριση του τρόπου βαδίσματος. Στα smartphones η απόκτηση τέτοιων δεδομένων συχνά γίνεται με χρήση αισθητήρων κίνησης ή/και άλλων συσκευών (wearables), που ο χρήστης πρέπει να τοποθετήσει σε συγκεκριμένα σημεία στο σώμα του.

  Στην λογική αυτή, οι Gafurov κ.ά. [36] ανέλυσαν την απόδοση ενός συστήματος, που χρησιμοποιεί μια εξωτερική συσκευή, η οποία μπορεί να τοποθετηθεί σε 4 διαφορετικά σημεία (αστράγαλος, ισχίο, τσέπη, μπράτσο). Τα πειράματα που πραγματοποιήθηκαν σε ικανοποιητικό πλήθος χρηστών, κατάφεραν να πετύχουν EER 5%, χρησιμοποιώντας k-Nearest Neighbors (kNN) και με την συσκευή τοποθετημένη στο πόδι. Σε αντίθεση, οι Hoang κ.ά. [37], [38] συνέλεξαν δεδομένα βαδίσματος από το ενσωματωμένο επιταχυνσιόμετρο των smartphones. Τα πειράματα πραγματοποιήθηκαν με δεδομένα από συγκεκριμένες συσκευές και σχετικά μικρό πλήθος χρηστών, ωστόσο τα αποτελέσματά τους είναι αρκετά καλά, υπογραμμίζοντας την αποτελεσματικότητα των SVMs και εισάγοντας την ιδέα μιας πολυτροπικής προσέγγισης.

- Δεδομένα Πληκτρολόγησης (Keystroke): Καθώς το πληκτρολόγιο αποτελεί συσκευή εισόδου για τεράστιο πλήθος συσκευών, η ένταξή του σε μηχανισμούς αυθεντικοποίησης ήταν μια ιδέα που εξαρχής αποσκοπούσε στον έμμεσο και συνεχή έλεγχο.

  Έτσι, οι Buriro κ.ά. [39] σχεδίασαν ένα σχήμα ελέγχου βασισμένο στις κινήσεις των χεριών του χρήστη κατά την αλληλεπίδρασή του με 10 πλήκτρα. Οι συγγραφείς συνέλεξαν δεδομένα από 97 χρήστες μέσω εφαρμογής που ανέπτυξαν και στην συνέχεια διεξήγαγαν πειράματα, πετυχαίνοντας ακρίβεια 85,77% και FAR 7,32%. Ομοίως, οι Zahid κ.ά. [40] μελέτησαν τη συμπεριφορά πληκτρολόγησης 25 χρηστών, μέσω εφαρμογής που ανέπτυξαν και εισήγαγαν μεγάλη ποικιλία χαρακτηριστικών, προτείνοντας έναν ασαφή ταξινομητή και πετυχαίνοντας μηδενικό FRR και FAR 2%. Τέλος, οι Giuffrida κ.ά. [41] δοκιμάζοντας τον συνδυασμό δεδομένων πληκτρολόγησης

και αισθητήρων κίνησης κατέληξαν στο ότι τα δεδομένα που προκύπτουν από την χρήση των αισθητήρων είναι πιο χρήσιμα όσον αφορά τον έλεγχο ταυτότητας.

- Δεδομένα Αφής (Touch): Όπως και το πληκτρολόγιο, πλέον η οθόνη αφής αποτελεί αναπόσπαστο κομμάτι πολλών ηλεκτρονικών συσκευών. Η διαφορά είναι πως η οθόνη αφής παρέχει περισσότερες λειτουργίες και συνήθως αποτελεί τον μοναδικό τρόπο αλληλεπίδρασης με την συσκευή. Έτσι, η χρήση χειρονομιών επιτρέπει την εφαρμογή συνεχούς – έμμεσης αυθεντικοποίησης σε μια ποικιλία συσκευών (smartwatches, ψηφιακές κάμερες, συστήματα πλοήγησης και οθόνες) με οικονομικό τρόπο.

  Στην κατεύθυνση αυτή, οι Antal κ.ά. [42] έδωσαν βαρύτητα στα swipes και μελέτησαν τα χαρακτηριστικά τους, χρησιμοποίησαν δεδομένα από 40 χρήστες που συλλέχθηκαν κατά την διάρκεια συμπλήρωσης ενός ερωτηματολογίου και παρουσίασαν αποτελέσματα με EER 0,004% για αλγορίθμους Random Forests. Οι Khan και Hengartner [43], συλλέγοντας δεδομένα από 32 χρήστες έδειξαν ότι η επίγνωση του περιεχομένου την οθόνης (context-aware) βελτιώνει την ακρίβεια. Επιπλέον, οι Karanikiotis κ.ά. [44] χρησιμοποιώντας SVMs, πρότειναν μια αρχιτεκτονική πολλαπλών μοντέλων που συνεργάζονται μεταξύ τους και εξασφαλίζουν την ικανότητα του συστήματος για γενίκευση. Επιπροσθέτως, υπογράμμισαν την ανάγκη για την δημιουργία ενός συστήματος που θα συμπεριλαμβάνει ένα υποσύστημα εμπιστοσύνης, λαμβάνοντας υπόψιν μία σειρά χειρονομιών. Στην υλοποίηση τους τα διάφορα μοντέλα, με την απόφασή τους, μεταβάλλουν τα επίπεδα εμπιστοσύνης και αναλόγως πραγματοποιείται το κλείδωμα της συσκευής. Τα αποτελέσματά τους ήταν ιδιαίτερα ικανοποιητικά και μάλιστα σημειώνεται ότι τα δεδομένα που χρησιμοποίησαν προέρχονται από το σύνολο BrainRun [35], που δημιούργησαν οι ίδιοι και προσομοιώνει ικανοποιητικά δεδομένα πραγματικών συνθηκών. Σε παρόμοιο πλαίσιο κινήθηκε και η Παλάζη [45], η οποία εφαρμόζοντας πολλαπλά μοντέλα SVMs και υιοθετώντας το υποσύστημα εμπιστοσύνης κατάφερε να πετύχει, για το ίδιο σύνολο δεδομένων, μέσο FAR 2,46%, ενώ είναι σε θέση να εντοπίσει έναν μη εξουσιοδοτημένο χρήστη από αρκετά μικρό αριθμό χειρονομιών.

Πέραν όμως αυτών των κατηγοριών, όλο και πιο δημοφιλής γίνεται ο έλεγχος ταυτότητας πολλών παραγόντων (multimodal). Πρόκειται για συστήματα που προσφέρουν ισχυρά και ακριβή αποτελέσματα, παρέχοντας μια ασφαλή και ευέλικτη μέθοδο για έλεγχο ταυτότητας, λαμβάνοντας υπόψη πιθανές αλλαγές στα δεδομένα. Η σχεδίαση τέτοιων συστημάτων

αποτελεί εφικτή λύση στα smartphones, καθώς η ποικιλία αισθητήρων επιτρέπει την ανάγνωση πολλών βιομετρικών χαρακτηριστικών. Η υλοποίησή τους μπορεί να γίνει τόσο σε επίπεδο χαρακτηριστικών, όπου τα χαρακτηριστικά από διάφορα βιομετρικά δεδομένα συγκεντρώνονται για την δημιουργία ενός ενιαίου μοντέλου μηχανικής μάθησης, όσο και σε αλγοριθμικό επίπεδο ή/και σε επίπεδο απόφασης. Δηλαδή, το σύστημα μπορεί να περιέχει ένα σύνολο αλγορίθμων και μοντέλων, ανάλογο της ποικιλίας των δεδομένων. Κάθε μοντέλο διαχειρίζεται δεδομένα συγκεκριμένου είδους, ενώ στην συνέχεια συνεργάζονται όλα μαζί για να πάρουν μια κοινή απόφαση.

Παράδειγμα τέτοιων συστημάτων αποτελεί το RiskCog, όπου οι Zhu κ.ά. [46] πρότειναν μια μέθοδο βασισμένη σε SVM, που μπορεί να επικυρώσει τους χρήστες μέσα σε 3,2 δευτερόλεπτα, χρησιμοποιώντας δεδομένα από αισθητήρες smartphones και smartwatches. Τα πειράματα διεξήχθησαν σε μεγάλο πλήθος χρηστών και οι συγγραφείς αναφέρουν μέση ακρίβεια συστήματος 93,8% και 9,.6% για σταθερούς και κινούμενους χρήστες, αντίστοιχα. Ομοίως, οι Lee κ.ά. [47] πρότειναν το SmarterYou, ένα σύστημα βασισμένο στο συνδυασμό μετρήσεων smartphones, wearables και περιεχομένου οθόνης. Τα πειράματά τους, σε ένα σύνολο 35 χρηστών, έδειξαν ακρίβεια 98,1%, FRR 0,9% και FAR 2,8% σε ένα παράθυρο ελέγχου 6 δευτερολέπτων. Οι Liang κ.ά. [48] πρότειναν ένα σύστημα βασισμένο σε δεδομένα αισθητήρων και αφής. Αφού συγκέντρωσαν δεδομένα 20 χρηστών, από συγκεκριμένες συσκευές, δοκίμασαν πλήθος αλγορίθμων και κατάφεραν ακρίβεια 95,96%, FRR 2,55% και FAR 6,94%. Ο Feng κ.ά. συνδύασαν δεδομένα αφής, με δεδομένα από wearables [49] και με context-aware τεχνικές [50]. Το πρώτο, γνωστό ως FAST αξιολογήθηκε σε 40 χρήστες πετυχαίνοντας FAR 4,66% και FRR 0,13%. Το δεύτερο, γνωστό ως TIPS αξιολογήθηκε σε ελεγχόμενο περιβάλλον με 100 χρήστες πετυχαίνοντας ακρίβεια 90%.

Στο παρακάτω πίνακα (Πίνακας 1) παρουσιάζονται, συγκεντρωτικά, κάποιες από τις παραπάνω έρευνες:

Πίνακας 1: Συγκεντρωτικά Μελέτες Ερευνητικής Περιοχής

Study	Modalities	Sensors	Classifiers	#Users	ERR (%)	FAR (%)	FRR (%)	Accuracy (%)	Auth. Time (ms)	Platform
[33]	Free Motion	Ac, Gy	LSTM	47	-	-	-	96,70	$20*10^3$	GoogleNexus5X (A-8.1)
[34]	Free Motion	Ac, Ma, Or	SVM	4	-	-	-	90,00	$20*10^3$	GoogleNexus5 (A-4.4)
[35]	Free Motion	Ac, Gy	SVM	100	8,33	-	-	-	$5*10^3$	Samsung GalaxyS4 (A-4.4)
[36]	Free Motion	Ac, Gy	SVM	100	2,35	-	-	-	$3*10^3$	-
[37]	Free Motion	Ac, Gy	SVM	14	-	4,34	5,38	-	-	-
			LOF		-	2,02	6,74	-	-	
[39]	Gait	MRC – Ankle	k-NN	21	5,00	-	-	85,70	-	-
		MRC – Hip		100	13,00	-	-	73,20	-	
		MRC – Pocket		50	7,30	-	-	86,30	-	
		MRC – Arm		30	10,00	-	-	71,70	-	
[40]	Gait	Ac	SVM	11	-	-	-	92,70	-	GoogleNexusOne (A-2.1)
[41]	Gait	Ac	SVM	14	-	-	-	91,33	-	LGOptimusG (A-4.1.2)
[42]	Keystrokes	-	MLP	97	-	11,72	29,16	-	-	-
[43]	Keystrokes	-	Distance	25	4,00	-	-	-	632-2151	Samsung SCH-V740 (NA)
[44]	Keystrokes	Ac, Gy	k-NN	20	0,08	-	-	-	200	-
[45]	Swipes	Or	RF	40	0,20	-	-	-	-	GoogleNexus7 (A-4.1.2)
[47]	Swipes	-	SVM	2.221	-	-	2,33	-	-	-
[49]	Wearables & Motion	Ac, Gy, Gr	SVM	1.513	-	-	-	95,57	$3,2*10^3$	Computer Simulation
[50]	Wearables & Motion	Ac, Gy, Ma, Or, Li	KRR	35	-	2,80	3,90	98,10	-	GoogleNexus5 (A-4.0)

Ac: Accelerometer, Gy: Gyroscope, Ma: Magnetometer, Or: Orientation, Gr: Gravity, Li: Light
k-NN: k-Nearest Neighbor, SVM: Support Vector Machine, LSTM: Long Sort Term Memory, CC: Cross Correlation, FC: Fuzzy Commitment, RF: Random Forest, MLP: Multilayer Perceptron

Όπως φαίνεται, οι έρευνες στο συγκεκριμένο πρόβλημα είναι πολυάριθμες και η κάθε μία εισάγει τα δικά της στοιχεία. Προκύπτει λοιπόν, πως η συνεχής – έμμεση αυθεντικοποίηση είναι εφαρμόσιμη και μπορεί να φέρει ικανοποιητικά αποτελέσματα. Ιδιαίτερα η χρήση ή/και ο συνδυασμός βιομετρικών χαρακτηριστικών, έχει οδηγήσει στην ανάπτυξη συστημάτων που φαίνεται να καλύπτουν, τόσο τις ανάγκες ασφάλειας όσο και χρηστικότητας. Ωστόσο, εκτός των θετικών συμπερασμάτων γεννούνται και κάποιοι προβληματισμοί, που αφορούν:

- Τα συστήματα που στηρίζονται σε δεδομένα από wearables, καθώς είναι πιθανό να αναγκάσουν τον χρήστη να αγοράσει μία δευτερεύουσα συσκευή, αν θέλει να ασφαλίσει περαιτέρω το smartphone του.

- Αποτελέσματα ερευνών που στηρίχθηκαν σε δεδομένα λίγων χρηστών ή συγκεκριμένων συσκευών ή που συγκεντρώθηκαν με μία αυστηρά ορισμένη διαδικασία. Σε αυτές τις περιπτώσεις, δημιουργούνται αμφιβολίες για την αποτελεσματικότητα σε πραγματικές συνθήκες.

- Αλγόριθμους που κατά την εκπαίδευσή τους έγινε χρήση δεδομένων κακόβουλων χρηστών, καθώς σε πραγματικές συνθήκες είναι πιθανό τα μοναδικά διαθέσιμα δεδομένα να προέρχονται μόνο από τον ιδιοκτήτη της συσκευής.

- Μεθοδολογίες που απαιτούν μεγάλους ρυθμούς δειγματοληψίας ή πόρους ψηλής ισχύος, καθώς μπορεί να οδηγήσουν στην μείωση της απόδοσης της μπαταρίας αλλά και του smartphone.

- Συστήματα που βασίζονται αποκλειστικά σε έναν μοναδικό τύπο δεδομένων, μπορεί να θεωρηθούν ανεπαρκείς στην περίπτωση που αυτά τα δεδομένα δεν είναι διαθέσιμα. Για παράδειγμα, στην περίπτωση που το επιταχυνσιόμετρο μιας συσκευής παρουσιάζει σφάλματα, τότε ένα σύστημα βασιζόμενο αποκλειστικά σε δεδομένα επιταχυνσιομέτρου θα υπολειτουργεί.

- Έρευνες που παρουσιάζουν αποτελέσματα με μετρικές που δεν είναι αντιπροσωπευτικές στην φύση του προβλήματος και έτσι δημιουργούν αμφιβολίες για την πραγματική αποτελεσματικότητα του συστήματος που προτείνουν.

4 Μεθοδολογία

Στην ενότητα αυτή παρουσιάζεται η μεθοδολογία που ακολουθήθηκε στη συγκεκριμένη εργασία, για την αντιμετώπιση του προβλήματος συνεχούς – έμμεσης αυθεντικοποίησης στα smartphones. Κεντρική ιδέα είναι η υλοποίηση ενός συστήματος που θα ελέγχει την αυθεντικότητα ενός χρήστη βάση ενός συνδυασμού συμπεριφορικών χαρακτηριστικών. Θα εκμεταλλεύεται τα πλεονεκτήματα, τόσο δεδομένων κίνησης που παράγονται από το επιταχυνσιόμετρο και το γυροσκόπιο της συσκευής, όσο και δεδομένων που εξάγονται από την οθόνη αφής, όταν υπάρχει αλληλεπίδραση με τον χρήστη. Έτσι, ο έλεγχος θα μπορεί να εκτελείται συνεχώς και με διαφανή τρόπο προς τον χρήστη, αποτελώντας ένα μοναδικό ή ένα συμπληρωματικό επίπεδο ασφάλειας, που δεν απαιτεί δευτερεύον εξοπλισμό και περισσότερους πόρους, από αυτούς που η συσκευή μπορεί να διαθέσει.

Ωστόσο, για την σωστή ανάπτυξη ενός τέτοιου συστήματος, αναγκαία ήταν η εκτέλεση πειραμάτων που απαντούν σε μια σειρά από ερωτήματα και προβληματισμούς. Η περιγραφή αυτών, αναπτύσσεται στην συνέχεια της ενότητας και αφορά την επιλογή δεδομένων εκπαίδευσης και αξιολόγησης, την εξαγωγή και επιλογή βέλτιστων χαρακτηριστικών για κάθε είδος δεδομένων, την επιλογή βέλτιστων παραμέτρων για τα μοντέλα μηχανικής μάθησης και τέλος τη διαμόρφωση ενός τρόπου αξιολόγησης, που ανταποκρίνεται στο γενικότερο πρόβλημα της αυθεντικοποίησης.

4.1 Επιλογή Δεδομένων

4.1.1 Σύνολο Δεδομένων

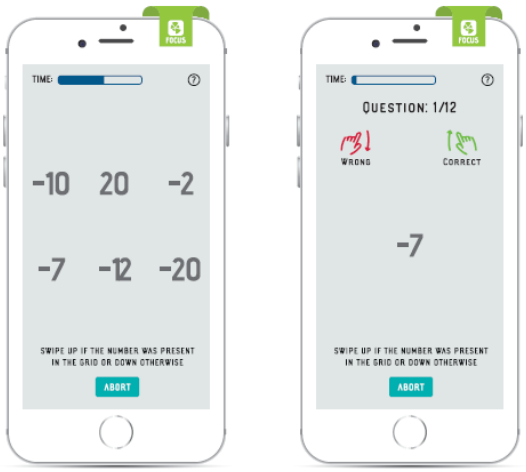
Τα δεδομένα που χρησιμοποιήθηκαν, επιλέχθηκαν από το σύνολο δεδομένων BrainRun [35]. Το BrainRun είναι ένα σύνολο συμπεριφορικών δεδομένων και ξεχωρίζει γιατί η λήψη τους δεν έγινε υπό συνθήκες εργαστηρίου. Πιο συγκεκριμένα, οι συγγραφείς ανέπτυξαν μια εφαρμογή για Android και iOS συσκευές που περιλαμβάνει μια λίστα παιχνιδιών κατάρτισης εγκεφάλου (Brain Training Games), τα οποία έχουν σκοπό τη συλλογή δεδομένων με ανεπιτήδευτο τρόπο.

Τα παιχνίδια που περιλαμβάνονται στην εφαρμογή διαχωρίζονται σε 5 κατηγορίες, με διαφορετικά επίπεδα δυσκολίας. Κάθε παιχνίδι εξετάζει διαφορετική πνευματική λειτουργία των χρηστών και εστιάζει στην συλλογή δεδομένων με συγκεκριμένα χαρακτηριστικά. Με αυτό τον τρόπο η συμπεριφορά των χρηστών εξετάζεται σφαιρικά και παρέχεται μεγάλο πλήθος πληροφορίας. Παρακάτω περιγράφονται οι 5 κατηγορίες παιχνιδιών:

1. *Mathisis:* Περιλαμβάνει την επίλυση μικρών μαθηματικών εξισώσεων, με σκοπό τη συλλογή οριζόντιων swipes. Στον χρήστη παρουσιάζεται μια εξίσωση και του ζητείται να σύρει αριστερά ή δεξιά, ανάλογα με το αν η εξίσωση είναι λανθασμένη ή σωστή.

Σχήμα 19: Παράδειγμα Mathisis

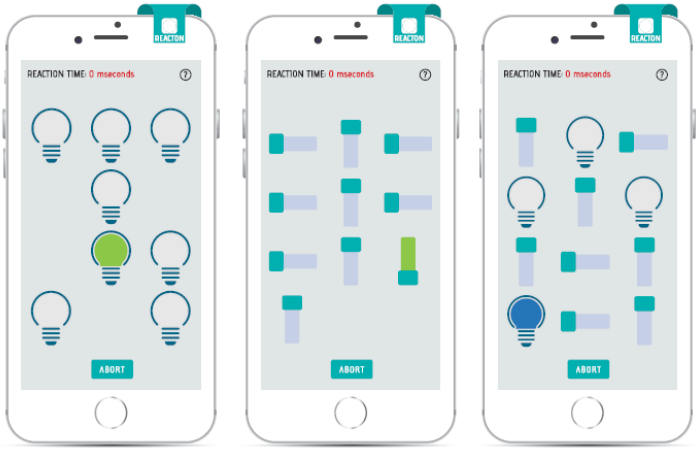
2. *Focus:* Στοχεύει στις δεξιότητες απομνημόνευσης των χρηστών και την συλλογή κατακόρυφων swipes (scrolls). Αρχικά παρουσιάζεται ένα σύνολο σχημάτων ή/και αριθμών για ένα μικρό χρονικό διάστημα. Στη συνέχεια, το σύνολο εξαφανίζεται και εμφανίζεται ένα σχήμα ή ένας αριθμός. Εάν η καινούργια απεικόνιση υπήρχε στο αρχικό σύνολο, τότε ο χρήστης πρέπει να σύρει προς τα πάνω, αλλιώς προς τα κάτω.



Σχήμα 20: Παράδειγμα Focus

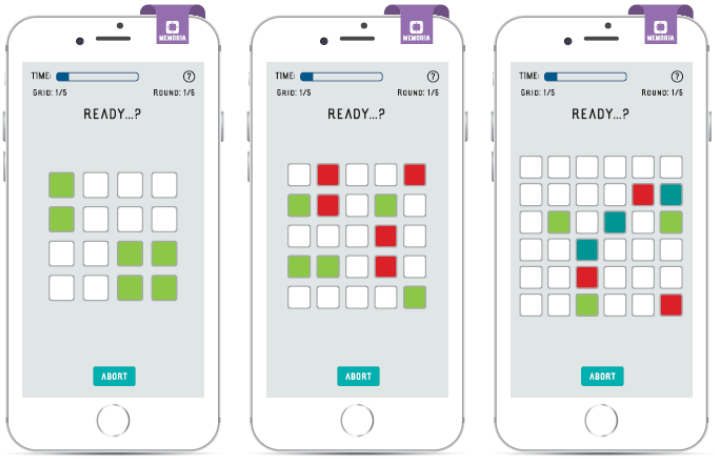
3. *Reacton:* Βασίζεται στις αντιδράσεις του χρήστη και συνδυάζει taps και swipes. Το παιχνίδι περιλαμβάνει ένα πλέγμα από λαμπτήρες και διακόπτες. Σε τυχαία χρονικά

διαστήματα ένα από αυτά αλλάζει χρώμα (ενεργοποιείται). Στόχος είναι η απενεργοποίηση του αντικειμένου το συντομότερο δυνατό. Αν είναι λαμπτήρας, ο χρήστης πρέπει να κάνει tap πάνω του. Αν είναι διακόπτης, ο χρήστης πρέπει να τον μετακινήσει, κάνοντας swipe.



