ΕΤΗΣΙΑ ΕΚΘΕΣΗ ΠΡΟΟΔΟΥ

(διάστημα από 8/11/2020 έως 7/11/2021)

Αγγελάκης Δημήτριος

Α.Μ.: 1903

«ΣΥΝΤΟΝΙΣΜΕΝΗ ΚΙΝΗΣΗ ΠΟΛΛΑΠΛΩΝ ΒΡΑΧΙΟΝΩΝ ΜΕ ΧΡΗΣΗ ΔΙΕΠΑΦΗΣ ΥΠΟΛΟΓΙΣΤΗ ΕΓΚΕΦΑΛΟΥ»

Η παρούσα διατριβή ξεκίνησε από 8-11-2019.

Ακολουθεί συνοπτική ανάπτυξη του αντικειμένου της ΔΔ για το ακαδημαικο ετος 2020-2021

Παρουσιάζονται οι πειραματικές διαδικασίες που χρησιμοποιήθηκαν και τα αποτελέσματα που λήφθηκαν στο διάστημα του ενός έτους.

Η παρούσα διδακτορική διατριβή αφορά στον σχεδιασμό και ανάπτυξη υπολογιστικών εργαλείων εγκεφάλου-υπολογιστή (BCI) με χρήση ηλεκτροεγκεφαλογραφημάτων (EEG) και αλγορίθμων μηχανικής μάθησης , Ο στόχος είναι να δημιουργηθεί ένα σύστημα επικοινωνίας που θα μετατρέπει την εγκεφαλική δραστηριότητα σε εντολές ελέγχου για ρομποτικό σύστημα πολλαπλών βραχιόνων με 6 βαθμούς ελευθερίας (6Dof).

Εύρεση βέλτιστου αλγόριθμου Μηχανικής Μάθησης για πρόβλεψη κίνησης ρομποτικού βραχίονα με χρήση BCI

Στο παρόν κεφάλαιο δημιουργηθηκε ένα ML(machine learning) μοντέλο για την πρόβλεψη μίας δεδομένης κίνησης (right-None-left) με δεδομένα από EEG με χρήση του EMOTIV EPOC σε προγραμματιστικό περιβάλλον Python 3.6

Μέρος Ι : Προσέγγιση σταθερών χαρακτηριστικών:

1- φόρτωση δεδομένων

2- Εξαγωγή χαρακτηριστικών

3- προεπεξεργασία (τυποποίηση δεδομένων κ.λπ.)

4- δοκιμή διαφορετικών μοντέλων

5- συντονισμός του καλύτερου μοντέλου και βελτιστοποίηση της απόδοσης του.

Μέρος ΙΙ: Πολυμεταβλητή προσέγγιση χρονοσειρών:

1- φόρτωση δεδομένων

2- προεπεξεργασία (τυποποίηση δεδομένων κ.λπ.)

3- μοντελοποίηση

Χρήση SVM (Support Vector Machines), Decision Tree Classifier, Random Forest Classifier, Extreme Gradient Boosting Classifier (XGBoost), Long Short Term Memory networks

Μετά το πέρας των δοκιμών η πρόβλεψη κίνησης(αριστερά) ήταν απόλυτα επιτυχής με 98% ακρίβεια.

Εισαγωγή καινουριού κεφαλαίου ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΔΙΕΠΑΦΕΣ ΕΓΚΕΦΑΛΟΥ ΥΠΟΛΟΓΙΣΤΗ:

Όπως έχει αναφερθεί στα προηγούμενα κεφάλαια, ένα σύστημα ή πρόγραμμα που παρέχει άμεση σύνδεση μεταξύ υπολογιστή και εγκεφάλου ορίζεται ως σύστημα διεπαφής εγκεφάλου υπολογιστή (Brain Computer Interface). Η χρήση ενός τέτοιου συστήματος επικοινωνίας ωφελεί την τεχνολογία και την ιατρική με ποικίλους τρόπους, η οποία περιλαμβάνει την ικανότητα εργασίας μέσω υποκατάστασης ή ενίσχυσης στα ανθρώπινα άκρα, η οποία με τη σειρά της παρέχει κάποιο βαθμό ελευθερίας σε ανθρώπους με κινητικά προβλήματα ακόμη και με νευρωνική αποκατάσταση. Μπορεί να χρησιμοποιηθεί στον έλεγχο ταυτοπροσωποίησης του χρήστη σε υπολογιστικά συστήματα, παρέχει δηλαδή ένα εγκεκριμένο σύστημα ελέγχου ταυτότητας και αδειοδότησης χρήστη(user authentication). Έρευνες επίσης εστιάζουν σε επαναστατικές μεθόδους στα βιντεοπαιχνίδια και την ψυχαγωγία , την ρομποτική, σε εφαρμογές που βασίζονται σε smartphones, την τεχνητή νοημοσύνη και πολλά άλλα. Αυτή η ευρεία εφαρμογή καθιστά τα Brain Computer Interface (BCI) εξαιρετικά δημοφιλές στους ερευνητές και διερευνώνται νέοι τρόποι για να διευρύνουν τις χρήσεις τους για αυξημένη κατανόηση μεταξύ των γύρω συστημάτων, των χρηστών και του εγκεφάλου.

Η εστίαση βέβαια της αναπτυσσόμενης συγκεκριμένης βιομηχανίας παραμένει στα οφέλη και στις πολλαπλές εφαρμογές της, αγνοώντας κατάφωρα τα ζητήματα ασφάλειας στον κυβερνοχώρο που σχετίζονται με αλγόριθμους και συσκευές BCI. Οι εμπειρογνώμονες στον τομέα της ασφάλειας άρχισαν να εργάζονται σε θέματα ασφάλειας που σχετίζονται με τα BCI μετά από πολλές παραβιάσεις της ασφάλειας με την πάροδο του χρόνου. Αυτές οι επιθέσεις ή παραβιάσεις μπορούν να είναι πολλών τύπων στους οποίους τα εγκεφαλικά δεδομένα και μοτίβα (patterns) των χρηστών είναι υψίστης σημασίας για πολλούς αντιπάλους(μεταξύ

εταιρειών που παράγουν συστήματα BCI) και απειλητικούς παράγοντες(πχ κακόβουλοι hackers). Στην παρούσα έρευνα θα γίνει προσέγγιση για έναν ποιοτικό χαρακτηρισμό των επιθέσεων ασφαλείας που επηρεάζουν κάθε φάση του κύκλου BCI για να αναλυθούν οι επιπτώσεις τους και τα πιθανά αντίμετρα με σύγχρονα προϊόντα της αγοράς.

Διάφορα μέτρα μετριασμού όπως η ανίχνευση και η απόκριση Endpoint (EDR, endpoint detection and response) σχετικά με την ενσωμάτωσή του τόσο για την προστασία όσο και για την ανίχνευση συσκευών και προγραμμάτων BCI, καθώς αρκετά από αυτά λειτουργούν ως τελικά σημεία που δημιουργούν και αποθηκεύουν σημαντικές πληροφορίες.

Διατίθενται πολλές κορυφαίες λύσεις EDR όπως το FortiEdr της Fortinet, το Crowdstrike και το F-safe κ.λπ., οι οποίες θα συζητηθούν για να ελεγχθεί η βιωσιμότητά τους σε ένα τόσο προηγμένο πεδίο. Διαφορετικές εφαρμογές, τις οποίες αναφέραμε παραπάνω, θα διερευνηθούν περαιτέρω μαζί με προκλήσεις ασφάλειας στον επιστημονικό κλάδο της πληροφορικής και πως αυτές μπορούν να αντιμετωπιστούν και θα προταθούν λύσεις για τη μείωση του αντίκτυπου τέτοιων προκλήσεων

Αποδελτίωση σχετικής βιβλιογραφίας 31 άρθρων

Συγγραφή σχετικού κεφαλαίου διατριβής 6000 λέξεων

Συγγραφή ενός Systematic Literature review paper: Cybersecurity issues in brain-computer interfaces: a critical analysis of existing literature and future prospects 11.000 λέξεων

.

Αγγελάκης Δημήτριος

Υπ.Διδάκτορας, Τμήμα Μηχανικών Βιοϊατρικής