Σχήμα 21: Παράδειγμα Reacton

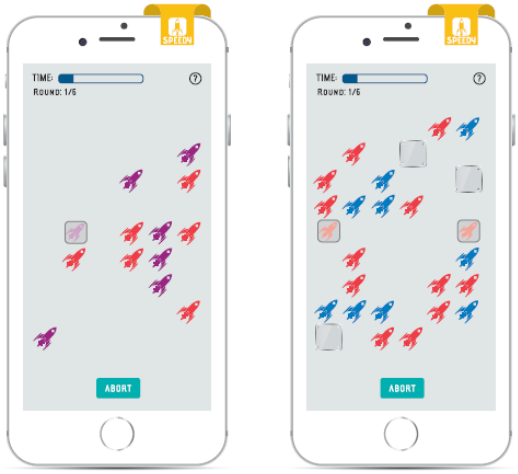
4. *Memoria:* Είναι ένα ακόμα παιχνίδι απομνημόνευσης που στοχεύει στη συλλογή taps. Το παιχνίδι ξεκινά με ένα πλέγμα από λευκά πλακίδια που μετά από λίγο ορισμένα αλλάζουν χρώμα και ο χρήστης έχει ένα χρονικό διάστημα για να τα απομνημονεύσει. Στην συνέχεια, όλα τα πλακίδια γίνονται άσπρα και ο χρήστης καλείται να επιλέξει εκείνα που είχαν ένα συγκεκριμένο χρώμα.



Σχήμα 22: Παράδειγμα Memoria

5. *Speedy:* Έχει να κάνει με την ταχύτητα κινήσεως των χρηστών και την συλλογή taps. Κατά την εκκίνηση εμφανίζεται ένα πλέγμα από πυραύλους δύο χρωμάτων. Κάνοντας

tap σε έναν πύραυλο, ο χρήστης μπορεί να τον μετατρέψει στο άλλο χρώμα. Στόχος του παιχνιδιού είναι όλοι οι πύραυλοι να αποκτήσουν το ίδιο χρώμα, το συντομότερο δυνατό.



Σχήμα 23: Παράδειγμα Speedy

Συνολικά το σύνολο BrainRun περιλαμβάνει 3,11 εκατομμύρια χειρονομίες από 2.218 χρήστες. Ωστόσο, τα δεδομένα που συλλέγονται από την εφαρμογή δεν είναι μόνο πληροφορίες χειρονομιών. Κατά την εκτέλεση γίνεται συλλογή δεδομένων από τους αισθητήρες αλλά και πληροφοριών σχετικών με την συσκευή και την πορεία του χρήστη στα διάφορα παιχνίδια. Πιο συγκεκριμένα, μπορεί να γίνει ο παρακάτω διαχωρισμός:

1. *Δεδομένα Χειρονομιών (Gestures)*: Περιλαμβάνουν πληροφορίες, για τα σημεία της οθόνης αφής, που εμπλέκονται σε κάθε tap και swipe. Στους παρακάτω πίνακες (Πίνακας 2, Πίνακας 3), φαίνονται λεπτομερώς οι πληροφορίες που αποθηκεύονται για κάθε gesture.

2. *Δεδομένα Αισθητήρων Κίνησης (Sensors)*: Πρόκειται για μετρήσεις, που εξάγονται από τους αισθητήρες κίνησης της συσκευής. Αν και η εφαρμογή διαθέτει μετρήσεις από περισσότερους αισθητήρες, για την εργασία αυτή θα γίνει περιγραφή, μόνο του τρόπου αποθήκευσης των μετρήσεων του επιταχυνσιομέτρου και του γυροσκοπίου. Ο τρόπος αποθήκευσης, είναι ίδιος και για τους δύο αισθητήρες και φαίνεται στον παρακάτω πίνακα (Πίνακας 4).

3. *Δεδομένα Χρηστών/Συσκευών/Παιχνιδιών (Users/Devices/Games)*: Δεδομένα που περιέχουν πληροφορίες για τους εγγεγραμμένους χρήστες, τις καταχωρημένες συσκευές και τα παιχνίδια που έπαιξαν οι χρήστες. Οι πληροφορίες αυτές

διευκολύνουν τις διαδικασίες δημιουργίας όψεων και εξαγωγής επιθυμητών συνόλων δεδομένων. Για παράδειγμα, η συσχέτιση μίας χειρονομίας με τον χρήστη που την πραγματοποίησε και την συσκευή στην οποία πραγματοποιήθηκε, επιτυγχάνεται μέσω δεδομένων, αυτής της κατηγορίας.

Πίνακας 2: Γνωρίσματα Χειρονομιών

Γνωρίσματα	Περιγραφή
type	Ο τύπος χειρονομίας (swipe ή tap)
session_id	Το id της τρέχουσας περιόδου λειτουργίας (εάν η εφαρμογή επανεκκινηθεί, δημιουργείται ένα διαφορετικό αναγνωριστικό συνεδρίας
device_id	Το id της συσκευής στην οποία έγινε η χειρονομία
t_start	Η χρονική σήμανση κατά την έναρξη της χειρονομίας
t_stop	Η χρονική σήμανση κατά την λήξη της χειρονομίας
screen	Το όνομα της οθόνης στην οποία έγινε η χειρονομία (π.χ. ReactonGame-1.1.4)
data	Μια λίστα που περιέχει πληροφορίες για τα σημεία που εμπλέκονται στη χειρονομία (Πίνακας 3)

Πίνακας 3: Γνωρίσματα Σημείων Χειρονομιών

Γνωρίσματα	Περιγραφή
moveX	Η οριζόντια συντεταγμένη του σημείου
moveY	Η κατακόρυφη συντεταγμένη του σημείου
x0	Η οριζόντια συντεταγμένη του αρχικού σημείου της χειρονομίας
y0	Η κατακόρυφη συντεταγμένη του αρχικού σημείου της χειρονομίας
dx	Η οριζόντια απόσταση του σημείου με το αρχικό
dy	Η κατακόρυφη απόσταση του σημείου με το αρχικό
vx	Η οριζόντια ταχύτητα στο σημείο
vy	Η κατακόρυφη ταχύτητα στο σημείο

Πίνακας 4: Γνωρίσματα Μετρήσεων Αισθητήρων (Επιταχυνσιόμετρο / Γυροσκόπιο)

Γνωρίσματα	Περιγραφή
x	Η επιτάχυνση / περιστροφή της συσκευής στον άξονα x
y	Η επιτάχυνση / περιστροφή της συσκευής στον άξονα y
z	Η επιτάχυνση / περιστροφή της συσκευής στον άξονα z
screen	Το όνομα της οθόνης στην οποία έγινε η μέτρηση
player_id	Το id του χρήστη που σχετίζεται με την μέτρηση
timestamp	Η χρονική σήμανση της διαδικασίας μετρήσεων, στην οποία ανήκει η μέτρηση

Τέλος, επισημαίνεται ότι ο τρόπος αποθήκευσης των δεδομένων αισθητήρων κίνησης, διαφέρει από αυτόν των δύο άλλων κατηγοριών. Ωστόσο, και στις δύο περιπτώσεις, οποιαδήποτε χρονική επισήμανση δίνεται σε unix σε χιλιοστά του δευτερολέπτου (unix timestamp in milliseconds).

4.1.2 Κριτήρια & Τελική Επιλογή

Όπως αναφέρθηκε, το σύνολο BrainRun περιέχει μεγάλο πλήθος χρηστών και δεδομένων. Η χρήση ολόκληρου του συνόλου για την σχεδίαση, βελτιστοποίηση και αξιολόγηση του συστήματος ήταν αδύνατη, καθώς απαιτούσε μεγαλύτερη από την διαθέσιμη υπολογιστική ισχύ και πολύ μεγάλο χρόνο αναμονής για την εξαγωγή αποτελεσμάτων σε κάθε βήμα. Επιπλέον, κάθε παιχνίδι (Mathisis, Focus, Reacton, Memoria, Speedy) προσφέρει διαφορετικά δεδομένα και επιλέχθηκε να γίνει ανάλυση κάθε παιχνιδιού ξεχωριστά. Έτσι, προς αυτή την κατεύθυνση, κρίθηκε απαραίτητή η επιλογή ενός υποσυνόλου χρηστών, για κάθε παιχνίδι.

Τα κριτήρια επιλογής εφαρμόστηκαν σε επίπεδο ποιότητας και ποσότητας δεδομένων, στηρίχθηκαν στην βιβλιογραφία, στην φύση των δεδομένων και σε δοκιμές. Με σκοπό να εξασφαλιστεί η εξαγωγή γενικευμένων συμπερασμάτων, αποφασίστηκε να είναι ίδια τα κριτήρια μεταξύ των διαφορετικών παιχνιδιών. Συνεπώς, τα κριτήρια επιλογής πρέπει να εξασφαλίζουν επαρκή πλήθος χρηστών και στα 5 παιχνίδια. Αναλυτικότερα, η διαδικασία επιλογής, η οποία πραγματοποιήθηκε για κάθε παιχνίδι, περιλάμβανε:

1. Την ταξινόμηση χρηστών με δεδομένα επιταχυνσιομέτρου που τηρούν τα παρακάτω κριτήρια.

2. Την ταξινόμηση χρηστών με δεδομένα γυροσκοπίου που τηρούν τα παρακάτω κριτήρια.

3. Την ταξινόμηση χρηστών με δεδομένα χειρονομιών που τηρούν τα παρακάτω κριτήρια.

4. Την επιλογή του μέγιστου κοινού υποσυνόλου των τριών παραπάνω συνόλων.

Μετά από δοκιμές και την ταυτόχρονη παρακολούθηση και των 5 παιχνιδιών, ένας χρήστης μπορεί να κριθεί κατάλληλος για ένα παιχνίδι εάν:

- Στα δεδομένα αισθητήρων:

- Έχει τουλάχιστον 3.000 δείγματα επιταχυνσιομέτρου και 3.000 δείγματα γυροσκοπίου, για το συγκεκριμένο παιχνίδι, αριθμός που τέθηκε ώστε να υπάρχει στην συνέχεια επαρκής αριθμός δειγμάτων για την εκπαίδευση των ML μοντέλων και την αξιολόγηση του συστήματος.

- Τα παραπάνω δείγματα πρέπει να προέρχονται από πακέτα μετρήσεων (timestamps) με τουλάχιστον 2 εγγραφές. Τα πακέτα μετρήσεων πρέπει να περιέχουν επαρκεί αριθμό δειγμάτων, ώστε να μπορούν να σχηματιστούν ακολουθίες και στην συνέχεια να μπορεί να γίνει η εξαγωγή χαρακτηριστικών.

- Τα παραπάνω δείγματα δεν προέρχονται από πακέτα μετρήσεων, που κατά πλειοψηφία οι εγγραφές τους παρουσιάζουν μηδενική τιμή στους άξονες x και y, υποδηλώνοντας ότι η συσκευή είναι τοποθετημένη σε επιφάνεια.

- Στα δεδομένα αφής:

  - Χρησιμοποιεί συσκευή με μέγιστο μέγεθος 600 * 1000 pixels, με σκοπό να αποφευχθούν δεδομένα από μεγαλύτερες συσκευές, όπως tablets που μπορεί να αλλοιώσουν τα αποτελέσματα.

  - Έχει τουλάχιστον 300 swipes ή taps, καθώς έτσι εξασφαλίζεται ένας επαρκής αριθμός δειγμάτων για την σωστή εκπαίδευση των ML μοντέλων και την αξιολόγηση του συστήματος.

  - Τα παραπάνω swipes πρέπει να έχουν πλήθος σημείων στο εύρος [4, 10] και η διάρκειά τους να είναι μικρότερη από 30ms. Σε αντίθετη περίπτωση, ένα gesture με τα αντίθετα χαρακτηριστικά θεωρείται εσφαλμένα swipe.

Εφαρμόζοντας τα παραπάνω κριτήρια, οι διαθέσιμοι χρήστες για το κάθε παιχνίδι φαίνονται στον παρακάτω πίνακα (Πίνακας 5). Παρατηρείται πως οι διαθέσιμοι χρήστες διαχωρίζονται σε αυτούς που επιλέχθηκαν για την εκπαίδευση του συστήματος και σε αυτούς που χρησιμοποιήθηκαν αποκλειστικά για την αξιολόγηση του συστήματος. Πιο συγκεκριμένα, τα αποτελέσματα των χρηστών εκπαίδευσης είναι αυτά που χρησιμοποιήθηκαν στην επιλογή των διάφορων παραμέτρων και την βελτιστοποίηση του συστήματος, ενώ τα αποτελέσματα των χρηστών αξιολόγησης είναι αυτά που δείχνουν αντικειμενικά την αποτελεσματικότητα του

συστήματος. Από τον πίνακα παρατηρείται πως ο αριθμός των χρηστών εκπαίδευσης είναι μικρότερος από των αριθμό των χρηστών αξιολόγησης. Το γεγονός αυτό δικαιολογείται για δύο βασικούς λόγους:

1. Οι χρήστες εκπαίδευσης χρησιμοποιούνται στα περισσότερα πειράματα που πραγματοποιήθηκαν και έτσι η επιλογή ενός μεγάλου αριθμού χρηστών για την εκτέλεση των πειραμάτων εισάγει μεγάλη καθυστέρηση. Επιπλέον, ο αριθμός χρηστών που επιλέχθηκε θεωρείται ταυτόχρονα ικανοποιητικός για την εξαγωγή γενικευμένων συμπερασμάτων, καθώς πειράματα που πραγματοποιήθηκαν με αυξημένο αριθμό χρηστών καθυστερούσαν αρκετά την εξαγωγή αποτελεσμάτων αλλά ταυτόχρονα δεν έδιναν περισσότερη πληροφορία.

2. Ο αριθμός των χρηστών αξιολόγησης είναι μεγάλος ώστε το σύστημα να αξιολογηθεί αντικειμενικά, να δοκιμαστεί σε δεδομένα διαφορετικών χρηστών, με διαφορετικές συμπεριφορές και να ελεγχθεί η ικανότητά του για γενίκευση. Όπως είδη αναφέρθηκε, έρευνες που αξιολογούνται σε μικρό αριθμό χρηστών μπορεί να παρουσιάζουν αποτελέσματα που δεν ανταποκρίνονται στην πραγματικότητα.

Πίνακας 5: Αριθμός Διαθέσιμων Χρηστών

Παιχνίδι	**Mathisis**	**Focus**	**Reacton**	**Memoria**	**Speedy**
Αριθμός Χρηστών Εκπαίδευσης	15	15	15	15	15
Αριθμός Χρηστών Αξιολόγησης	24	30	45	44	45
Σύνολο	39	45	60	59	60

Τέλος, σημειώνεται ότι ο αριθμός των δεδομένων αισθητήρων περιορίστηκε στις 20.000, ενώ των δεδομένων χειρονομιών στις 2.000. Οι περισσότεροι χρήστες δεν ξεπερνούσαν αυτά τα όρια, ωστόσο όσοι το έκαναν επιβάρυναν σημαντικά τις διαδικασίες, χωρίς να προσφέρουν σημαντική πληροφορία.

4.2 Εξαγωγή & Επιλογή Χαρακτηριστικών

Σε συνέχεια της επιλογής χρηστών και δεδομένων, απαραίτητη είναι η διαδικασία εξαγωγής και επιλογής χαρακτηριστικών για την σωστή εκπαίδευση των μοντέλων μηχανικής μάθησης όσο και για την αποτελεσματικότητα του τελικού συστήματος.

4.2.1 Χαρακτηριστικά Αισθητήρων Κίνησης

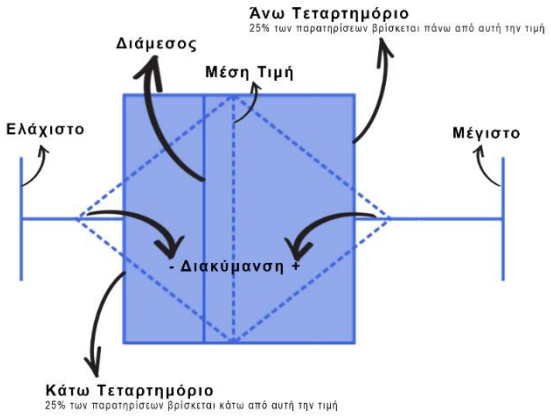
Οι αισθητήρες λαμβάνουν πολλές μετρήσεις ανά δευτερόλεπτο, βάσει συγκεκριμένου ρυθμού δειγματοληψίας. Κατά την διαδικασία αυτή μπορεί να υπάρξουν σφάλματα και είναι πιθανό μετρήσεις να παραληφθούν ή να περιέχουν λανθασμένες και ακραίες τιμές. Έτσι, για την ανάπτυξη αποδοτικών μοντέλων, κρίνεται απαραίτητη η εξερεύνηση των δεδομένων, η ελαχιστοποίηση των σφαλμάτων και η εξαγωγή χαρακτηριστικών από ένα σύνολο μετρήσεων.

4.2.1.1 Επιλογή Γνωρισμάτων

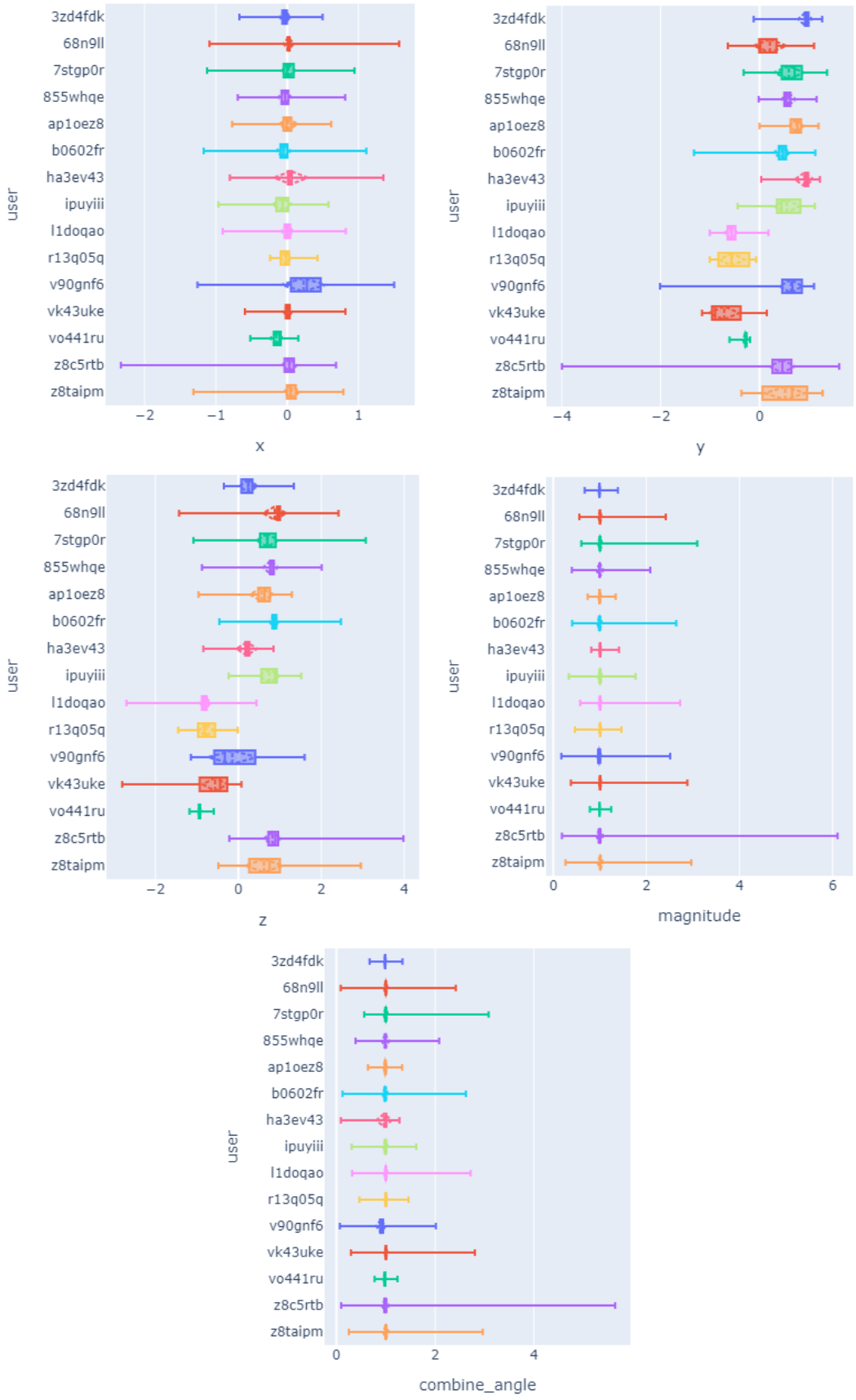
Είναι πιθανό, γνωρίσματα (Πίνακας 4) των μετρήσεων να περιέχουν πληροφορία μη σχετική με το πρόβλημα ή πληροφορία που είδη έχει δοθεί μέσο άλλων γνωρισμάτων. Η χρήση τέτοιων γνωρισμάτων κατά την εκπαίδευση των ML αλγορίθμων μπορεί να επηρεάσει αρνητικά το τελικό αποτέλεσμα και έτσι αυτά τα γνωρίσματα μπορούν να θεωρηθούν πλεονάζοντα και είναι απαραίτητη η απομάκρυνσή τους.

Προς αυτή την κατεύθυνση, χρησιμοποιήθηκαν τα δεδομένα των 15 χρηστών κάθε παιχνιδιού για την δημιουργία θηκογραμμάτων (box plots). Τα θηκογράμματα είναι διαγράμματα που απεικονίζουν την κατανομή ενός επιθυμητού μεγέθους, πιο συγκεκριμένα δίνουν την πληροφορία για τις εφτά τιμές που φαίνονται στο παρακάτω σχήμα (Σχήμα 24).

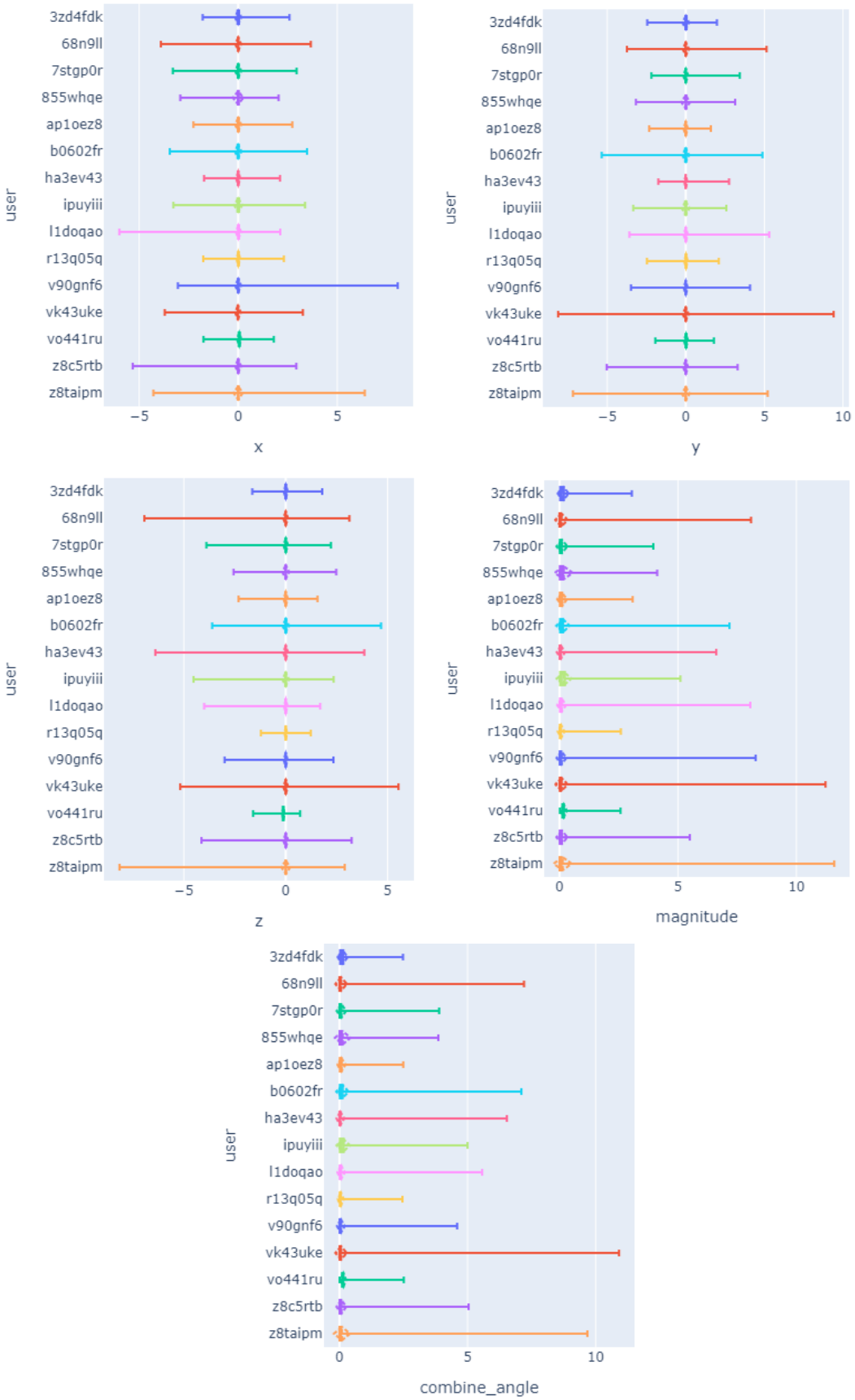
Τα παρακάτω θηκογράμματα αφορούν τους χρήστες του Mathisis, τόσο για το επιταχυνσιόμετρο (Σχήμα 25), όσο και για το γυροσκόπιο (Σχήμα 26). Στον οριζόντιο άξονα φαίνονται τα ονόματα των χρηστών, ενώ στον κατακόρυφο οι τιμές του αντίστοιχου γνωρίσματος. Στα γνωρίσματα συμπεριλαμβάνονται το μήκος του συνολικού διανύσματος (magnitude) και το μήκος του επιπέδου y – z (combine angle), καθώς οι κινήσεις του καρπού και του πήχη συχνά εκτελούνται γύρω από αυτούς τους 2 άξονες.



Σχήμα 24: Θηκόγραμμα



Σχήμα 25: Κατανομές Γνωρισμάτων Επιταχυνσιομέτρου



Σχήμα 26: Κατανομές Γνωρισμάτων Γυροσκοπίου

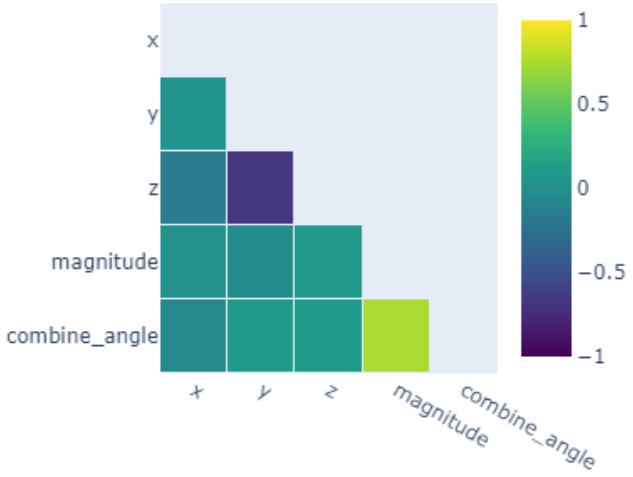
Παρατηρώντας τα αποτελέσματα προκύπτουν τα εξής συμπεράσματα:

- Τα δεδομένα του επιταχυνσιομέτρου παρουσιάζουν μεγαλύτερη διαφοροποίηση μεταξύ των χρηστών σε σχέση με του γυροσκοπίου. Κάτι που εξηγείται από το γεγονός ότι το γυροσκόπιο διατηρεί σταθερό τον προσανατολισμό του. Ωστόσο, μπορεί να αποτελέσει ένα επιπλέον επίπεδο ακριβείας και για αυτό επιλέχθηκε ο συνδυασμός του με το επιταχυνσιόμετρο.

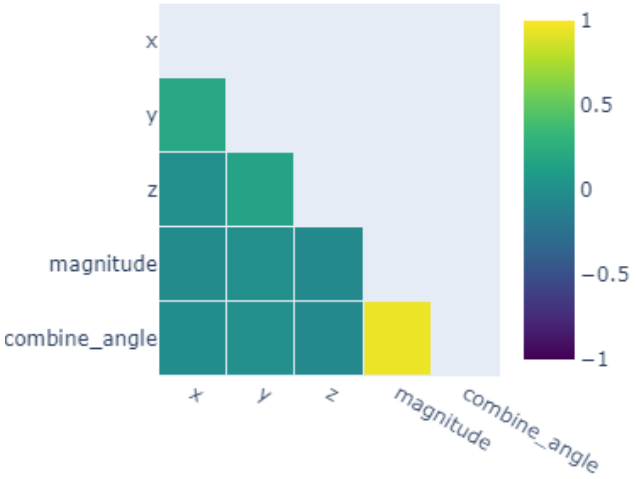
- Οι μεταβλητές combined angle και magnitude στο γυροσκόπιο έχουν κατώτερη τιμή το μηδέν, ενώ στο επιταχυνσιόμετρο οι τιμές βρίσκονται γύρω από το 1.

- Στο επιταχυνσιόμετρο η μεταβλητή y φαίνεται να παρουσιάζει τη μεγαλύτερη διαφοροποίηση μεταξύ των χρηστών αλλά και μεγάλη διακύμανση στα δεδομένα ενός χρήστη.

Παρόμοια συμπεράσματα προκύπτουν και για τα υπόλοιπα παιχνίδια και έτσι τα αντίστοιχα διαγράμματα παραλείπονται. Ωστόσο, τα συμπεράσματα αυτά δεν οδηγούν σε ξεκάθαρη επιλογή. Για τον λόγο αυτό, δημιουργήθηκαν οι παρακάτω πίνακες συσχέτισης, τόσο για τα γνωρίσματα του επιταχυνσιομέτρου (Σχήμα 27) όσο και του γυροσκοπίου (Σχήμα 28).



Σχήμα 27: Πίνακας Συσχέτισης Γνωρισμάτων Επιταχυνσιομέτρου



Σχήμα 28: Πίνακας Συσχέτισης Γνωρισμάτων Γυροσκοπίου

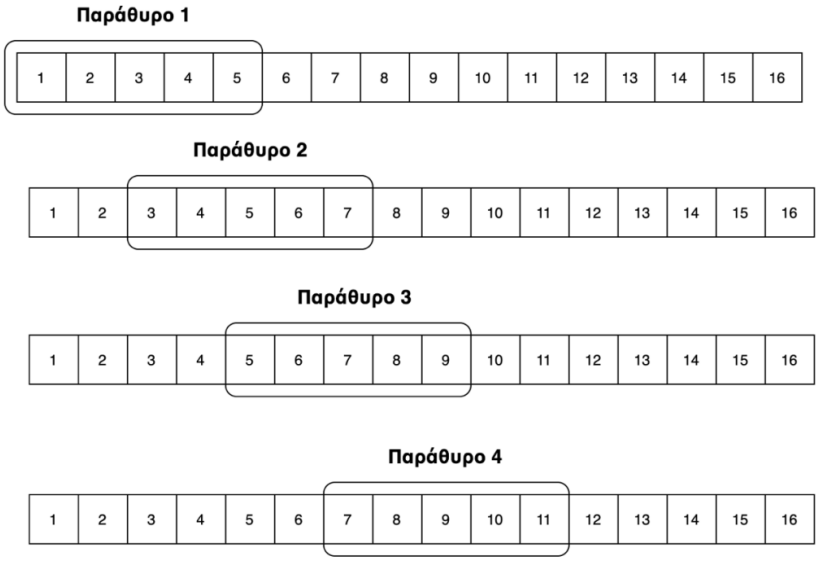
Οι πίνακες αυτοί χρησιμοποιούν τη συσχέτιση Pearson και αφορούν τα δεδομένα του Mathisis, παρουσιάζοντας όμως και την εικόνα των υπόλοιπων παιχνιδιών. Φαίνεται πως και για τους δύο τύπους δεδομένων, τα μεγέθη magnitude και combine angle παρουσιάζουν μεγαλύτερη συσχέτιση, ενώ στα δεδομένα επιταχυνσιομέτρου υπάρχει έντονη αρνητική συσχέτιση και μεταξύ των y και z. Αξιοποιώντας τα συμπεράσματα των παραπάνω διαγραμμάτων και εκτελώντας διάφορες δοκιμές, αποφασίστηκε να χρησιμοποιηθούν οι μεταβλητές x, y και magnitude στα επόμενα βήματα.

4.2.1.2 Ελαχιστοποίηση Σφαλμάτων

Όπως υπογραμμίστηκε παραπάνω, οι μετρήσεις δεν είναι πάντα αξιόπιστες ενώ ταυτόχρονα το πλήθος τους μπορεί να γίνει πολύ μεγάλο. Έτσι, στοχεύοντας στην ελαχιστοποίηση των εσφαλμένων μετρήσεων αλλά και την μοντελοποίηση της συμπεριφοράς του χρήστη, είναι απαραίτητη η σχεδίαση συστημάτων που βασίζονται σε ακολουθίες μετρήσεων. Με αυτό τον τρόπο η εξαγωγή χαρακτηριστικών και συνεπώς η είσοδος των ML αλγορίθμων βασίζεται σε ένα σύνολο μετρήσεων, κάνοντας το σύστημα πιο ανθεκτικό σε σφάλματα των αισθητήρων.

Προκειμένου να δημιουργηθούν οι ακολουθίες, επιλέχθηκε μια τεχνική κατάτμησης κυλιόμενου παραθύρου. Πιο συγκεκριμένα, για κάθε αισθητήρα, οι εγγραφές που βρίσκονται στο ίδιο πακέτο μετρήσεων (timestamp) και στην ίδια οθόνη ομαδοποιούνται και στην συνέχεια διαχωρίζονται σε τμήματα συγκεκριμένου μεγέθους και ποσοστού επικάλυψης. Η μεθοδολογία αυτή φαίνεται στο Σχήμα 29, όπου το μέγεθος παραθύρου είναι 5 δείγματα και η επικάλυψη είναι 3 δείγματα ή αλλιώς το βήμα είναι 2. Στο πρώτο παράθυρο επιλέχθηκαν τα πρώτα 5 δείγματα, στο δεύτερο παράθυρο επιλέχθηκαν 3 από τα προηγούμενα δείγματα και 2 νέα και ούτω καθεξής, μέχρι να τμηματοποιηθούν όλα τα δεδομένα. Αν το πλήθος των μετρήσεων είναι μικρότερο του παραθύρου, τότε το μέγεθος παραθύρου μεταβάλλεται. Ενώ,

αν στο τέλος της κατάτμησης περισσέψει σημαντικός αριθμός μετρήσεων, μεταβάλλεται το ποσοστό επικάλυψης ώστε συμπεριληφθούν και αυτές.

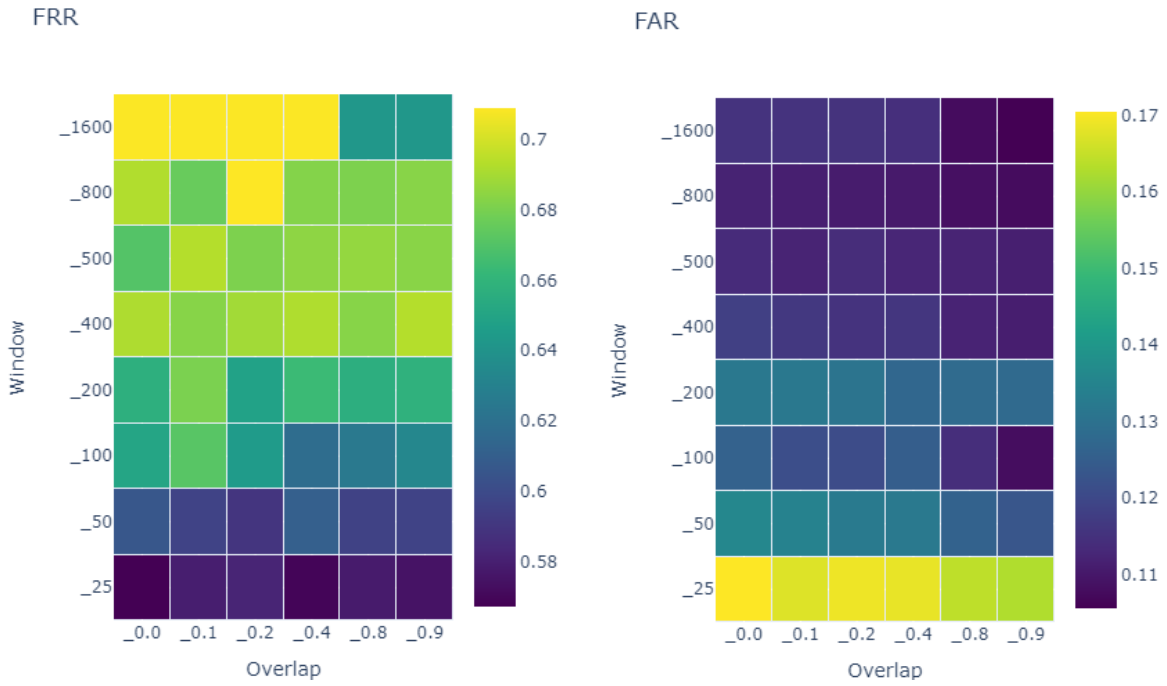


Σχήμα 29: Κατάτμηση με Κυλιόμενο Παράθυρο

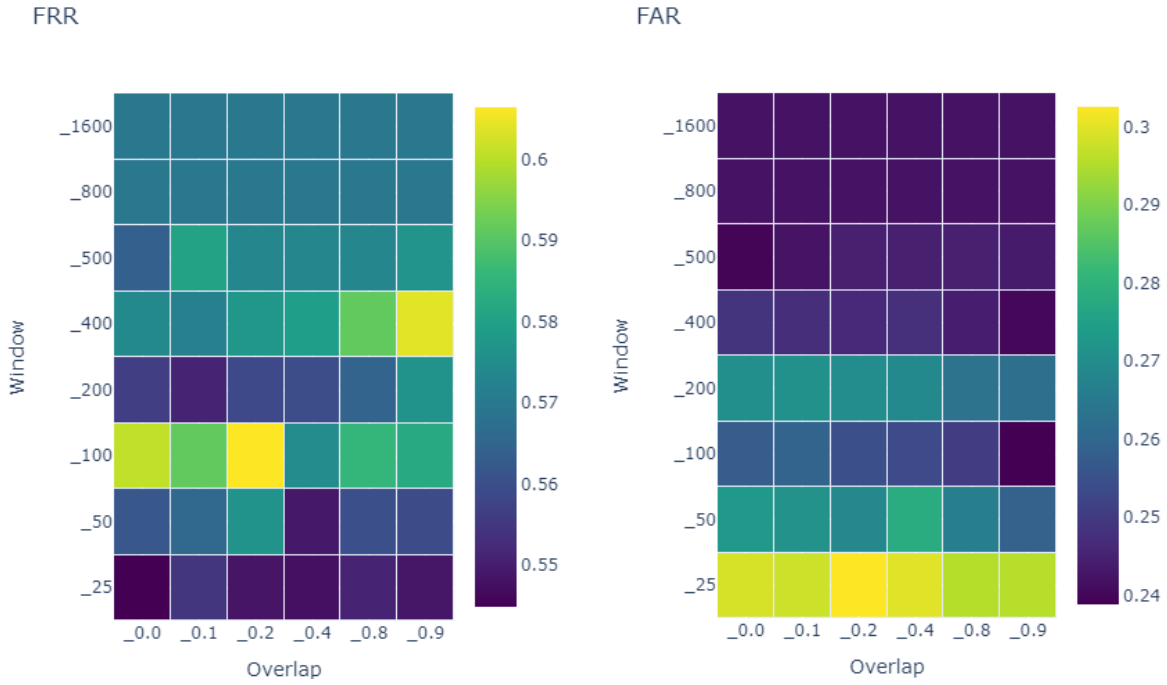
Για την επιλογή του μεγέθους παραθύρου και του ποσοστού επικάλυψης δεν υπάρχει κάποια προκαθορισμένη μέθοδος. Πολλές φορές η επιλογή γίνεται βάση της συχνότητας δειγματοληψίας των αισθητήρων, ενώ άλλες εμπειρικά. Το σύνολο δεδομένων BrainRun διαθέτει μετρήσεις από πολλές και διαφορετικές συσκευές και η συχνότητα δειγματοληψίας δεν είναι συγκεκριμένη, οπότε εφαρμόστηκε αναζήτηση πλέγματος και για τα δύο μεγέθη. Για το μέγεθος παραθύρου δοκιμάστηκαν οι τιμές [25, 50, 100, 200, 400, 500, 800, 1600] και για το ποσοστό επικάλυψης οι τιμές [0.0, 0.1, 0.2, 0.4, 0.8, 0.9]. Στα παρακάτω σχήματα (Σχήμα 30, Σχήμα 31) φαίνεται πως μεταβάλλονται οι μετρικές FRR και FAR. Οι μετρικές εξήχθησαν από απλά μοντέλα, με χρήση όλων των χαρακτηριστικών που αναφέρονται στην επόμενη ενότητα και προέκυψαν ως μέσος όρος των 15 χρηστών του παιχνιδιού Mathisis.

Όπως αποδεικνύεται, οι μετρικές μεταβάλλονται αντιστρόφως ανάλογα. Οι τιμές του FAR είναι αρκετά μικρότερες από αυτές του FRR. Το ποσοστό επικάλυψης φαίνεται να επηρεάζεται με μη σταθερό τρόπο. Παρατηρώντας τα διαγράμματα και των άλλων παιχνιδιών, που έχουν παρόμοια συμπεριφορά, αποφασίστηκε η τιμή παραθύρου να είναι 50 δείγματα και η επικάλυψη 60%. Έτσι, αν γίνει η υπόθεση ότι η συχνότητα δειγματοληψίας είναι 50Hz, μια συχνότητα που χρησιμοποιείται συνήθως για την συλλογή δεδομένων από αισθητήρες

κίνησης [51], σημαίνει ότι απαιτείται χρονικό διάστημα μόλις 1 δευτερολέπτου για την συλλογή ενός παραθύρου ή αλλιώς 50 μετρήσεων, για την επίτευξη τουλάχιστον ενός ελέγχου.



Σχήμα 30: Πλέγμα Αναζήτησης Μεγέθους Παραθύρου & Επικάλυψης - Επιταχυνσιόμετρο



Σχήμα 31: Πλέγμα Αναζήτησης Μεγέθους Παραθύρου & Επικάλυψης – Γυροσκόπιο

4.2.1.3 Τελική Επιλογή Χαρακτηριστικών

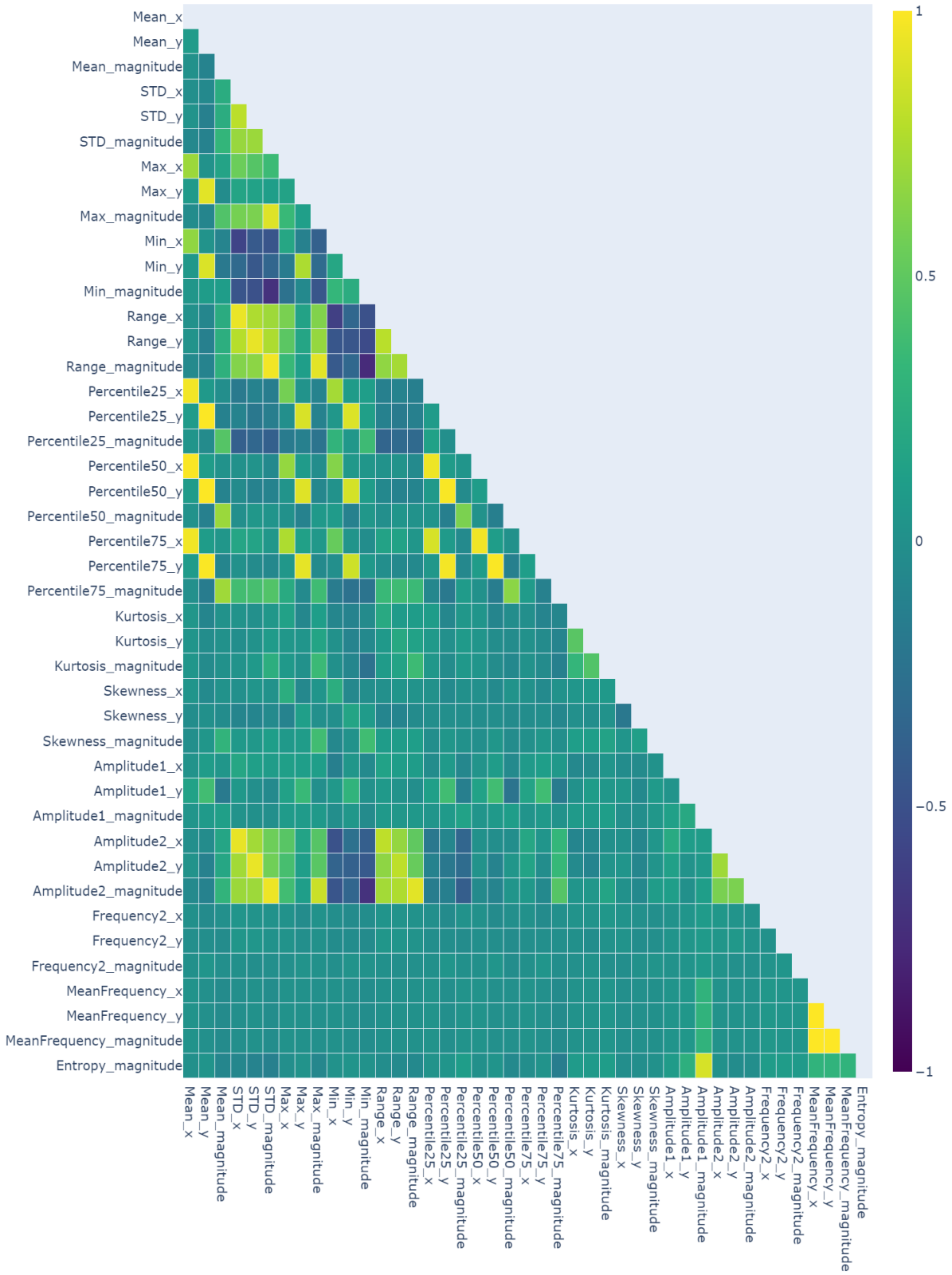
Κατά την επιλογή του παραθύρου και του ποσοστού επικάλυψης έγινε χρήση αρκετών χαρακτηριστικών. Ουσιαστικά τα χαρακτηριστικά που επιλέχθηκαν είναι διάφορες μετρικές που περιγράφουν μια ακολουθία, τόσο στο πεδίο του χρόνου όσο και της συχνότητας. Πιο συγκεκριμένα, για κάθε ένα γνώρισμα (x, y, magnitude), έγινε ο υπολογισμός των παρακάτω χαρακτηριστικών (Πίνακας 6):

Πίνακας 6: Χαρακτηριστικά Ακολουθιών Μετρήσεων Αισθητήρων

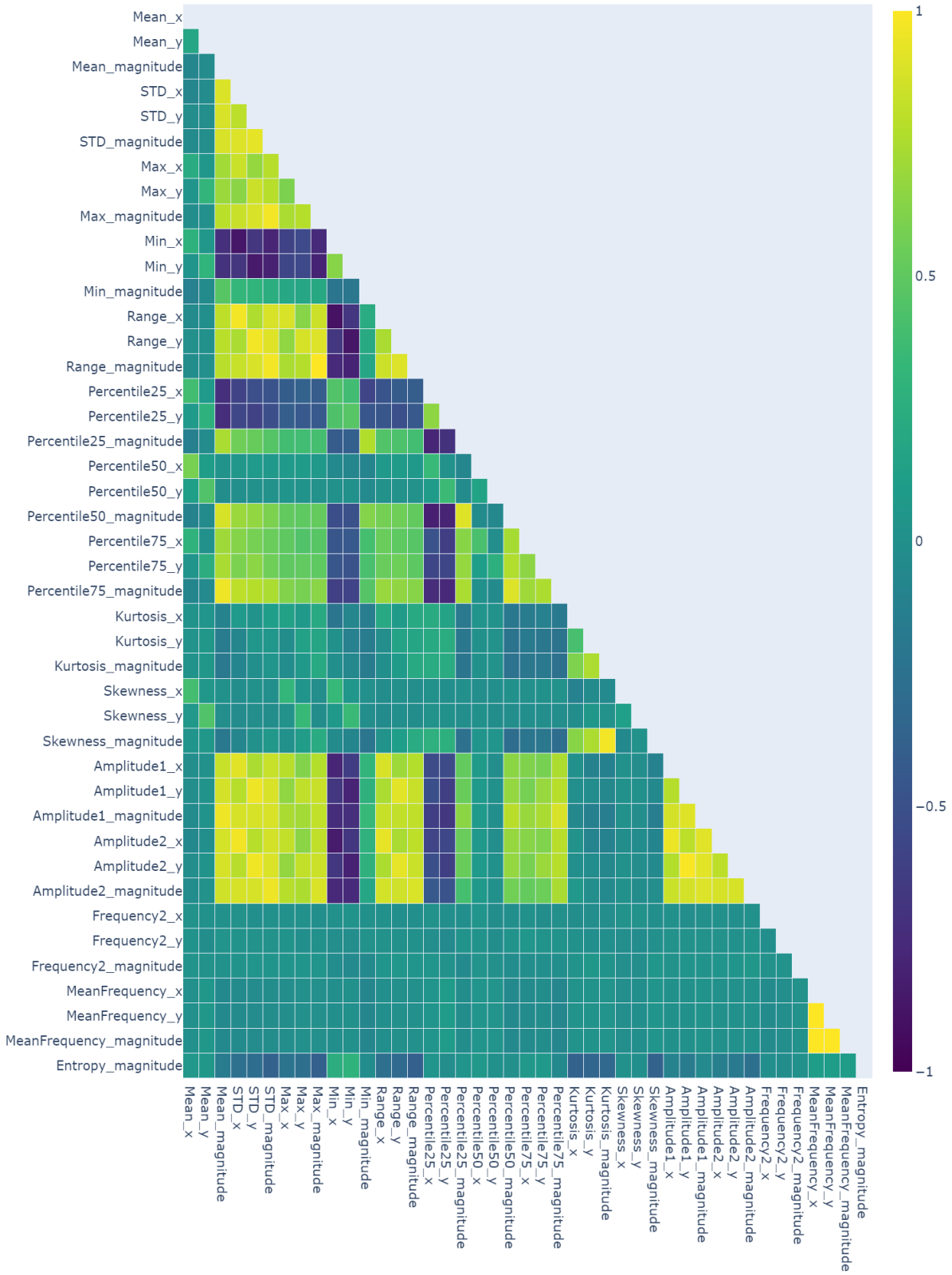
Χαρακτηριστικά	Περιγραφή
Mean	Η μέση τιμή των δειγμάτων της ακολουθίας
STD	Η τυπική απόκλιση των δειγμάτων της ακολουθίας
Max	Η μέγιστή τιμή των δειγμάτων της ακολουθίας
Min	Η ελάχιστη τιμή των δειγμάτων της ακολουθίας
Range	Η διαφορά της μέγιστης και ελαχίστης τιμής
Percentile25	Η τιμή κάτω από την οποία μπορεί να βρεθεί το 25% των παρατηρήσεων
Percentile50	Η τιμή κάτω από την οποία μπορεί να βρεθεί το 50% των παρατηρήσεων
Percentile75	Η τιμή κάτω από την οποία μπορεί να βρεθεί το 75% των παρατηρήσεων
Kurtosis	Ο βαθμός συγκέντρωσης των δεδομένων γύρω από τη μέση τιμή
Skewness	Ο βαθμός συμμετρίας των δεδομένων γύρω από τη μέση τιμή
Entropy	Η διασπορά της φασματικής κατανομής των μετρήσεων
Amplitude1	Το πλάτος της πρώτης υψηλότερης κορυφής στο πεδίο συχνότητας (Fast Fourier Transform – FFT)
Amplitude2	Το πλάτος της δεύτερης υψηλότερης κορυφής στο πεδίο συχνότητας (FFT)
Frequency2	Η συχνότητα της δεύτερης υψηλότερης κορυφής στο πεδίο συχνότητας (FFT)
Mean Frequency	Η μέση συχνότητα στο πεδίο συχνότητας (FFT)

Η χρήση όλων των χαρακτηριστικών και για τα 3 γνωρίσματα μπορεί να επηρεάσει αρνητικά την απόδοση του συστήματος. Η πολυπλοκότητα των ML μοντέλων αυξάνεται, φαινόμενα υπερεκπαίδευσης μπορούν να δημιουργηθούν πιο εύκολα και ταυτόχρονα η διαδικασία αυθεντικοποίησης κοστίζει σε χρόνο. Έτσι, κρίθηκε απαραίτητη η εξερεύνηση των συσχετίσεων και επιλογή συγκεκριμένων χαρακτηριστικών. Παρακάτω φαίνονται οι πίνακες συσχετίσεων, που βοήθησαν στην επιλογή χαρακτηριστικών, τόσο για το επιταχυνσιόμετρο όσο και για το γυροσκόπιο (Σχήμα 32, Σχήμα 33).

Οι συγκεκριμένοι πίνακες αφορούν το παιχνίδι Mathisis, ωστόσο παρόμοιοι είναι και αυτοί των υπόλοιπων παιχνιδιών. Μελετώντας προσεκτικά του πίνακες και εκτελώντας δοκιμές επιλέχθηκαν τα τελικά χαρακτηριστικά και για τους δύο αισθητήρες, τα οποία φαίνονται αναλυτικά στον παρακάτω πίνακα (Πίνακας 7).



Σχήμα 32: Πίνακας Συσχετίσεων Χαρακτηριστικών Επιταχυνσιομέτρου



Σχήμα 33: Πίνακας Συσχετίσεων Χαρακτηριστικών Γυροσκοπίου

Πίνακας 7: Τελικά Χαρακτηριστικά Αισθητήρων Κίνησης

Αισθητήρας	Γνωρίσματα	Τελικά Χαρακτηριστικά
Επιταχυνσιόμετρο	x	Mean, STD, Max, Min, Percentile25, Percentile50, Percentile75, Kurtosis, Skewness, Amplitude1, Amplitude2, Frequency2, Mean Frequency
	y	Mean, STD, Max, Min, Percentile25, Percentile50, Percentile75, Kurtosis, Skewness, Amplitude1, Frequency2
	magnitude	Mean, STD, Max, Min, Percentile25, Percentile50, Percentile75, Kurtosis, Skewness, Amplitude, Frequency2
Γυροσκόπιο	x	Mean, Max, Min, Percentile75, Kurtosis, Skewness, Amplitude1, Frequency2, Mean Frequency
	y	Mean, Min, Kurtosis, Skewness, Frequency2
	magnitude	Mean, Min, Kurtosis, Skewness, Frequency2

Σημειώνεται ότι, μετά την τελική επιλογή έγινε η επανάληψη του προηγούμενου βήματος, δηλαδή επαληθεύθηκε ότι και για τα υποσύνολα των χαρακτηριστικών που επιλέχθηκαν, το μέγεθος του παραθύρου και το ποσοστό επικάλυψης παραμένουν τα βέλτιστα και για τους δύο αισθητήρες.

4.2.2 Χαρακτηριστικά Δεδομένων Αφής

Στην περίπτωση των δεδομένων αφής η διαδικασία εξαγωγής χαρακτηριστικών είναι αρκετά πιο απλή. Τα χαρακτηριστικά εξαρτώνται αποκλειστικά από το gesture (tap ή swipe) που εξετάζεται. Αυτά που απαιτούνται είναι ο κατάλληλος μετασχηματισμός των δεδομένων και η βέλτιστή επιλογή χαρακτηριστικών. Όσον αναφορά των μετασχηματισμό, αναφέρεται ότι λόγω της ποικιλίας συσκευών, είναι αναγκαία η μετατροπή των χειρονομιών έτσι ώστε όλα τα δεδομένα να προσαρμοστούν σε συσκευή συγκεκριμένου μεγέθους και να εξασφαλιστεί η σωστή αξιολόγηση του συστήματος σε δεδομένα μη εξουσιοδοτημένων χρηστών. Ως προεπιλογή τέθηκε μια συσκευή με πλάτος 400 και ύψος 700 pixels.

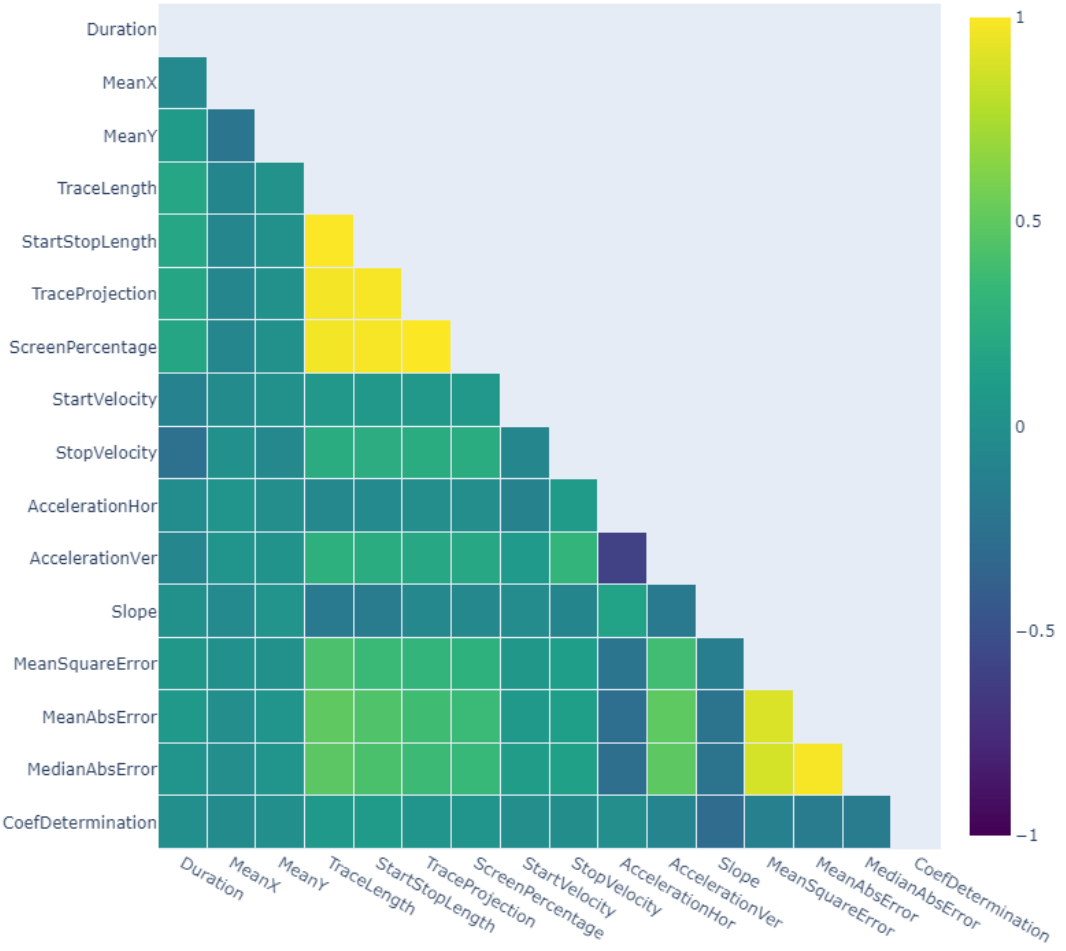
4.2.2.1 Τελική Επιλογή Χαρακτηριστικών

Για τα swipes, που αποτελούν το κύριο σημείο ενδιαφέροντος, η αρχική επιλογή χαρακτηριστικών βασίστηκε στην βιβλιογραφία, ενώ η τελική έγινε από πίνακες συσχέτισης και δοκιμές για κάθε παιχνίδι. Για τα taps επιλέχθηκε απλά το χαρακτηριστικό της διάρκειας (duration), με σκοπό να παρατηρηθεί η συμπεριφορά του συστήματος σε τέτοια δεδομένα.

Στον παρακάτω πίνακα (Πίνακας 8) φαίνονται τα αρχικά χαρακτηριστικά που επιλέχθηκαν για τα swipes και στο Σχήμα 34 ο πίνακας συσχέτισης αυτών για το Mathisis, που είναι αντιπροσωπευτικός και για τα υπόλοιπα παιχνίδια που περιέχουν swipes (Focus, Reacton).

Πίνακας 8: Αρχικά Χαρακτηριστικά Swipes

Χαρακτηριστικά	Περιγραφή
Duration	Η συνολική διάρκεια του swipe σε ms
Mean X	Το μέσο σημείο του swipe στον οριζόντιο άξονα
Mean Y	Το μέσο σημείο του swipe στον κάθετο άξονα
Trace Length	Το συνολικό μήκος του swipe
Start Stop Length	Η Ευκλείδεια απόσταση του τελευταίου και του αρχικού σημείου
Trace Projection	Η απόσταση των τελικών και αρχικών οριζόντιων ή κάθετων συντεταγμένων του swipe, αναλόγως του προσανατολισμού του
Screen Percentage	Το ποσοστό της οθόνης που καλύπτει το swipe
Start Velocity	Η αρχική ταχύτητα του swipe
Stop Velocity	Η τελική ταχύτητα του swipe
Horizontal Acceleration	Η οριζόντια επιτάχυνση του swipe
Vertical Acceleration	Η κατακόρυφη επιτάχυνση του swipe
Slope	Η κλίση της ευθείας που προσεγγίζει καλύτερα το swipe
Mean Square Error	Το μέσο τετραγωνικό σφάλμα μεταξύ του swipe και της ευθείας γραμμής
Mean Absolute Error	Το μέσο απόλυτο σφάλμα μεταξύ του swipe και της ευθείας γραμμής
Median Absolute Error	Το διάμεσο απόλυτο σφάλμα μεταξύ του swipe και της ευθείας γραμμής
Coefficient of Determination	Ο συντελεστής προσδιορισμού μεταξύ του swipe και της ευθείας γραμμής



Σχήμα 34: Πίνακας Συσχετίσεων Χαρακτηριστικών Swipes

Τα τελικά χαρακτηριστικά που επιλέχθηκαν, τόσο για τα swipes όσο και για τα taps, αναγράφονται στο παρακάτω πίνακα (Πίνακας 9)

Πίνακας 9: Τελικά Χαρακτηριστικά Gestures

Είδος Gesture	Τελικά Χαρακτηριστικά
Tap	Duration
Swipe	Duration, Mean X, Mean Y, Trace Length, Trace Projection, Start Velocity, Stop Velocity, Horizontal Acceleration, Vertical Acceleration, Slope, Mean Square Error, Coefficient of Determination

4.3 Επιλογή Βέλτιστων Μοντέλων Μηχανικής Μάθησης

Επόμενο πρόβλημα αποτελεί η σχεδίαση ενός συστήματος μοντέλων μηχανικής μάθησης και η βέλτιστη επιλογή των παραμέτρων τους. Βασική ιδέα είναι η σχεδίαση ενός ανεξάρτητου ταξινομητή για κάθε κατηγορία δεδομένων (επιταχυνσιόμετρο, γυροσκόπιο, swipes, taps), ώστε το τελικό σύστημα να μπορεί να λειτουργήσει και στο ενδεχόμενο που υπάρχουν δεδομένα από μία κατηγορία.

Αρχικά, κάθε ταξινομητής αποτελούνταν από έναν αλγόριθμο RBF-OCSVM, δηλαδή OCSVM με RBF kernel, επιλογή που έγινε καθώς από την βιβλιογραφία και τα πειράματα προκύπτει ότι αποδίδει καλύτερα από άλλους στο συγκεκριμένο πρόβλημα. Συγκεκριμένα, στην python η βιβλιοθήκη που χρησιμοποιήθηκε υλοποιεί τον OCSVM με βάση την εκδοχή των Schölkopf κ.ά. [26]. Σε αυτή την περίπτωση, το πρόβλημα που υπάρχει είναι η βέλτιστη επιλογή των παραμέτρων nu και gamma. Όπως αναφέρουν οι Karanikiotis κ.ά.[44], οι άνθρωποι έχουν πολύ διαφορετικές συμπεριφορές και τα χαρακτηριστικά που εξάγονται από τον καθένα έχουν αρκετά μεγάλη διακύμανση. Έτσι, η επιλογή ενός μοναδικού μοντέλου με βέλτιστές παραμέτρους, για ένα ευρύτερο σύνολο χρηστών είναι αδύνατη. Στο πλαίσιο αυτό, για κάθε ταξινομητή, αντί να γίνει χρήση ενός μοναδικού μοντέλου RBF-OCSVM, με ένα ζεύγος τιμών nu και gamma, χρησιμοποιείται ένας μεγάλος αριθμός μοντέλων, καλύπτοντας μια ευρύτερη περιοχή nu – gamma.

Όλα τα μοντέλα RBF-OCSVM, με τις διαφορετικές παραμέτρους, χρησιμοποιούν το ίδιο σύνολο εκπαίδευσης και εκπαιδεύονται με τον ίδιο ακριβώς τρόπο. Τα εκπαιδευμένα μοντέλα που προκύπτουν, στην ουσία είναι αναπαραστάσεις των αντίστοιχων υπερπιπέδων που διαχωρίζουν τις παρατηρήσεις του συνόλου εκπαίδευσης από τον υπόλοιπο χώρο. Η μέση

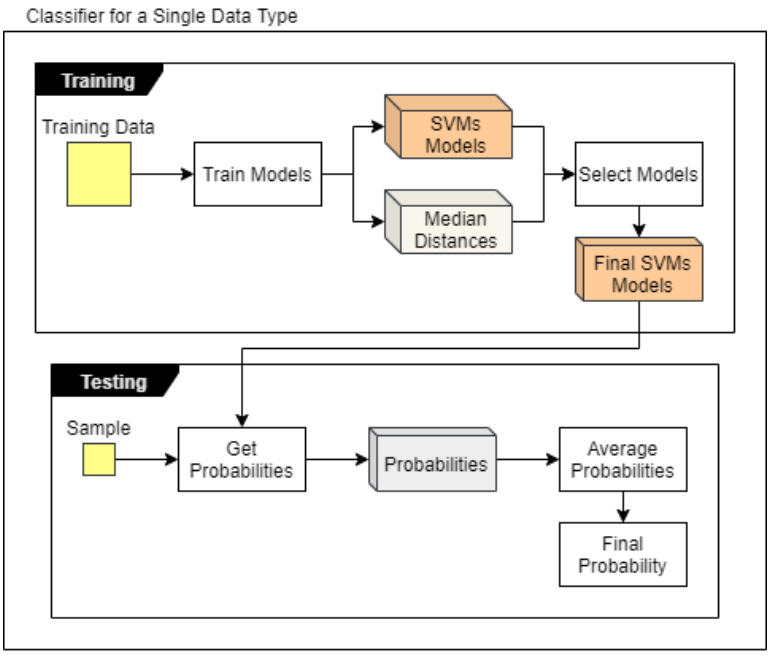
απόσταση που έχει ένα υπερεπίπεδο από τις παρατηρήσεις εκπαίδευσης είναι ένα μέτρο το όποιο δείχνει πόσο καλά το αντίστοιχο μοντέλο έχει μοντελοποίηση την συμπεριφορά του χρήστη. Όσο μικρότερη είναι αυτή η απόσταση, τόσο καλύτερη η μοντελοποίηση. Έτσι, σε συνέχεια της εκπαίδευσης, πραγματοποιείται η επιλογή συγκεκριμένου αριθμού μοντέλων, που παρουσιάζουν τις μικρότερες αυτές αποστάσεις.

Κατά την φάση της δοκιμής, κάθε νέο δείγμα ταξινομείται από όλα τα μοντέλα που επιλέχθηκαν. Στην πραγματικότητα, κάθε μοντέλο επιστρέφει την πιθανότητα το δείγμα να ανήκει ή όχι στην κλάση του χρήστη. Η πιθανότητα αυτή υπολογίζεται από μια συνάρτηση, η οποία είναι διαφορετική για κάθε μοντέλο και ορίζεται από τον λόγο της απόστασης του δείγματος από το υπερεπίπεδο προς την μέγιστη απόσταση του συνόλου εκπαίδευσης από το υπερεπίπεδο. Στο τέλος, κάθε ταξινομητής επιστρέφει τον μέσο όρο των πιθανοτήτων όλων των μοντέλων που επιλέχθηκαν. Αν η μέση πιθανότητα κυμαίνεται στο διάστημα (0, 1] το δείγμα ανήκει στην κλάση του ιδιοκτήτη, ενώ αν κυμαίνεται στο διάστημα [-1, 0] το δείγμα δεν ανήκει στην κλάση του ιδιοκτήτη.

Οι παραπάνω διαδικασίες παρουσιάζονται σχηματικά στο παρακάτω διάγραμμα (Σχήμα 35) και με βάση αυτήν τη λογική, προκύπτουν δύο βασικά ερωτήματα:

- Ποιες είναι οι κατάλληλες περιοχές nu – gamma για κάθε κατηγορία δεδομένων;

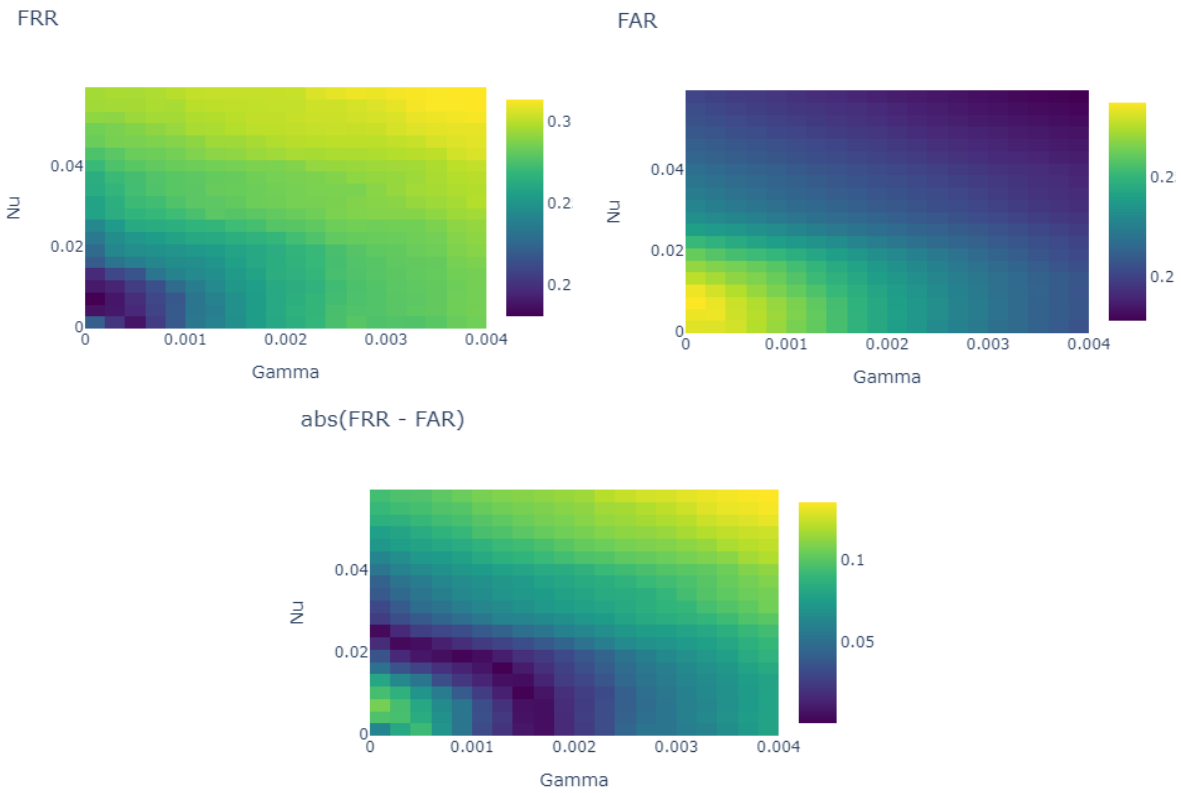
- Ποιος είναι ο κατάλληλος αριθμός μοντέλων που για κάθε κατηγορία δεδομένων;



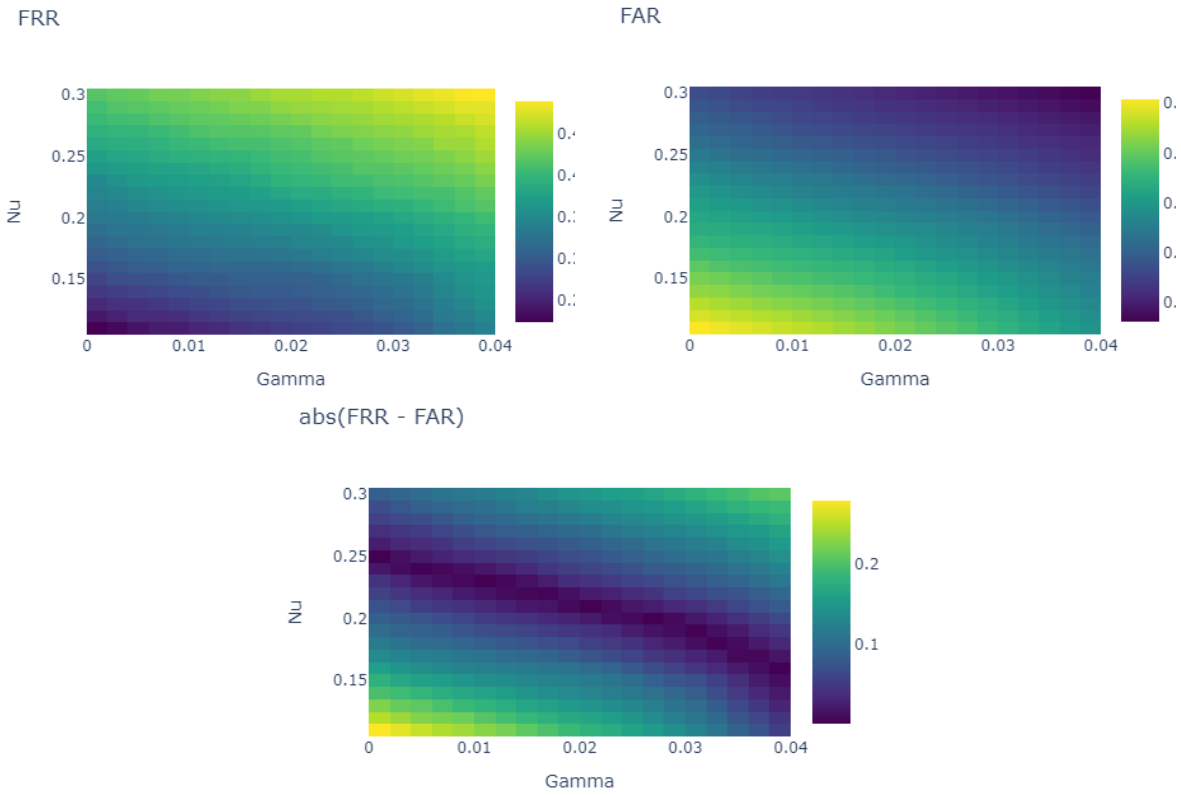
Σχήμα 35: Εκπαίδευση & Δοκιμή Ταξινομητή Μίας Κατηγορίας Δεδομένων

4.3.1 Επιλογή Περιοχών Παραμέτρων

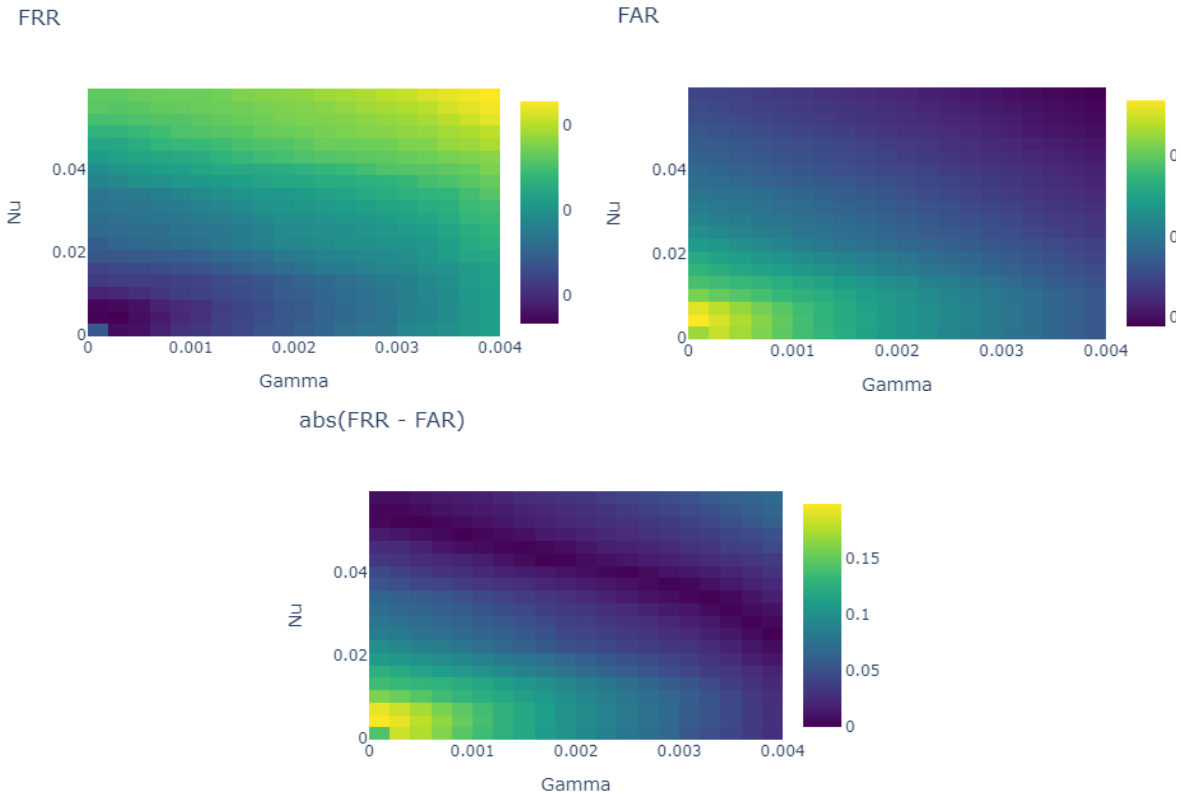
Για την επιλογή κατάλληλων παραμέτρων nu – gamma, απαραίτητη ήταν η εκτέλεση αναζητήσεων πλέγματος. Για κάθε κατηγορία παιχνιδιού και δεδομένων πραγματοποιήθηκαν πειράματα για διάφορες τιμές nu και gamma και δημιουργήθηκαν χάρτες που οπτικοποιούν την συμπεριφορά των μετρικών FAR και FRR. Παρακάτω παρουσιάζονται οι χάρτες για τα δεδομένα επιταχυνσιομέτρου στο Mathisis (Σχήμα 36) και στο Focus (Σχήμα 38) αλλά και για τα δεδομένα του γυροσκοπίου στο Mathisis (Σχήμα 37). Σημειώνεται ότι, ο τρίτος χάρτης παρουσιάζει την απόλυτη διαφορά των άλλων δύο και βοηθάει στον εντοπισμό περιοχών που οι μετρικές FAR και FRR έχουν την μικρότερη απόκλιση. Οι περιοχές αυτές είναι που εξασφαλίζουν την ταυτόχρονη επίτευξη ασφάλειας και ευχρηστίας και έτσι η αναζήτηση βέλτιστων παραμέτρων ανάγεται στην αναζήτηση παραμέτρων που αντικατοπτρίζουν αυτές τις περιοχές.



Σχήμα 36: Αναζήτηση Πλέγματος nu & gamma - Mathisis, Επιταχυνσιόμετρο



Σχήμα 37: Αναζήτηση Πλέγματος nu & gamma - Mathisis, Γυροσκόπιο



Σχήμα 38: Αναζήτηση Πλέγματος nu & gamma - Focus, Επιταχυνσιόμετρο

Παρατηρείται πως η συμπεριφορά των μετρικών διαφέρει μεταξύ διαφορετικών παιχνιδιών και δεδομένων. Τα δεδομένα του επιταχυνσιομέτρου παρουσιάζουν διαφορετική συμπεριφορά στο Mathisis και στο Focus, ενώ ταυτόχρονα διαφέρουν και από αυτά του γυροσκοπίου στο ίδιο παιχνίδι. Η συμπεριφορά αυτή παρουσιάζεται σε όλες τις κατηγορίες δεδομένων και συνεπώς για την δημιουργία ταξινομητών, που θα μπορούν να αποδώσουν καλά σε όλα τα παιχνίδια, χρειάζεται η ταυτόχρονη εξέταση όλων των παιχνιδιών για μία κατηγορία δεδομένων με σκοπό την εξαγωγή μίας περιοχής που θα καλύπτει τις ανάγκες όλων των παιχνιδιών ταυτόχρονα. Οι τελικές περιοχές που διαμορφώθηκαν για κάθε κατηγορία φαίνονται στο παρακάτω πίνακα (Πίνακας 10):

Πίνακας 10: Περιοχές nu & gamma ανά Κατηγορία Δεδομένων

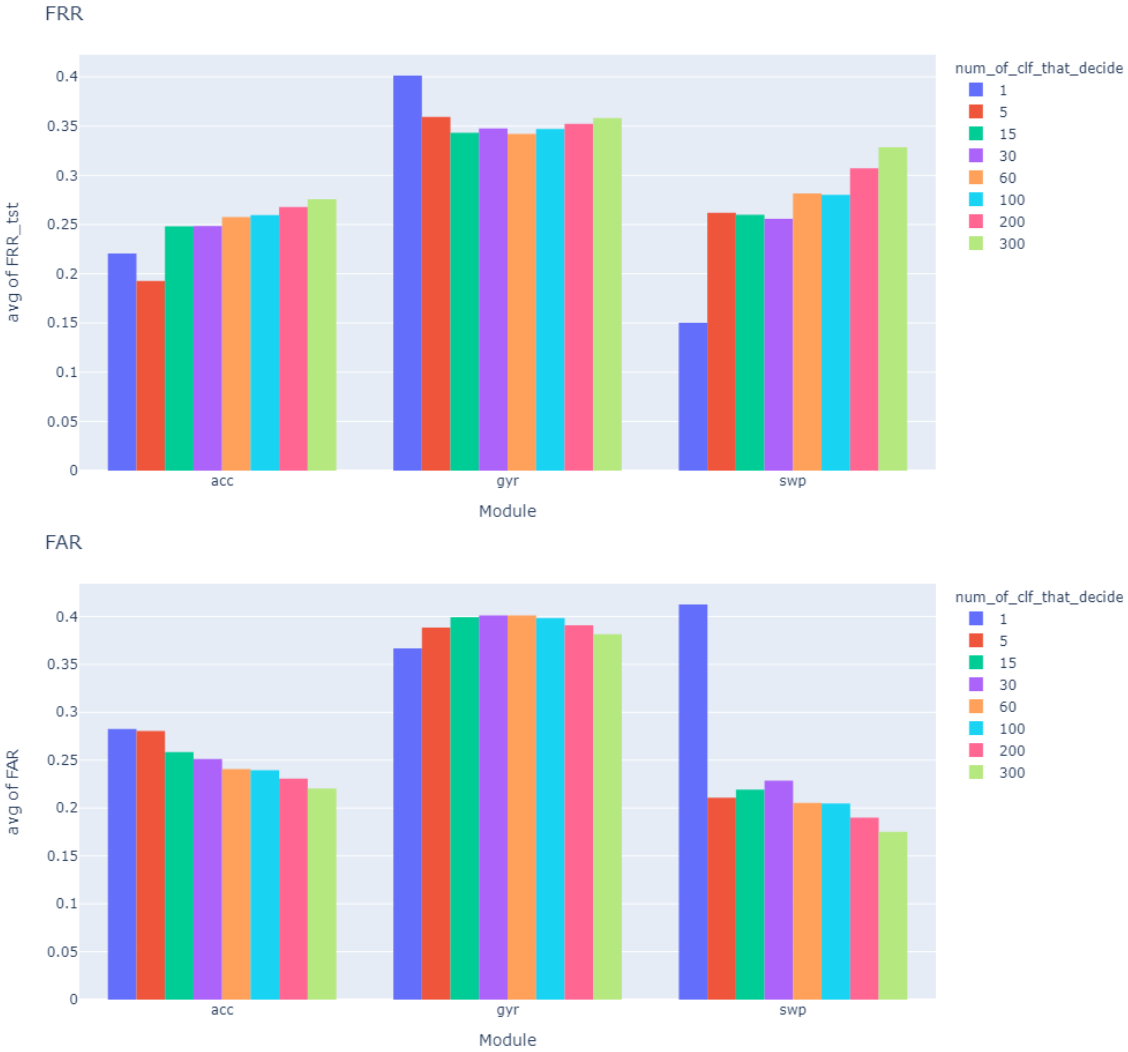
Κατηγορία	Nu			Gamma		
	Αρχική Τιμή	Τελική Τιμή	Βήμα	Αρχική Τιμή	Τελική Τιμή	Βήμα
Επιταχυνσιόμετρο	0.001	0.06	0.003	0.0001	0.004	0.0002
Γυροσκόπιο	0.11	0.31	0.01	0.001	0.04	0.002
Swipes	0.01	0.21	0.01	0.001	0.06	0.003
Taps	0.02	0.6	0.03	0.7	0.795	0.005

4.3.2 Επιλογή Πλήθους Τελικών Μοντέλων

Παρόμοια λογική εφαρμόστηκε και για την επιλογή του κατάλληλου αριθμού των μοντέλων, που θα συνεργάζονται για την εξαγωγή της τελικής πιθανότητας, σε κάθε κατηγορία δεδομένων. Για κάθε παιχνίδι και για κάθε τύπο δεδομένων δοκιμάστηκαν οι τιμές [1, 5, 15, 50, 100, 200, 300] και καταγράφηκαν οι μετρικές FRR και FAR. Τα συμπεράσματα που προέκυψαν, έδειξαν ότι 50 μοντέλα δίνουν ικανοποιητική απόδοση σε κάθε κατηγορία δεδομένων. Ωστόσο, μετά την κατασκευή του τελικού συστήματος και συστήματος αξιολόγησης, η διαδικασία επαναλήφθηκε για τις τιμές [1, 5, 15, 30, 60, 100, 200, 300] και τα αποτελέσματα για το Mathisis φαίνονται παρακάτω (Σχήμα 39). Οι τελικές τιμές που επιλέχθηκαν παρουσιάζονται στον παρακάτω πίνακα (Πίνακας 11).

Πίνακας 11: Βέλτιστος Αριθμός Μοντέλων ανά Κατηγορία Δεδομένων

Κατηγορία	Βέλτιστος Αριθμός Μοντέλων
Επιταχυνσιόμετρο	30
Γυροσκόπιο	60
Swipes	60
Taps	60



Σχήμα 39: Βέλτιστος Αριθμός Μοντέλων ανά Κατηγορία Δεδομένων - Mathisis

4.4 Αξιολόγηση & Σύνοψη Συστήματος

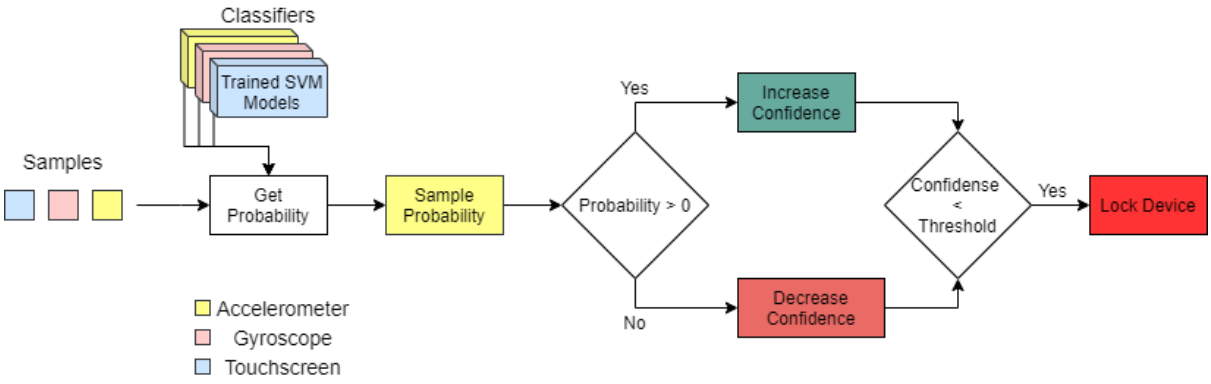
Η σχεδίαση του τελικού συστήματος βασίστηκε στα παραπάνω αποτελέσματα. Ωστόσο, αυτά δεν είναι τα μοναδικά στοιχεία που το αποτελούν. Για την ολοκληρωμένη σχεδίασή του και την εκτέλεση διαφορετικών πειραμάτων, έγινε η ένταξή τους σε μια ακολουθία βημάτων που εμπεριέχει: την συνολική προεπεξεργασία δεδομένων, την εξαγωγή των βέλτιστων χαρακτηριστικών, την εκπαίδευση των ταξινομητών αλλά και την τελική αξιολόγηση που προσομοιώνει σενάρια πραγματικής χρήσης.

4.4.1 Μέθοδος Αξιολόγησης

Η αξιόλογη αφορά την καταγραφή των μετρικών που αναφέρθηκαν στην ενότητα 2.6. Αυτό που διαφέρει στην συγκεκριμένη περίπτωση είναι ότι υπάρχουν 4 διαφορετικοί ταξινομητές, που ο καθένας εξάγει την δικιά του απόφαση. Συνεπώς, στο σύστημα αξιολόγησης συμπεριλαμβάνεται και το σύστημα που δέχεται αυτές τις αποφάσεις και επιλέγει τελικά αν θα κλειδώσει την συσκευή ή όχι.

Η ιδέα είναι ότι αφού ο χρήστης ξεκλειδώσει την συσκευή, θα γίνεται η καταγραφή δεδομένων από του αισθητήρες, τα δεδομένα αυτά θα εισάγονται σε μία ουρά και κάθε ταξινομητής θα καλείται να βγάλει μια απόφαση, όταν στην έξοδο της ουράς βρεθεί εγγραφή του αντίστοιχου τύπου. Η χρήση κάθε μεμονωμένης απόφασης για το κλείδωμα της συσκευής είναι μη αποδοτική, κάτι που οφείλεται στις ψηλές σχετικά μετρικές FRR και FAR των ταξινομητών που φαίνονται και στα παραπάνω σχήματα (Σχήμα 36, Σχήμα 37, Σχήμα 38 και Σχήμα 39). Για τον λόγο αυτό, γίνεται η εισαγωγή ενός συστήματος εμπιστοσύνης, παρόμοιο με αυτό που πρότειναν οι Karanikiotis κ.ά. [44], όπου οι ταξινομητές επηρεάζουν την ίδια μεταβλητή ανάλογα με την απόφασή τους και αν η μεταβλητή πέσει κάτω από ένα συγκεκριμένο όριο, τότε η συσκευή κλειδώνει.

Πιο συγκεκριμένα, τίθεται ένα αρχικό επίπεδο εμπιστοσύνης και ένα κατώτατο όριο. Κάθε ταξινομητής επιστρέφει την πιθανότητα ένα δείγμα να ανήκει ή όχι στην κλάση του ιδιοκτήτη, στο διάστημα [-1, 1]. Αυτή η πιθανότητα πολλαπλασιάζεται με μία σταθερά, ανάλογη του παιχνιδιού και του προσήμου, και έναν αριθμό που εκφράζει την εμπιστοσύνη του συστήματος σε κάθε ταξινομητή (Εξ.6). Ο τελικός αριθμός που προκύπτει προστίθεται στο επίπεδο εμπιστοσύνης και αν αυτό πέσει κάτω από το όριο τότε η συσκευή κλειδώνει. Η παραπάνω διαδικασία παρουσιάζεται στο παρακάτω σχήμα (Σχήμα 40).



Σχήμα 40: Σύστημα Εμπιστοσύνης (Confidence Level)

$$CL_n = \begin{cases} CL_{n-1} + PositiveStep(Game) * Weights(DataType) * abs(p), & p > 0 \\ CL_{n-1} + NegativeStep(Game) * Weights(DataType) * abs(p), & p \leq 0 \end{cases} \quad (Εξ.6)$$

Περιγραφή όρων:

CL_n	: Η υφιστάμενη τιμή του επιπέδου εμπιστοσύνης.
CL_{n-1}	: Η καινούργια τιμή του επιπέδου εμπιστοσύνης.
$PositiveStep(Game)$	: Θετική σταθερά ανάλογη του παιχνιδιού (Πίνακας 12).
$NegativeStep(Game)$	: Αρνητική σταθερά ανάλογη του παιχνιδιού (Πίνακας 12).
$Weights(DataType)$	: Θετική σταθερά ανάλογη του τύπου δεδομένων.
$abs(p)$	: Η απόλυτη τιμή της πιθανότητα.

Η αρχική τιμή εμπιστοσύνης (initial confidence level), το κατώτατο όριο (threshold) αλλά και τα βήματα αύξησης (positive step) και μείωσης (negative step) επιλέχθηκαν μετά από διάφορα πειράματα και παρουσιάζονται στο παρακάτω πίνακα (Πίνακας 12). Τα βάρη που αφορούν τον τύπο δεδομένων, ορίζονται από την μετρική FAR των αντίστοιχων ταξινομητών στο σύνολο εκπαίδευσης.

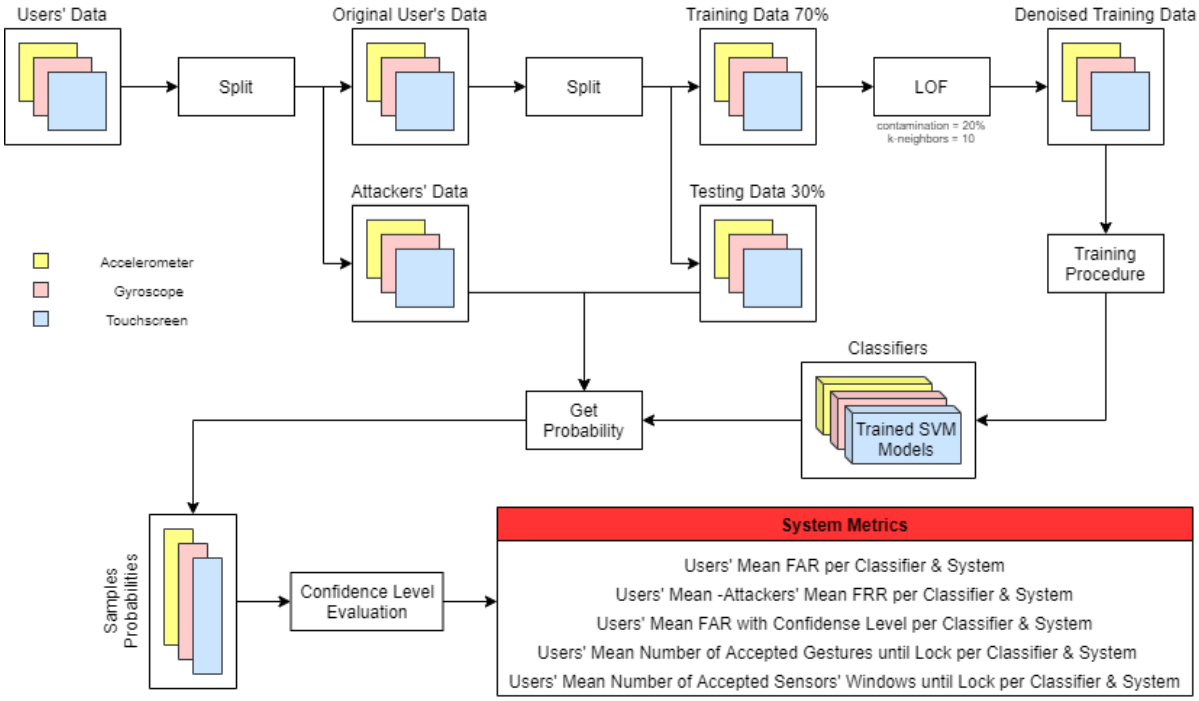
Πίνακας 12: Παράμετροι Επιπέδου Εμπιστοσύνης

Initial Confidence Level			60		
Threshold			35		
	Mathisis	**Focus**	**Reacton**	**Speedy**	**Memoria**
Negative Step	-15	-15	-15	-15	-15
Positive Step	+10	+10	+10	+10	+10

Στο σημείο αυτό σημειώνεται ότι σε ένα τέτοιο σύστημα οι μετρικές FAR και FRR δεν εκφράζουν αντιπροσωπευτικά την αποτελεσματικότητα του συστήματος. Πλέον η FRR πρέπει να οριστεί ως το ποσοστό των φορών που ο χρήστης κλειδώθηκε έξω σε σύγκριση με το σύνολο των δειγμάτων αξιολόγησης. Ενώ η μετρική FAR δεν μπορεί να υπολογιστεί και για αυτό τον λόγο οι μετρικές που εξετάζονται είναι ο αριθμός των χειρονομιών και των παραθύρων αισθητήρων κίνησης που πρόλαβε να δημιουργήσει ένας μη εξουσιοδοτημένος χρήστης μέχρι τελικά να κλειδώσει η συσκευή.

4.4.2 Σύνοψη Συστήματος

Συνοψίζοντας, το τελικό σύστημα είναι αυτό που ενσωματώνει τα αποτελέσματα και τις επιλογές των παραπάνω μελετών και δημιουργεί μια ροή πληροφορίας από την είσοδο με τα δεδομένα των χρηστών προς την έξοδο με τις μετρικές αξιολόγησης του συστήματος. Πιο συγκεκριμένα ένα ενδεικτικό διάγραμμα του συστήματος αποτυπώνεται στο παρακάτω σχήμα (Σχήμα 41).



Σχήμα 41: Σύνοψη Συστήματος

Όπως φαίνεται, η είσοδος του συστήματος είναι οι πίνακες των δεδομένων του επιταχυνσιομέτρου, του γυροσκοπίου και των χειρονομιών. Αυτοί οι πίνακες περιέχουν δεδομένα όλων των χρηστών προς εξέταση και συγκεκριμένα είναι οι πίνακες που προκύπτουν μετά την εξαγωγή χαρακτηριστικών, όπως αυτή περιγράφεται στην ενότητα 4.2. Στο παραπάνω σχήμα, αυτή η διαδικασία, καθώς και η διαδικασία επιλογής χρηστών, που περιγράφεται στην ενότητα 4.1 παραλείπονται για λόγους ευχρηστίας και εύκολης κατανόησης του συστήματος.

Έτσι, αφού το σύστημα λάβει τους πίνακες με τα χαρακτηριστικά αρχικό μέλημα έχει τον ορισμό ενός χρήστη ως ιδιοκτήτη και τον διαχωρισμό των δεδομένων του από τους υπόλοιπους χρήστες, οι οποίοι αναλαμβάνουν τον ρόλο κακόβουλων χρηστών. Τα δεδομένα αυτών των χρηστών, μαζί με το 30% των δεδομένων του ιδιοκτήτη θα αποτελέσουν το σύνολο αξιολόγησης του συστήματος, ενώ το υπόλοιπο 70% των δεδομένων του ιδιοκτήτη θα αποτελέσουν το σύνολο εκπαίδευσης των ταξινομητών. Σημειώνεται ότι, όταν το σύστημα εξετάζει το σύνολο χρηστών εκπαίδευσης (Πίνακας 5), τα δεδομένα των κακόβουλων χρηστών και το 30% των δεδομένων του ιδιοκτήτη αποτελούν στην ουσία το σύνολο επικύρωσης (validation set), που χρησιμοποιείται στο στάδιο της βελτιστοποίησης του συστήματος. Στην περίπτωση του συνόλου χρηστών αξιολόγησης (Πίνακας 5), τα ίδια δεδομένα αποτελούν το σύνολο αξιολόγησης του συστήματος (testing set).

Όπως φαίνεται και από το παραπάνω σχήμα, το επόμενο βήμα είναι η αποθορυβοποίηση του συνόλου εκπαίδευσης. Το βήμα αυτό υλοποιείται με την βοήθεια του αλγορίθμου LOF, που στοχεύει στον εντοπισμό ακραίων εγγραφών και στην απομάκρυνσή τους από το σύνολο εκπαίδευσης. Σκοπός του βήματος αυτού είναι η κατασκευή αποτελεσματικότερων μοντέλων, με καλύτερη ικανότητα γενίκευσης. Ωστόσο, η αποτελεσματικότητα αυτής της διαδικασίας μπορεί να αμφισβητηθεί και χρειάζονται πειράματα για να αποδειχτεί η σημασία της. Για τον λόγο αυτό, στο επόμενο κεφάλαιο παρουσιάζονται τόσο πειράματα που εφαρμόζουν αποθορυβοποίηση με LOF, όσο και άλλα που την παραλείπουν.

Τέλος, τα δεδομένα εκπαίδευσης (αποθορυβοποιημένα ή όχι) χρησιμοποιούνται για την εκπαίδευση των ταξινομητών, όπως αυτή περιγράφεται στην ενότητα 4.3, ενώ τα δεδομένα αξιολόγησης για την προσομοίωση χρήσης του συστήματος και την εξαγωγή μετρικών αξιολόγησης.

5 Πειράματα & Αποτελέσματα

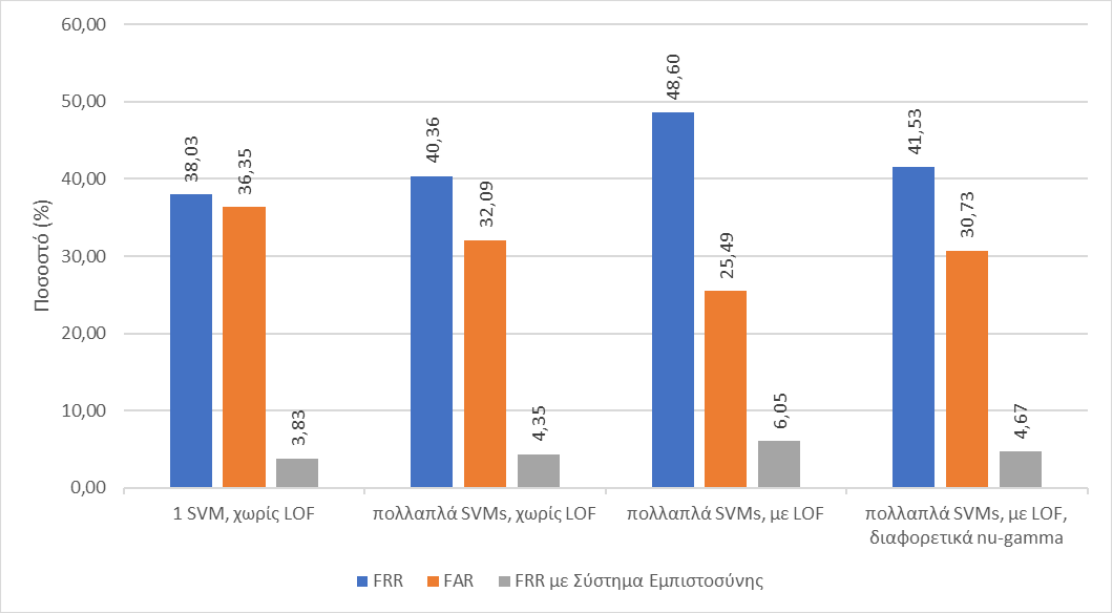
Αφού παρουσιάστηκε η μεθοδολογία, έγινε ο προσδιορισμός των παραμέτρων και αναπτύχθηκε η δομή του συστήματος, στην ενότητα αυτή παρουσιάζονται τα αποτελέσματα των πειραμάτων που εκτελέστηκαν. Αυτά αφορούν όλες τις κατηγορίες παιχνιδιού, για κάθε τύπο δεδομένων και περιγράφονται χρησιμοποιώντας τις μετρικές που αναφέρθηκαν στην προηγούμενη ενότητα. Όπως υπογραμμίστηκε στην υποενότητα 4.1.2, υπάρχουν αποτελέσματα από ένα μικρότερο σύνολο χρηστών και ένα μεγαλύτερο. Το πρώτο απευθύνεται στην διαδικασία της εκπαίδευσης και βελτιστοποίησης, ενώ το δεύτερο εξετάζει την αποτελεσματικότητα του συστήματος σε τελείως ξένα δεδομένα.

Στόχος της ενότητα αυτής είναι να δείξει την απόδοση του συστήματος δίνοντας βάση στα παιχνίδια Mathisis και Focus, καθώς παιχνίδια όπως τα Reacton, Memoria και Speedy περιέχουν taps, τα οποία δεν μελετήθηκαν σε βάθος. Πιο συγκεκριμένα, παρουσιάζονται τα οφέλη των επιλογών που έγιναν, εξετάζεται η σημασία της αποθορυβοποίησης των δεδομένων στο στάδιο της προεπεξεργασίας και αναλύεται η ικανότητα γενίκευσης των μοντέλων. Επιπλέον, φτάνοντας στο τέλος της ενότητας, παρατίθενται συγκρίσεις με άλλες μεθόδους, αναδεικνύεται ο ρόλος του εν λόγω συστήματος στο πρόβλημα της έμμεσης αυθεντικοποίησης και δίνονται κάποια συμπεράσματα.

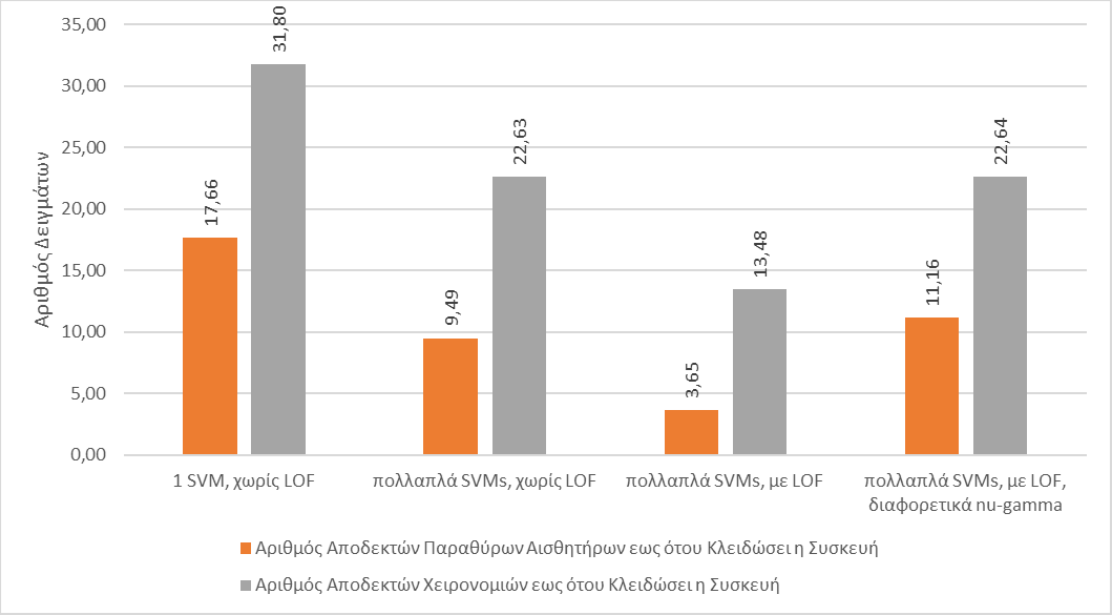
5.1 Πειράματα Χρηστών Συνόλου Εκπαίδευσης

Κατά τις διαδικασίες εκπαίδευσης και βελτιστοποίησης προέκυψαν αρκετά χρήσιμα συμπεράσματα για τις διάφορες παραμέτρους του συστήματος. Πέραν αυτών όμως, η αξιολόγηση του συστήματος με το σύνολο εκπαίδευσης, δίνει χρήσιμες πληροφορίες για το επίπεδο προεπεξεργασίας που απαιτείται και την αρχιτεκτονική των μοντέλων.

Στα παρακάτω διαγράμματα φαίνονται τόσο οι μετρικές FAR και FRR, όσο και οι μετρικές που εξάγονται με την ενσωμάτωση του συστήματος εμπιστοσύνης. Στο Σχήμα 42 αναπαρίστανται οι μετρικές που εκφράζουν ποσοστό, ενώ στο Σχήμα 43 αυτές που εκφράζονται σε αριθμό δειγμάτων. Τα διαγράμματα παρουσιάζουν τα αποτελέσματα τεσσάρων πειραμάτων, που πραγματοποιήθηκαν στο σύνολο των χρηστών εκπαίδευσης. Στο πρώτο (1 SVM, χωρίς LOF) χρησιμοποιείται 1 μόνο SVM για κάθε τύπο δεδομένων χωρίς να πραγματοποιείται προεπεξεργασία, στο δεύτερο (πολλαπλά SVMs, χωρίς LOF) χρησιμοποιούνται πολλαπλά SVMs για κάθε τύπο δεδομένων χωρίς προεπεξεργασία, στο τρίτο (πολλαπλά SVMs, με LOF) χρησιμοποιώντας της αρχιτεκτονική του δεύτερου εισάγεται ένα επίπεδο προεπεξεργασίας με LOF για την αποθορυβοποίηση των δειγμάτων εκπαίδευσης και, τέλος, στο τέταρτο ελέγχεται η απόδοση του τρίτου χρησιμοποιώντας διαφορετικές περιοχές nu – gamma.



Σχήμα 42: Ποσοστιαίες Μετρικές σε Πειράματα στο Σύνολο Χρηστών Εκπαίδευσης



Σχήμα 43: Μετρικές Αριθμού Δειγμάτων σε Πειράματα στο Σύνολο Χρηστών Εκπαίδευσης

Πιο συγκεκριμένα, τα αποτελέσματα των πειραμάτων προκύπτουν από τον μέσο όρο των μετρικών, όλων των χρηστών του συνόλου εκπαίδευσης και των 5 παιχνιδιών (Mathisis, Focus, Reacton, Memoria, Speedy). Δηλαδή, αφού βρέθηκαν οι μετρικές κάθε χρήστη, για κάθε παιχνίδι, υπολογίστηκε ο μέσος όρος για κάθε παιχνίδι και στην συνέχεια ο τελικός μέσος όρος, για κάθε μετρική.

Παρατηρώντας τα παραπάνω ραβδογράμματα, ιδιαίτερα στο πρώτο σχήμα (Σχήμα 42), γίνεται ξεκάθαρη η αποτελεσματικότητα του συστήματος εμπιστοσύνης στην μείωση της μετρικής FRR. Η FRR με Σύστημα Εμπιστοσύνης είναι περίπου 10 φορές χαμηλότερη από την απλή FRR και στα τέσσερα πειράματα. Ωστόσο, κύριος σκοπός αυτών των αποτελεσμάτων είναι η αξιολόγηση της σημασίας τόσο της χρήσης πολλαπλών SVMs, όσο και της αποθορυβοποίησης των δεδομένων εκπαίδευσης με LOF. Όσον αφορά τα πολλαπλά SVMs, τα πειράματα ένα και δύο δείχνουν πως η χρήση τους μειώνει σε σημαντικό βαθμό την FAR και τον αριθμό αποδεκτών δειγμάτων από αισθητήρες και χειρονομίες κακόβουλων χρηστών. Ταυτόχρονα όμως, παρατηρείται και μια όχι τόσο σημαντική αύξηση στις μετρικές FRR, βλέποντας και πάλι τα δύο πρώτα πειράματα, φαίνεται αύξηση 1-2%. Όσον αφορά την αποθορυβοποίηση των δεδομένων, φαίνεται να επηρεάζει και αυτή με παρόμοιο τρόπο τα αποτελέσματα. Από το δεύτερο και τρίτο πείραμα, παρατηρείται πως η μείωση των μετρικών ασφαλείας είναι σημαντική, αλλά ταυτόχρονα σημαντική είναι και η αύξηση στις μετρικές FRR. Το γεγονός ότι ένα αποθορυβοποιημένο σύνολο εκπαίδευσης περιέχει δείγματα με μικρότερη διαφοροποίηση δικαιολογεί την παραπάνω συμπεριφορά, ωστόσο η μείωση της λειτουργικότητας του συστήματος δεν αποσαφηνίζει την σημασία της αποθορυβοποίησης στην απόδοση του τελικού συστήματος. Τέλος, παρατηρώντας και το τέταρτο πείραμα, υπογραμμίζεται πόσο σημαντικό ρόλο έχουν οι παράμετροι nu και gamma. Εκτελώντας ακριβώς τα ίδια βήματα με το πείραμα τρία, αλλά με διαφορετικές παραμέτρους, παρατηρείται μείωση των FRR και αύξηση των μετρικών ασφάλειας.

Συνοψίζοντας, τα συμπεράσματα που προκύπτουν είναι τα εξής:

- Το σύστημα εμπιστοσύνης είναι σημαντική προσθήκη, καθώς βοηθάει στην σημαντική μείωση των FRR και συνεπώς στην διατήρηση πιο λειτουργικού συστήματος.

- Τα πολλαπλά SVMs εξυπηρετούν την ασφάλεια του συστήματος, ρίχνοντας σημαντικά τον αριθμό αλληλεπιδράσεων που προλαβαίνει να κάνει ένας κακόβουλος χρήστης μέχρι να γίνει αντιληπτός.

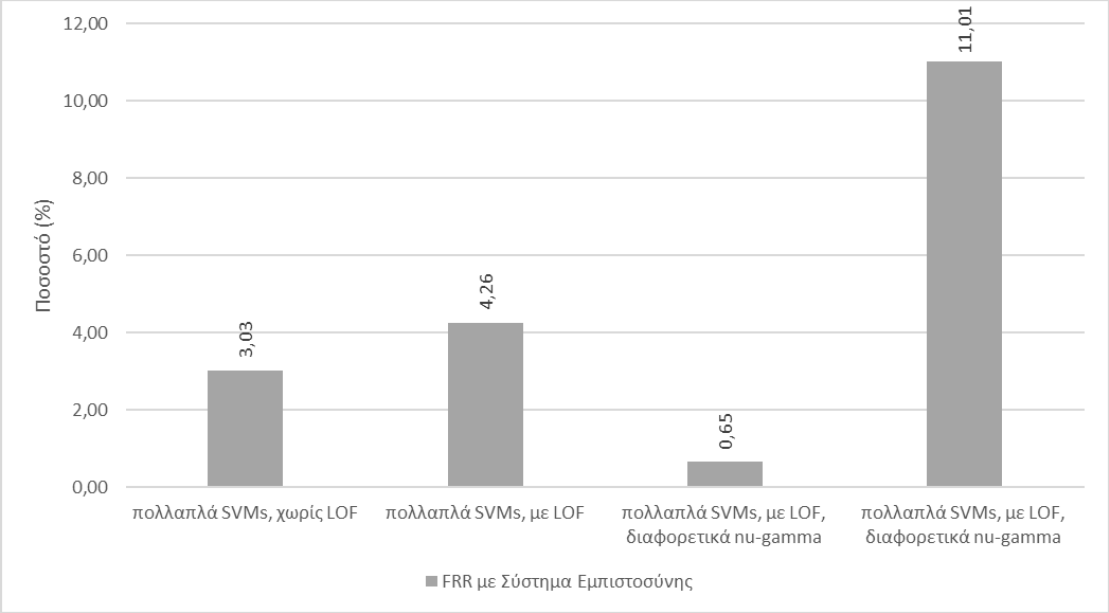
- Η αποθορυβοποίησης των δειγμάτων εκπαίδευσης με LOF εξυπηρετεί την ασφάλεια του συστήματος, αλλά ταυτόχρονα φαίνεται να μειώνει την χρηστικότητά του.

- Η χρήση διαφορετικών περιοχών nu – gamma μπορεί να χρησιμοποιηθεί για την εξισορρόπηση του συστήματος, κρατώντας μικρή την διαφορά μεταξύ των μετρικών ασφάλειας και ευχρηστίας.

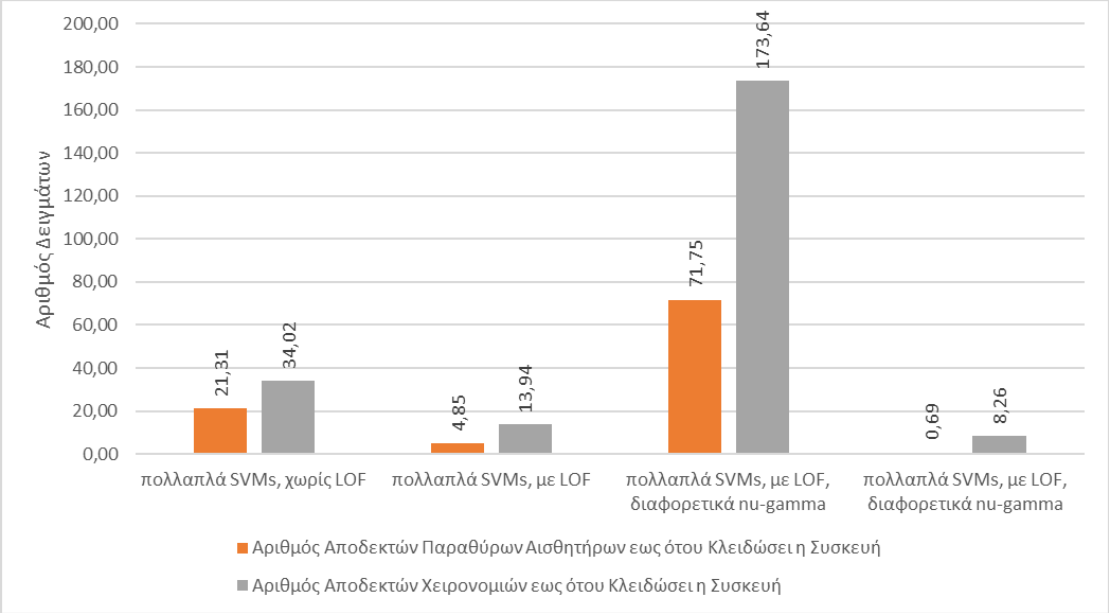
5.2 Πειράματα Χρηστών Συνόλου Αξιολόγησης

Στην υποενότητα αυτή παρουσιάζονται τα πειράματα που εκτελέστηκαν με το σύνολο των τελείως άγνωστων χρηστών. Εφαρμόζοντας τα συμπεράσματα της προηγούμενης ενότητας, στα πειράματα αυτά χρησιμοποιήθηκαν συστήματα πολλαπλών SVMs ανά τύπο δεδομένων, ο αριθμός των οποίων αναφέρθηκε σε προηγούμενη ενότητα (Πίνακας 11). Το πρώτο πείραμα αφορά σύστημα που δεν εφαρμόζει αποθορυβοποίηση στα δεδομένα εκπαίδευσης, ενώ τα υπόλοιπα πειράματα εξετάζουν συστήματα που ενσωματώνουν την αποθορυβοποίηση με LOF και χρησιμοποιούν διαφορετικές περιοχές nu – gamma. Στα παρακάτω ραβδογράμματα προβάλλονται μόνο οι μετρικές του τελικού συστήματος, δηλαδή οι μετρικές που προκύπτουν μετά την εφαρμογή του συστήματος εμπιστοσύνης, καθώς όπως αποδείχθηκε πριν, είναι μια σημαντική προσθήκη. Έτσι, στο Σχήμα 44 φαίνεται η μετρική FRR με Σύστημα Εμπιστοσύνης που εκφράζεται σε ποσοστό, ενώ στο Σχήμα 45 προβάλλονται ο αριθμός των αποδεκτών δειγμάτων από αισθητήρες και χειρονομίες, που προλαβαίνει να πραγματοποιήσει ένας κακόβουλος χρήστης μέχρι να κλειδώσει η συσκευή. Σημειώνεται ότι όπως και πριν, τα αποτελέσματα αυτά προκύπτουν από τον μέσο όρο των μετρικών, όλων των χρηστών του συνόλου αξιολόγησης και των 5 παιχνιδιών.

Παρατηρώντας τα ραβδογράμματα του πρώτου και του δεύτερου πειράματος, φαίνεται πως η προεπεξεργασία με LOF έχει πλέον ξεκάθαρη επιρροή. Ο αριθμός των αποδεκτών δειγμάτων από αισθητήρες και χειρονομίες μέχρι το κλείδωμα της συσκευής έχει μειωθεί σημαντικά, φτάνοντας σε αρκετά ικανοποιητικό επίπεδο. Ταυτόχρονα, η μετρική FRR, αν και έχει μια μικρή αύξηση, έχει παραμείνει σε ένα χαμηλό και αρκετά ικανοποιητικό επίπεδο. Επιπλέον, από τα πειράματα τρία και τέσσερα μπορεί να γίνει και πάλι κατανοητό πόσο σημαντική επιρροή έχουν οι παράμετροι nu και gamma στο τελικό αποτέλεσμα. Στο πείραμα τρία οι περιοχές nu – gamma που επιλέχθηκαν εξυπηρετούν περισσότερο τις προδιαγραφές ευχρηστίας (για παράδειγμα, στο Σχήμα 36, περιοχές με nu < 0,02 και με gamma < 0,001) και όπως αποδεικνύεται η FRR έχει πέσει κάτω από το 1%, ενώ ταυτόχρονα οι μετρικές ασφάλειας έχουν αυξηθεί αρκετά. Αντιθέτως, στο πείραμα τέσσερα οι περιοχές nu – gamma που επιλέχθηκαν εξυπηρετούν περισσότερο της προδιαγραφές ασφάλειας (για παράδειγμα, στο Σχήμα 36, περιοχές με nu > 0,04 και με gamma > 0,003) και έτσι παρατηρείται αύξηση στην FRR αλλά σημαντική μείωση στον αριθμό αποδεκτών δειγμάτων. Σημειώνεται πως στα πειράματα τρία και τέσσερα, η επιλογή των περιοχών nu – gamma που πραγματοποιήθηκε δεν είχε στόχο την εύρεση των βέλτιστων περιοχών αλλά την απλή προβολή της επιρροής των συγκεκριμένων παραμέτρων στο τελικό αποτέλεσμα.



Σχήμα 44: Ποσοστιαίες Μετρικές σε Πειράματα Πραγματικής Χρήσης



Σχήμα 45: Μετρικές Αριθμού Δειγμάτων σε Πειράματα Πραγματικής Χρήσης

Συνοψίζοντας τις παραπάνω παρατηρήσεις, προκύπτει πως:

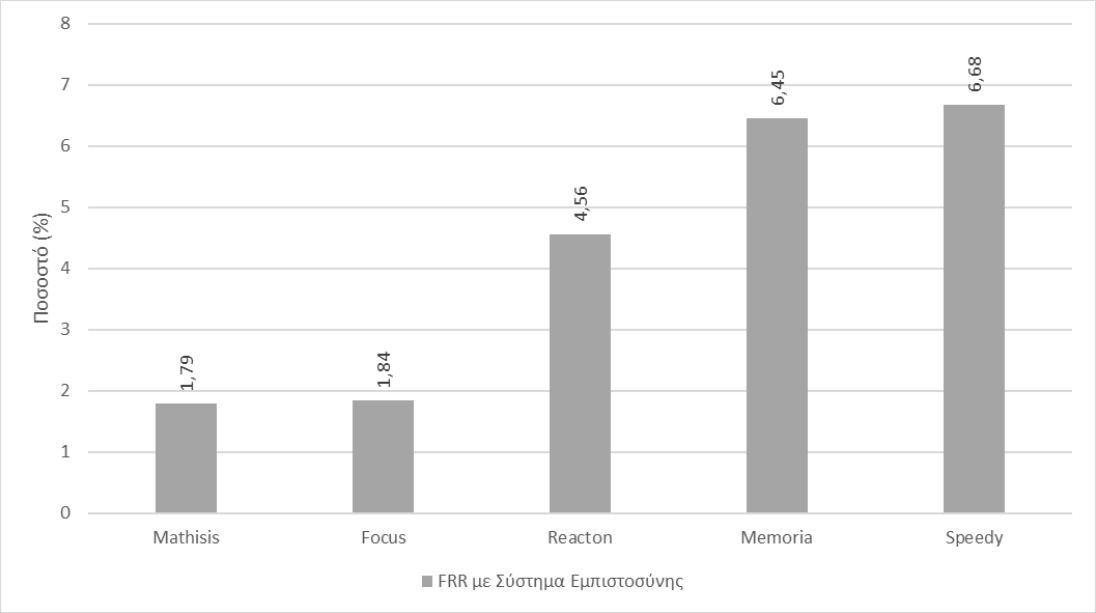
- Η αποθορυβοποίηση των δεδομένων εκπαίδευσης με LOF τελικά βοηθάει στην επίτευξη ικανοποιητικών επιπέδων ασφάλειας, αλλά και ικανοποιητικών επιπέδων ευχρηστίας. Μάλιστα, το συμπέρασμα αυτό έχει μεγαλύτερη βαρύτητα από το αντίστοιχο της προηγούμενης ενότητας, καθώς προκύπτει από την αξιολόγηση του συστήματος σε περισσότερα και τελείως άγνωστα δεδομένα.

- Η κατάλληλη επιλογή παραμέτρων nu και gamma, μπορεί να καθορίσει την αυστηρότητα του συστήματος. Στα πειράματα, οι παράμετροι ήταν ίδιες για όλους τους χρήστες. Ωστόσο, η επιλογή ξεχωριστών παραμέτρων για κάθε χρήστη, δηλαδή η εφαρμογή ενός τρόπου ή μιας μεθοδολογίας ώστε η επιλογή των περιοχών nu – gamma να εξαρτάται από την συμπεριφορά ενός χρήστη, μπορεί να βελτιώσει περισσότερο τα αποτελέσματα.

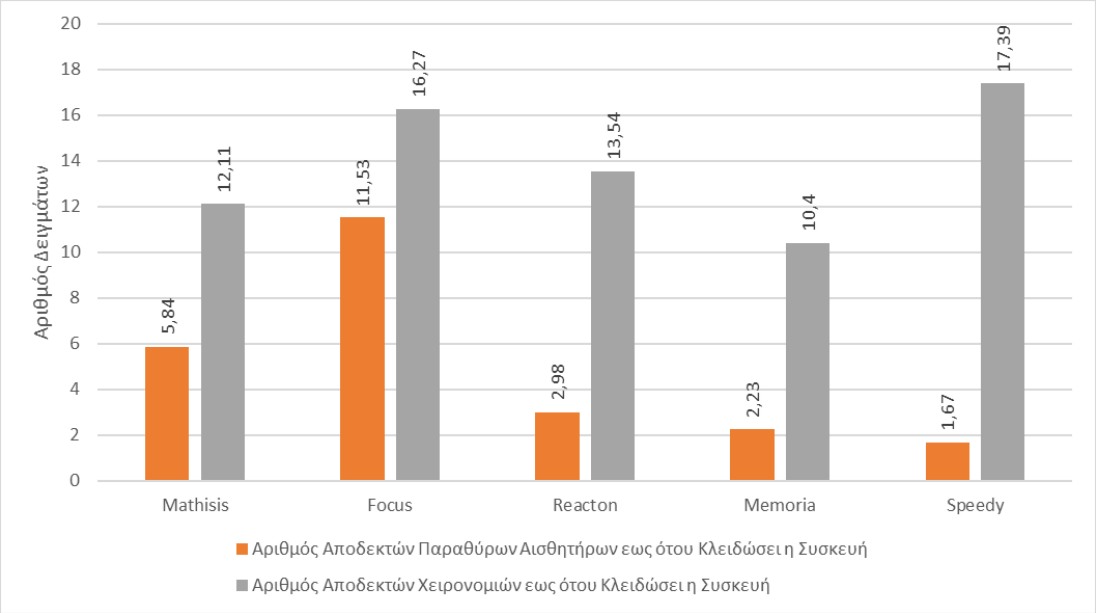
5.2.1 Αποτελέσματα Ανά Παιχνίδι

Θεωρώντας πως το σύστημα του δεύτερου πειράματος (πολλαπλά SVMs, με LOF), της ενότητας 5.2, είναι αυτό που καλύπτει καλύτερα και με σχετική ισορροπία τους στόχους ασφάλειας και ευχρηστίας, σε αυτή την υποενότητα παρουσιάζονται αναλυτικότερα τα αποτελέσματα του ίδιου συστήματος ανά τύπο παιχνιδιού. Συγκεκριμένα, παρουσιάζονται τα παρακάτω ραβδογράμματα (Σχήμα 46, Σχήμα 47). Σημειώνεται, πως για το συγκεκριμένο πείραμα οι περιοχές nu – gamma ορίζονται σύμφωνα με τον ακόλουθο πίνακα (Πίνακας 10).

Τα παιχνίδια κύριου ενδιαφέροντος είναι το Mathisis και το Focus, καθώς σε αυτά ο χρήστης αλληλεπιδρά με την συσκευή μέσω swipes, ενώ στα άλλα παιχνίδια χρησιμοποιεί taps (Memoria, Speedy) ή συνδυασμό των δύο (Reacton). Η εν λόγω εργασία δεν εμβαθύνει στην βελτιστοποίηση του συστήματος για τα taps, καθώς δεν πραγματοποιήθηκε μελέτη για την εξαγωγή και επιλογή βέλτιστων χαρακτηριστικών. Για αυτό τον λόγο, η παρατήρηση των αποτελεσμάτων των υπόλοιπων παιχνιδιών δίνει περισσότερη πληροφορία για την γενικότερη συμπεριφορά του συστήματος σε δεδομένα αισθητήρων κίνησης και μια πρώιμη εικόνα για το πως το σύστημα αντιμετωπίζει τα taps.



Σχήμα 46: Ποσοστιαίες Μετρικές Τελικού Συστήματος ανά Παιχνίδι



Σχήμα 47: Μετρικές Αριθμού Δειγμάτων Τελικού Συστήματος ανά Παιχνίδι

Παρατηρώντας λοιπόν τα αποτελέσματα για το Mathisis και το Focus, φαίνεται πως το σύστημα μπορεί να αναγνωρίσει ιδιαίτερα ικανοποιητικά τον πραγματικό χρήστη (FRR < 2%), αλλά είναι λιγότερο αποτελεσματικό στο να ανιχνεύει κακόβουλους χρήστες, ιδιαίτερα στο Focus. Συγκεκριμένα, το σύστημα χρειάζεται περίπου 6 δείγματα αισθητήρων κίνησης και 12 swipes για να αναγνωρίσει έναν κακόβουλο χρήστη στο Mathisis και περίπου 12 δείγματα αισθητήρων κίνησης και 16 swipes για να αναγνωρίσει έναν κακόβουλο χρήστη στο Focus.

Είναι πιθανό, η επιλογή διαφορετικών περιοχών nu – gamma να βελτίωνε τις συγκεκριμένες μετρικές, αυξάνοντας όμως και το FRR. Σημειώνεται όμως, πως ο αριθμός δειγμάτων από αισθητήρες εξαρτάται από την συχνότητα δειγματοληψίας και συνεπώς ο χρόνος που απαιτείται από το σύστημα για την συλλογή του συγκεκριμένου αριθμού δειγμάτων και την αναγνώριση του κακόβουλο χρήστη είναι σχετικός. Στην συγκεκριμένη εργασία, η συχνότητα δειγματοληψίας ορίστηκε στα 50Hz και έτσι υπολογίζεται ότι το σύστημα, στο σύνολό του (Σχήμα 45, δεύτερο πείραμα), χρειάζεται λιγότερο από 5 δευτερόλεπτά και κάτι λιγότερο από 14 δείγματα χειρονομιών για να κλειδώσει έναν κακόβουλο χρήστη.

Επιπλέον, ιδιαίτερη εντύπωση δημιουργούν και τα αποτελέσματα των υπόλοιπων παιχνιδιών. Αν και η μετρική FRR έχει σχετικά μεγαλύτερες αλλά ικανοποιητικές τιμές (4% < FRR < 7%), φαίνεται να απαιτείται μικρότερος αριθμό δεδομένων κίνησης (αριθμός παραθύρων αισθητήρων < 3) για να αναγνωρίσει το σύστημα έναν κακόβουλο χρήστη. Ωστόσο, αυτό που αξίζει σχολιασμό είναι πως ο αριθμός χειρονομιών που απαιτείται για την αναγνώριση κακόβολου χρήστη παραμένει αρκετά υψηλός. Αν και οι υπόλοιπες μετρικές ακολουθούν μια παρόμοια αναλογία σε όλα τα παιχνίδια, η οποία στην ουσία καθορίζεται από τις περιοχές nu – gamma που επιλέχθηκαν, η έλλειψη βέλτιστων χαρακτηριστικών στα taps κάνει τα 3 τελευταία παιχνίδια να παρουσιάζουν δυσανάλογα αυξημένο αριθμό απαιτούμενων χειρονομιών.

Προκύπτει λοιπόν πως:

- Το σύστημα αποδίδει ικανοποιητικά στα Mathisis και Focus. Ωστόσο, η επιλογή διαφορετικών περιοχών nu – gamma μπορεί να βελτιώσει περισσότερο το χάσμα μεταξύ ασφάλειας και ευχρηστίας, κρατώντας ταυτόχρονα όλες τις μετρικές σε αποδεκτές τιμές.

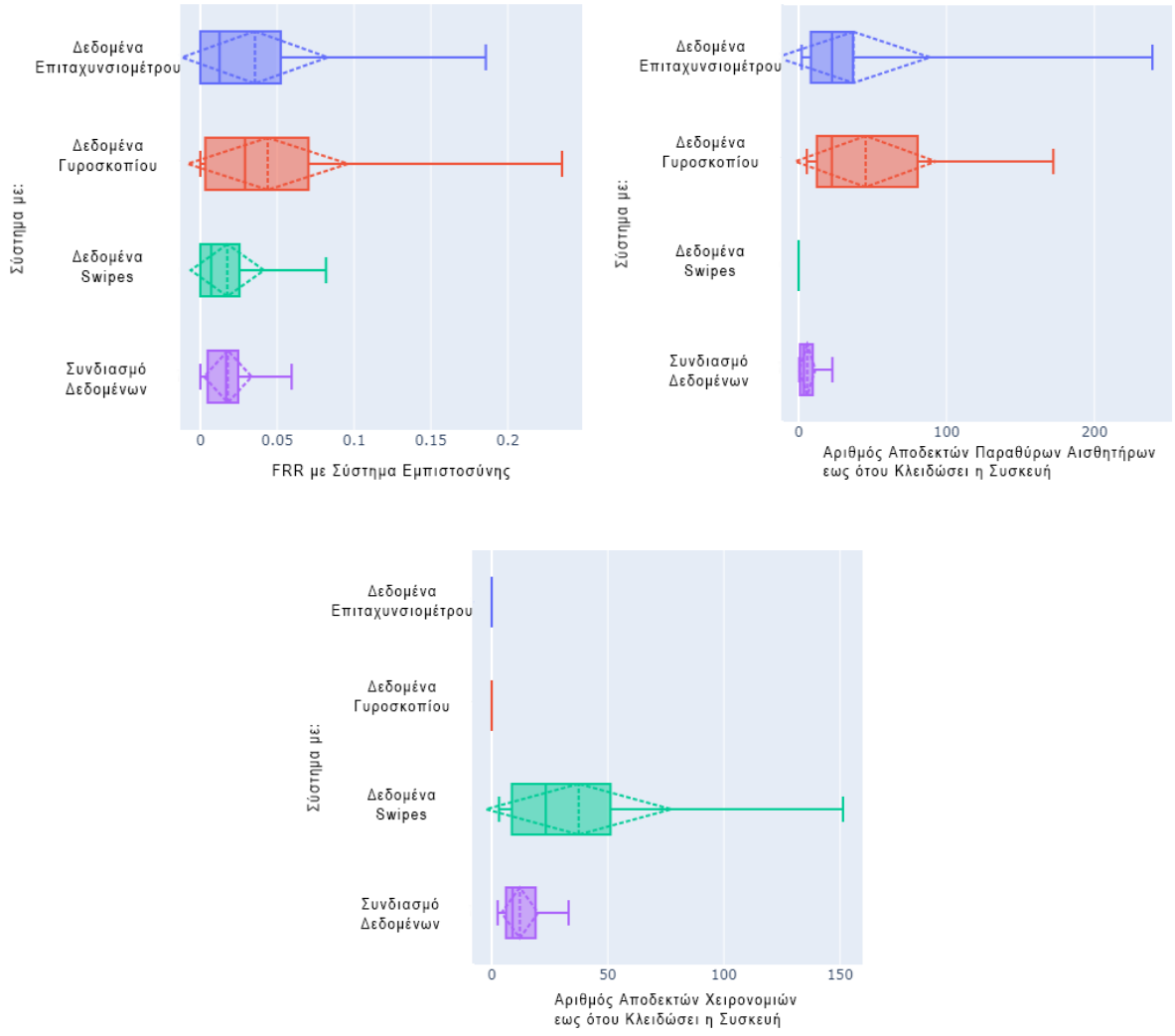
- Τα Reacton, Memoria και Speedy έχουν αρκετά ικανοποιητικά αποτελέσματα στην μετρική FRR και τον αριθμό αποδεκτών δειγμάτων από αισθητήρες κίνησης, ενώ ο υψηλός αριθμός χειρονομιών δικαιολογείται από την ύπαρξη taps.

5.3 Συγκρίσεις

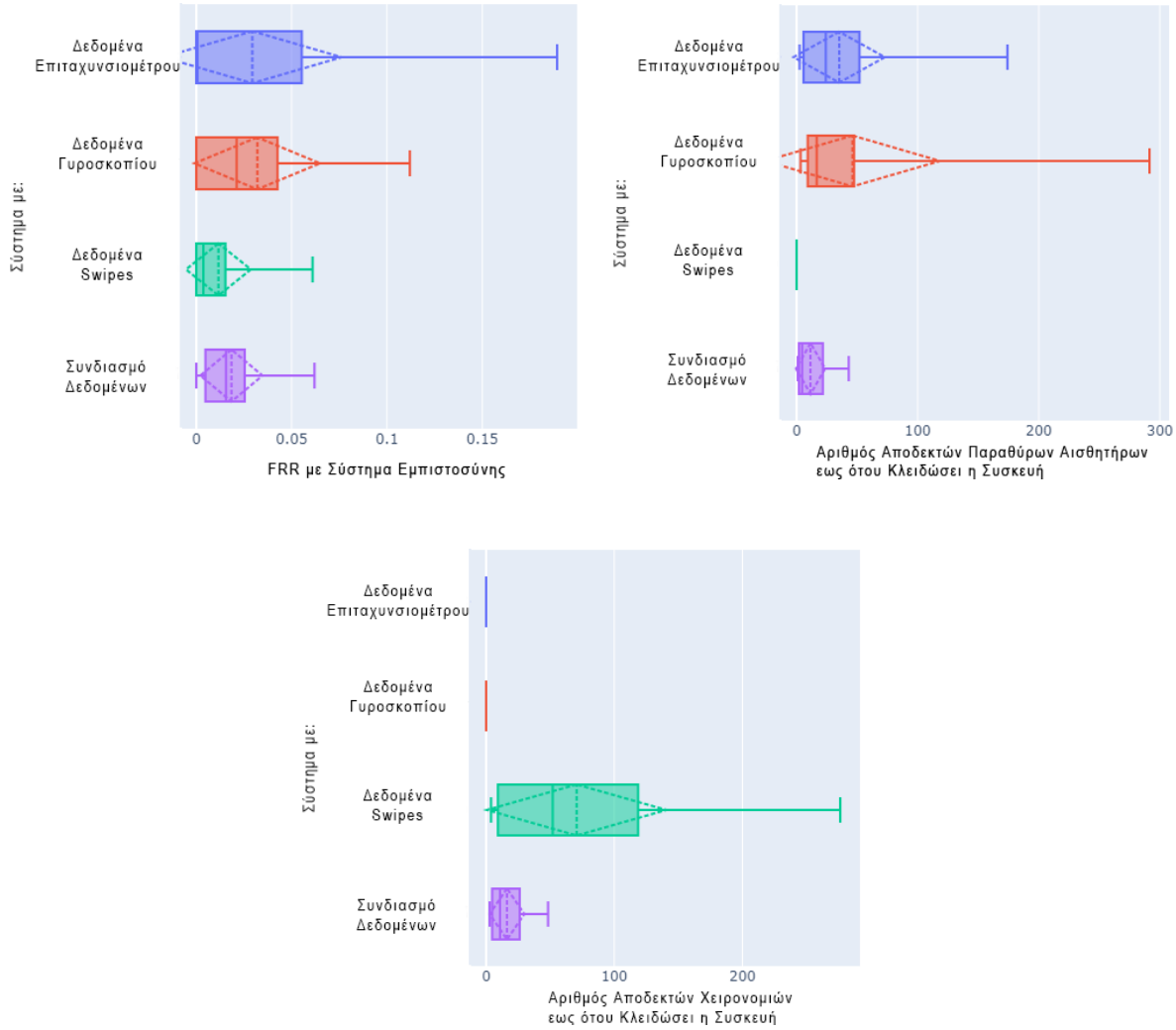
Τα παραπάνω πειράματα δίνουν χρήσιμές πληροφορίες, αλλά για την πλήρη αξιολόγηση του συστήματος απαραίτητη είναι και η σύγκρισή του με άλλες υλοποιήσεις. Στα διαγράμματα της ενότητας αυτής φαίνεται η σημασία της χρήσης δεδομένων διαφορετικών τύπων, καθώς το εν

λόγω σύστημα μπορεί να λειτουργήσει και όταν κάποια από τα δεδομένα που χρησιμοποιεί δεν είναι διαθέσιμα.

Στα παρακάτω θηκογράμματα (Σχήμα 48, Σχήμα 49), φαίνεται η απόδοση του συστήματος στα παιχνίδια Mathisis και Focus, σε σύγκριση με συστήματα που αξιοποιούν δεδομένα αποκλειστικά από το επιταχυνσιόμετρο, το γυροσκόπιο και την οθόνη αφής. Συγκεκριμένα, στα παρακάτω σχήματα φαίνονται θηκογράμματα για τις μετρικές FRR με Σύστημα Εμπιστοσύνης, Αριθμός Αποδεκτών Παραθύρων Αισθητήρων έως ότου Κλειδώσει η Συσκευή και Αριθμός Αποδεκτών Χειρονομιών έως ότου Κλειδώσει η Συσκευή. Οι μετρικές αυτές αναπαρίστανται για κάθε ένα σύστημα. Έτσι, είναι αναμενόμενο το σύστημα που λειτουργεί αποκλειστικά με δεδομένα swipes να έχει μηδενική τιμή στον αριθμό αποδεκτών δειγμάτων αισθητήρων και αντίστοιχα τα συστήματα που λειτουργούν αποκλειστικά με δεδομένα αισθητήρων να έχουν μηδενικό αριθμό αποδεκτών χειρονομιών.



Σχήμα 48: Σύγκριση Συστημάτων Mathisis



Σχήμα 49: Σύγκριση Συστημάτων Focus

Αυτό που φαίνεται, είναι ότι το εν λόγω σύστημα, δηλαδή το σύστημα με συνδυασμό δεδομένων παρουσιάζει μεγαλύτερη σταθερότητα σε σύγκριση με τα υπόλοιπα συστήματα και στα δύο παιχνίδια. Όσον αναφορά τις μετρικές ασφάλειας είναι καλύτερες από τα άλλα συστήματα και στα δύο παιχνίδια. Αντιθέτως, στο Focus, το σύστημα αποκλειστικά βασισμένο σε swipes φαίνεται να έχει ελάχιστα καλύτερα αποτελέσματα στην FRR. Ωστόσο, το γεγονός ότι η διαφορά είναι μικρή και ότι το σύστημα με συνδυασμό δεδομένων μπορεί να λειτουργήσει και όταν δεν υπάρχουν διαθέσιμα δεδομένα από κάποια κατηγορία, κάνει το εν λόγω σύστημα πιο αξιόπιστο και ευέλικτο.

Επιπλέον, για σφαιρική αξιολόγηση, στους παρακάτω πίνακες (Πίνακας 13, Πίνακας 14) αναγράφονται αναλυτικότερα τα αποτελέσματα των ερευνών της Τσίντζηρα [34] και της Παλάζη [45], που έχουν αξιολογηθεί στο ίδιο σύνολο δεδομένων.

Πίνακας 13: Σύγκριση Μετρικών Ασφάλειας

	Mathisis	Focus	Reacton	Memoria	Speedy
[34] (FAR %)	4,08	3,50	6,90	1,10	5,40
[45] (Αριθμός Αποδεκτών Χειρονομιών)	1,70	3,92	8,08 | 11,37 (Swipes | Taps)	21,83	277,47
Τρέχουσα Εργασία (Αριθμός Αποδεκτών Δειγμάτων Αισθητήρων & Χειρονομιών)	5,84 & 12,11	11,53 & 16,27	2,98 & 13,54	2,23 & 10,40	1,67 & 17,39

Πίνακας 14: Σύγκριση Μετρικών Χρηστικότητας

	Mathisis	Focus	Reacton	Memoria	Speedy
[34] (FRR %)	5,20	6,00	4,30	5,70	5,70
[45] (FRR με Σύστημα Εμπιστοσύνης %)	1,92	1,06	2,32 | 3,58 (Swipes | Taps)	3,44	0,065
Τρέχουσα Εργασία (FRR με Σύστημα Εμπιστοσύνης %)	1,79	1,84	4,56	6,45	6,68

Πριν όμως γίνει η καταγραφή των πορισμάτων, σημειώνεται ότι στην [34] το σύστημα αξιολόγησης δεν εμπεριέχει υποσύστημα εμπιστοσύνης και έτσι η σύγκριση δεν μπορεί να γίνει με απόλυτο τρόπο, ιδιαίτερα στο κομμάτι της ασφάλειας όπου χρησιμοποιούνται διαφορετικές μετρικές. Επιπλέον υπογραμμίζεται ότι σε σύγκριση με τα άλλα δύο, το σύστημα αυτής της εργασίας εξετάζεται σε μεγαλύτερο αριθμό χρηστών, άγνωστων κατά το στάδιο της βελτιστοποίησης. Έχοντας λοιπόν ως άξονες τις παραπάνω παρατηρήσεις, προκύπτει πως οι μετρικές χρηστικότητας και των τριών συστημάτων κυμαίνονται σε παρόμοιο επίπεδο, ενώ στο κομμάτι της ασφάλειας φαίνεται πως το εν λόγω σύστημα παρουσιάζει λίγο αυξημένες μετρικές στις οθόνες κύριου ενδιαφέροντος (Mathisis, Focus). Ωστόσο, η γενικότερη συμπεριφορά του προτεινόμενου συστήματος έχει μικρότερη διακύμανση μεταξύ όλων το παιχνιδιών. Επιπροσθέτως και σε σύγκριση με την [34], σημειώνεται ότι το παράθυρο κατάτμησης είναι αρκετά μικρότερο. Πιο συγκεκριμένα, σε αυτήν την εργασία χρησιμοποιούνται παράθυρα με μέγιστο μήκος 50 δείγματα, ενώ στην [34] το παράθυρο έχει σταθερό μήκος στα 500 δείγματα. Υποθέτοντας ότι η συχνότητα δειγματοληψίας και στις δύο περιπτώσεις κυμαίνεται κοντά στα 50Hz (με δεδομένο ότι και στις δύο περιπτώσεις χρησιμοποιείται το ίδιο σύνολο δεδομένων), συνεπάγεται ότι για την συλλογή ενός παραθύρου απαιτείται μόλις 1 δευτερόλεπτο για το εν λόγω σύστημα, έναντι 10 δευτερολέπτων που

απαιτείται στην εργασία της Τσίντζηρα [34]. Σημειώνεται ότι, οι μετρικές που χρησιμοποιούνται δεν είναι ίδιες, ωστόσο αυτή η υπόθεση δίνει μια ιδέα για την διαφορά σε χρόνο, που χρειάζονται τα δύο συστήματα για να κάνουν τουλάχιστον έναν έλεγχο.

Κάνοντας λοιπόν τις απαραίτητες συγκρίσεις, προκύπτουν τα εξής συμπεράσματα:

- Το εν λόγω σύστημα βασίζεται σε συνδυασμό δεδομένων, γεγονός που το καθιστά ικανό να λειτουργεί και σε περιπτώσεις που δεν υπάρχουν διαθέσιμα δεδομένα από κάποια κατηγορία.

- Το εν λόγω σύστημα παρουσιάζει παρόμοια συμπεριφορά με τα συστήματα που έχουν αξιολογηθεί στο ίδιο σύνολο δεδομένων, αλλά ταυτόχρονα τα αποτελέσματά του έχουν μικρότερη διακύμανση μεταξύ των διαφορετικών παιχνιδιών.

- Ο χρόνος που χρειάζεται το σύστημα, για να εκτελέσει έναν τουλάχιστον έλεγχο, είναι χαμηλότερος σε σύγκριση με άλλα συστήματα.

6 Συμπεράσματα & Μελλοντικές Ιδέες

Συνοψίζοντας, τα πειράματα που αναλύθηκαν στην προηγούμενη ενότητα δίνουν χρήσιμα συμπεράσματα, τόσο για τις τεχνικές που χρησιμοποιήθηκαν όσο και την απόδοση του τελικού συστήματος.

Όσον αφορά την μεθοδολογία και τις τεχνικές, τα σημαντικότερα συμπεράσματα δείχνουν πως:

- Η χρήση πολλαπλών RBF-OCSVMs εξυπηρετεί την ασφάλεια του συστήματος.
- Το σύστημα εμπιστοσύνης βοηθάει στην διαμόρφωση ενός εύχρηστου συστήματος.
- Η αποθορυβοποίηση των δεδομένων εκπαίδευσης με LOF βελτιώσει την ασφάλεια.
- Οι παράμετροι nu και gamma των RBF-OCSVMs, παίζουν καθοριστικό ρόλο στην διασφάλιση ισορροπίας μεταξύ ασφάλειας και ευχρηστίας παίζουν.

Εφαρμόζοντας λοιπόν την γνώση που αποκτήθηκε από τα πειράματα, αναπτύχθηκε ένα σύστημα που βασίζεται στο συνδυασμό τριών ανεξάρτητων υποσυστημάτων, που συνεργάζονται μεταξύ τους, μέσω ενός συστήματος εμπιστοσύνης. Κάνοντας την απαραίτητη αξιολόγηση, προκύπτει πως το σύστημα που προτείνεται από τη εν λόγω εργασία ξεχωρίσει για τους εξής λόγους:

- Τα τέσσερα ανεξάρτητα υποσυστήματα, που χρησιμοποιούνται για τους τέσσερις διαφορετικούς τύπους δεδομένων (επιταχυνσιόμετρο, γυροσκόπιο, swipes, taps), δίνουν την δυνατότητα στο τελικό σύστημα να μπορεί να ανταπεξέλθει και σε περιπτώσεις που υπάρχουν ελλείψεις σε δεδομένα αισθητήρων ή χειρονομιών.
- Οι τιμές των μετρικών είναι ικανοποιητικές σε όλα τα παιχνίδια. Συγκεκριμένα, τα αποτελέσματα στα Mathisis και Focus είναι παρόμοια με προηγούμενες εργασίες, αλλά ταυτόχρονα υπάρχει βελτίωση στα υπόλοιπα παιχνίδια και έτσι συνεπάγεται, πως υπάρχει μεγαλύτερη σταθερότητα σε περισσότερα σενάρια χρήσης.
- Ο έλεγχος που αφορά το κομμάτι των αισθητήρων, εφαρμόζεται σε αρκετά πιο σύντομο χρόνο, συγκριτικά με διαφορετικές υλοποιήσεις. Υποθέτοντας μια κοινή συχνότητα δειγματοληψίας μετρήσεων (50Hz), το σύστημα χρειάζεται το πολύ 1 δευτερόλεπτο για να κάνει έναν έλεγχο.

- Τα πειράματα, αλλά και η αξιολόγηση του συστήματος πραγματοποιήθηκαν σε ένα μεγάλο σύνολο χρηστών, τα δεδομένα των οποίων συλλέχθηκαν κατά μη ελεγχόμενο τρόπο. Το γεγονός αυτό, κάνει τα αποτελέσματα αξιόπιστα δίνοντας αρκετά αντιπροσωπευτική εικόνα για την λειτουργία του συστήματος στην πραγματικότητα.

Προκύπτει λοιπόν, πως το προτεινόμενο σύστημα είναι αποτελεσματικό και ταυτόχρονα πιο αξιόπιστο και σταθερό. Έτσι, η εργασία αυτή μπορεί να αποτελέσει βάση για την υλοποίηση μίας εφαρμογής έμμεσης και συνεχούς αυθεντικοποίησης, που θα διασφαλίζει την ασφάλεια των δεδομένα της συσκευής ενός χρήστη, με μη παρεμβατικό τρόπο. Σίγουρα όμως, η περεταίρω εξερεύνηση και εφαρμογή τεχνικών μπορούν να επιφέρουν σημαντικές βελτιώσεις. Προς την κατεύθυνση αυτή, παρουσιάζονται οι παρακάτω ιδέες:

- Η ενσωμάτωση ενός υποσυστήματος που θα επιλέγει με έναν ‘έξυπνο’ και δυναμικό τρόπο ποιος θα είναι ο ταξινομητής που θα έχει μεγαλύτερη επιρροή στις αποφάσεις.

- Η υλοποίηση της εφαρμογής με τρόπο που ο χρήστης θα μπορεί να ελέγξει την αυστηρότητα των ταξινομητών. Στην ουσία, ο χρήστης να μπορεί να επιλέξει τις περιοχές nu – gamma, που ανταποκρίνονται στις ανάγκες του, χρησιμοποιώντας κάποιο, φιλικό προς τον ίδιο, περιβάλλον. Για την εργασία η επιλογή των nu και gamma έγινε διασφαλίζοντας ικανοποιητικά αποτελέσματα για μεγάλο σύνολο χρηστών. Συνεπώς, η προσωπική επιλογή παραμέτρωων μπορεί να βελτιώσει περισσότερο την απόδοση.

- Η συσχέτιση του εν λόγω συστήματος με τεχνικές επίγνωσης πλαισίου (context-aware). Συγκεκριμένα, το περιεχόμενο της οθόνη μπορεί να δώσει σημαντικές πληροφορίες για την αναμενόμενη συμπεριφορά. Αυτές οι πληροφορίες μπορούν να φανούν ιδιαίτερα χρήσιμες στην ρύθμιση παραμέτρων, στην διαμόρφωση της τελικής απόφασης αλλά και στην ρύθμιση του συστήματος εμπιστοσύνης.

- Μεθοδολογίες που επιτρέπουν στο σύστημα να προσαρμόζεται και να εκπαιδεύεται συνεχώς σε καινούργια δεδομένα, θεωρούνται εξίσου σημαντικές. Το σύστημα πρέπει να έχει την ικανότητα να εξελίσσεται και να αλλάζει την συμπεριφορά του ανάλογα με το πως ο χρήστης αλλάζει τον τρόπο που αλληλεπιδρά με την συσκευή.

Βιβλιογραφία

[1] S. O'Dea, "Smartphone subscriptions worldwide 2016-2027." www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (accessed Feb. 16, 2022).

[2] Statista Research Department, "Time spent on smartphone everyday in Spain in 2019." www.statista.com/statistics/1185655/daily-time-spent-on-smartphones-spain/ (accessed Feb. 16, 2022).

[3] M. Rimol, "Kaspersky Lab Finds Over Half of Consumers Don't Password-Protect their Mobile Devices," 2018. https://usa.kaspersky.com/about/press-releases/2018_kaspersky-lab-finds-over-half-of-consumers-don-t-password-protect-their-mobile-devices (accessed Feb. 17, 2022).

[4] S. Gupta, A. Buriro, and B. Crispo, "Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access," *Mob. Inf. Syst.*, vol. 2018, pp. 1–16, 2018, doi: 10.1155/2018/2649598.

[5] S. Sonkamble, R. Thool, and B. Sonkamble, "Survey of biometric recognition systems and their applications," *J. Theor. Appl. Inf. Technol.*, vol. 11, no. 1, pp. 45–51, 2010.

[6] S. P. Banerjee and D. Woodard, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey," *J. Pattern Recognit. Res.*, vol. 7, no. 1, pp. 116–139, 2012, doi: 10.13176/11.427.

[7] Catalin Cimpanu, "Microsoft: Using multi-factor authentication blocks 99.9% of account hacks," *ZDNet*, 2019. www.mdsny.com/using-multi-factor-authentication-blocks-99-9-of-account-hacks/ (accessed Feb. 17, 2022).

[8] K. Thomas and A. Moscicki, "How effective is basic account hygiene at preventing hijacking," *Google Security Blog*, 2019. https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html (accessed Feb. 17, 2022).

[9] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and i know it's you!," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, May 2012, pp. 987–996, doi: 10.1145/2207676.2208544.

[10] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011, vol. 6531 LNCS, doi: 10.1007/978-3-642-18178-8_9.

[11] “Behavioral Biometrics Authentication,” *Optimal IdM*. https://optimalidm.com/solutions/identity-access-management/behavioral-biometrics-authentication/ (accessed Feb. 21, 2022).

[12] D. Jost, “What is an accelerometer?,” *Fierce Electronics*, 2019. https://www.fierceelectronics.com/sensors/what-accelerometer (accessed Feb. 21, 2022).

[13] d‘wise one, “What’s A Gyroscope And Accelerometer Doing In My Mobile Device?,” *Medium*, 2015. https://medium.com/chip-monks/whats-a-gyroscope-and-accelerometer-doing-in-my-mobile-device-eb7acbdfa4e0 (accessed Feb. 21, 2022).

[14] “Touch screen,” *Computer Hope*, 2021. https://www.computerhope.com/jargon/t/toucscre.htm#input (accessed Feb. 22, 2022).

[15] “Touch Screen Explained - Everything You Need To Know,” *HISTORY COMPUTER STAFF*, 2021. https://history-computer.com/touch-screen/ (accessed Feb. 22, 2022).

[16] “Touch Screen,” 2017. https://www.techopedia.com/definition/3055/touch-screen (accessed Feb. 22, 2022).

[17] R. Anyoha, “The History of Artificial Intelligence,” *Science In The News (SITN), Harvard University*, 2017. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ (accessed Feb. 28, 2022).

[18] “Machine Learning,” *IBM Cloud Education*, 2020. https://www.ibm.com/cloud/learn/machine-learning (accessed Feb. 28, 2022).

[19] I. SALIAN, “SuperVize Me: What’s the Difference Between Supervised, Unsupervised, Semi-Supervised and Reinforcement Learning?,” *NVIDIA*, 2018. https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/ (accessed Feb. 28, 2022).

[20] A. Al-Masri, “What Are Overfitting and Underfitting in Machine Learning?,” *Towards Data Science*, 2019. https://towardsdatascience.com/what-are-overfitting-and-underfitting-in-machine-learning-a96b30864690 (accessed Feb. 28, 2022).

[21] J. Brownlee, “One-Class Classification Algorithms for Imbalanced Datasets,” *Imbalanced Classification*, 2020. https://machinelearningmastery.com/one-class-classification-algorithms/ (accessed Mar. 01, 2022).

[22] “Novelty and Outlier Detection,” *scikit-learn 1.0.2*. https://scikit-

learn.org/stable/modules/outlier_detection.html (accessed Mar. 01, 2022).

[23] V. Jayaswal, “Local Outlier Factor (LOF) — Algorithm for outlier identification,” *Towards Data Science*, 2020. https://towardsdatascience.com/local-outlier-factor-lof-algorithm-for-outlier-identification-8efb887d9843 (accessed Mar. 02, 2022).

[24] Y. VERMA, “How to use Support Vector Machines for One-Class Classification?,” *DEVELOPERS CORNER*, 2021. https://analyticsindiamag.com/how-to-use-support-vector-machines-for-one-class-classification/ (accessed Mar. 03, 2022).

[25] S. S. Khan and M. G. Madden, “One-class classification: taxonomy of study and review of techniques,” *Knowl. Eng. Rev.*, vol. 29, no. 3, pp. 345–374, Jun. 2014, doi: 10.1017/S026988891300043X.

[26] B. Schölkopf, R. Williamson, A. Smola, J. Shawe-Taylor, and J. Piatt, “Support vector method for novelty detection,” 2000.

[27] D. M. J. Tax and R. P. W. Duin, “Support Vector Data Description,” *Mach. Learn.*, vol. 54, no. 1, pp. 45–66, Jan. 2004, doi: 10.1023/B:MACH.0000008084.60811.49.

[28] “RBF SVM parameters,” *scikit-learn 1.0.2*. https://scikit-learn.org/stable/auto_examples/svm/plot_rbf_parameters.html (accessed Mar. 03, 2022).

[29] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, “Sensor-Based Continuous Authentication of Smartphones’ Users Using Behavioral Biometrics: A Contemporary Survey,” *IEEE Internet of Things Journal*, vol. 8, no. 1. 2021, doi: 10.1109/JIOT.2020.3020076.

[30] S. Amini, S. Gupte, V. Noroozi, P. S. Yu, A. Pande, and C. Kanich, “Deepauth: A framework for continuous user re-authentication in mobile apps,” 2018, doi: 10.1145/3269206.3272034.

[31] W. H. Lee and R. B. Lee, “Multi-sensor authentication to improve smartphone security,” 2015, doi: 10.5220/0005239802700280.

[32] Y. Li, H. Hu, and G. Zhou, “Using Data Augmentation in Continuous Authentication on Smartphones,” *IEEE Internet Things J.*, vol. 6, no. 1, 2019, doi: 10.1109/JIOT.2018.2851185.

[33] Y. Li, H. Hu, Z. Zhu, and G. Zhou, “SCANet: Sensor-based Continuous Authentication with Two-stream Convolutional Neural Networks,” *ACM Trans. Sens. Networks*, vol. 16, no. 3, 2020.

[34] Α.-Α. Τσίντζηρα, “Συνεχής έμμεση αυθεντικοποίηση χρηστών κινητού τηλεφώνου με τη χρήση δεδομένων πλοήγησης,” Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2020.

[35] M. D. Papamichail, K. C. Chatzidimitriou, T. Karanikiotis, N. C. I. Oikonomou, A. L. Symeonidis, and S. K. Saripalle, “Brainrun: A behavioral biometrics dataset towards continuous implicit authentication,” *Data*, vol. 4, no. 2, 2019, doi: 10.3390/data4020060.

[36] D. Gafurov and E. Snekkenes, “Gait recognition using wearable motion recording sensors,” *EURASIP J. Adv. Signal Process.*, vol. 2009, 2009, doi: 10.1155/2009/415817.

[37] T. Hoang, V. Quang, D. Nguyen, and C. Deokjai, “Gait identification using accelerometer on mobile phone,” 2012, doi: 10.1109/ICCAIS.2012.6466615.

[38] T. Hoang, T. Nguyen, C. Luong, S. Do, and D. Choi, “Adaptive cross-device gait recognition using a mobile accelerometer,” *J. Inf. Process. Syst.*, vol. 9, no. 2, 2013, doi: 10.3745/JIPS.2013.9.2.333.

[39] A. Buriro, S. Gupta, B. Crispo, and F. Del Frari, “Dialerauth: A motion-assisted touch-based smartphone user authentication scheme,” in *CODASPY 2018 - Proceedings of the 8th ACM Conference on Data and Application Security and Privacy*, 2018, vol. 2018-Janua, doi: 10.1145/3176258.3176318.

[40] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, “Keystroke-based user identification on smart phones,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5758 LNCS, doi: 10.1007/978-3-642-04342-0_12.

[41] C. Giuffrida, K. Majdanik, M. Conti, and H. Bos, “I sensed it was you: Authenticating mobile users with sensor-enhanced keystroke dynamics,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014, vol. 8550 LNCS, doi: 10.1007/978-3-319-08509-8_6.

[42] M. Antal and L. Z. Szabó, “Biometric Authentication Based on Touchscreen Swipe Patterns,” *Procedia Technol.*, vol. 22, 2016, doi: 10.1016/j.protcy.2016.01.061.

[43] H. Khan and U. Hengartner, “Towards application-centric implicit authentication on smartphones,” 2014, doi: 10.1145/2565585.2565590.

[44] T. Karanikiotis, M. D. Papamichail, K. C. Chatzidimitriou, N. C. I. Oikonomou, A. L.

Symeonidis, and S. K. Saripalle, “Continuous Implicit Authentication through Touch Traces Modelling,” 2020, doi: 10.1109/QRS51102.2020.00026.

[45] Α. Παλάζη, “Συνεχής έμμεση αυθεντικοποίηση χρηστών κινητού τηλεφώνου μέσω ανάλυσης συμπεριφορών,” Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2021.

[46] T. Zhu *et al.*, “RiskCog: Unobtrusive real-time user authentication on mobile devices in the wild,” *IEEE Trans. Mob. Comput.*, vol. 19, no. 2, 2020, doi: 10.1109/TMC.2019.2892440.

[47] W. H. Lee and R. B. Lee, “Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning,” 2017, doi: 10.1109/DSN.2017.24.

[48] X. Liang, F. Zou, L. Li, and P. Yi, “Mobile terminal identity authentication system based on behavioral characteristics,” *Int. J. Distrib. Sens. Networks*, vol. 16, no. 1, 2020, doi: 10.1177/1550147719899371.

[49] T. Feng *et al.*, “Continuous mobile authentication using touchscreen gestures,” 2012, doi: 10.1109/THS.2012.6459891.

[50] T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. Shi, “TIPS: Context-aware implicit user identification using touch screen in uncontrolled environments,” 2014, doi: 10.1145/2565585.2565592.

[51] S. D. Bersch, D. Azzi, R. Khusainov, I. E. Achumba, and J. Ries, “Sensor data acquisition and processing parameters for human activity classification,” *Sensors (Switzerland)*, vol. 14, no. 3, 2014, doi: 10.3390/s140304239.