ΑΝΑΣΚΟΠΗΣΗ - REVIEW

ΝΟΣΗΛΕΥΤΙΚΗ 2025, 64(4): 27-36 • **HELLENIC JOURNAL OF NURSING** 2025, 64(4): 27-36

Θέματα Ασφάλειας στις Διεπαφές Εγκεφάλου – Η/Υ (BCI)

Ιωάννης Σταθούλης[1], Βησσαρίων Μπακάλης[2], Κώστας Βασιλάκης[3]

Security Issues in Brain – Computer Interfaces (BCI)

Abstract at the end of the article

[1]Βιοϊατρικός Μηχανικός PhD, Τμήμα Νοσηλευτικής, Πανεπιστήμιο Πελοποννήσου
[2]Εντεταλμένος Διδάσκων, Τμήμα Νοσηλευτικής, Πανεπιστήμιο Θεσσαλίας
[3]Καθηγητής, Τμήμα Πληροφορικής και Τηλεπικοινωνιών, Πανεπιστήμιο Πελοποννήσου

Υποβλήθηκε:09/04/2025
Επανυποβλήθηκε:15/07/2025
Εγκρίθηκε:10/11/2025

Υπεύθυνος αλληλογραφίας:
Ιωάννης Σταθούλης
e-mail: johnstathoulis@yahoo.gr, johnstathoulis@hotmail.com

Εισαγωγή: Τα συστήματα διασύνδεσης εγκεφάλου-υπολογιστή (BCI) εμφανίστηκαν για να αξιοποιήσουν και να ερμηνεύσουν την ηλεκτρική δραστηριότητα του εγκεφάλου για αλληλεπίδραση με εξωτερικές συσκευές. Το BCI, ή Brain-Machine Interface (BMI), ενσωματώνει υλικό και λογισμικό για να διευκολύνει την αλληλεπίδραση ανθρώπου-περιβάλλοντος ανεξάρτητα από τα περιφερικά νεύρα και τους μυς μέσω σημάτων ελέγχου από ηλεκτροεγκεφαλογραφικά δεδομένα. Στον τομέα της ασφάλειας, τα συστήματα BCI παραμένουν υποανάπτυκτα. Η σημασία της ασφάλειας στα συστήματα BCI συγκέντρωσε την προσοχή μόλις πρόσφατα, οδηγώντας στην εμφάνιση όρων όπως η νευροασφάλεια και η νευροηθική. Η βιβλιογραφία έχει εντοπίσει κατηγορίες απειλών ασφαλείας που επηρεάζουν την ακεραιότητα και την εμπιστευτικότητα του BCI, ωστόσο εξακολουθούν να λείπουν διεξοδικές έρευνες για αυτά τα ζητήματα.

Σκοπός: Σκοπός της παρούσας βιβλιογραφικής ανασκόπησης είναι η περιγραφή των πιθανών επιθέσεων ασφαλείας που επηρεάζουν την κάθε φάση του κύκλου ενός συστήματος BCI. Επίσης, η ανάλυση των επιπτώσεων των επιθέσεων αυτών καθώς και τα πιθανά αντίμετρα που μπορούν να χρησιμοποιηθούν και πώς αυτά τεκμηριώνονται βάσει της διεθνούς βιβλιογραφίας.

Υλικό και Μέθοδος: Πραγματοποιήθηκε αφηγηματική βιβλιογραφική ανασκόπηση βασισμένη σε άρθρα από επιστημονικές βάσεις δεδομένων (PubMed /Medline, Google Scholar) με τη χρήση συγκεκριμένων λέξεων-κλειδιών στην ελληνική και αγγλική γλώσσα, σε έντυπα βιβλία και αναφορές στο διαδίκτυο.

Αποτελέσματα: Μια κριτική επισκόπηση της βιβλιογραφίας αποκαλύπτει ότι ο τομέας της ασφάλειας που επικεντρώνεται στις τεχνολογίες συστημάτων BCI δεν είναι ακόμη ώριμος, δημιουργώντας ευκαιρίες για κακόβουλους φορείς να εξαπολύσουν επιθέσεις. Ακόμα και μη εξεζητημένες επιθέσεις μπορούν ωστόσο να έχουν σημαντικό αντίκτυπο τόσο στις τεχνολογίες συστημάτων BCI όσο και στην ασφάλεια των χρηστών. Επιπλέον, η ανάπτυξη πρωτοβουλιών τυποποίησης για την ενοποίηση των συστημάτων BCI όσον αφορά τις πληροφορίες αναγνωρίζεται ως ευκαιρία. Καλά μελετημένοι τομείς, όπως οι εμφυτεύσιμες ιατρικές συσκευές και το Διαδίκτυο των πραγμάτων, μπορούν να παράσχουν καθοδήγηση για την ανάπτυξη ισχυρών μηχανισμών ασφάλειας, ενώ η ευαισθητοποίηση των χρηστών σε θέματα ασφάλειας στα συστήματα BCI θεωρείται ζωτικής σημασίας.

Συμπεράσματα: Σημαντικές εξελίξεις στην έρευνα BCI έχουν σημειωθεί τις τελευταίες δύο δεκαετίες, αξιοποιώντας καθιερωμένες μεθοδολογίες στην επεξεργασία σήματος και την αναγνώριση προτύπων. Πολλές μελέτες έχουν βελτιώσει την ακρίβεια του BCI και έχουν προτείνει μεθόδους για αποτελεσματική μεταφορά πληροφοριών, παρά τις προκλήσεις στην επεξεργασία εγκεφαλικού σήματος. Κατά συνέπεια, η διάρκεια εκπαίδευσης των χρηστών έχει μειωθεί, διευκολύνοντας την ευρύτερη εφαρμογή BCI για άτομα με αναπηρίες, συμπεριλαμβανομένης της επεξεργασίας κειμένου και της νευροπροσθετικής. Οι περισσότερες εφαρμογές BCI βρίσκονται ακόμη στη φάση της έρευνας και δεν είναι ακόμη κατάλληλες για ευρεία καθημερινή χρήση. Οι τρέχοντες περιορισμοί περιλαμβάνουν χαμηλούς ρυθμούς μεταφοράς πληροφοριών, μεταβλητή αξιοπιστία και ταλαιπωρία λόγω απαιτήσεων συντήρησης ηλεκτροδίων και χειρισμού λογισμικού. Υπάρχουν πολλά προτεινόμενα αντίμετρα για τον μετριασμό των κινδύνων, αλλά η εκτεταμένη έρευνα εξακολουθεί να είναι απαραίτητη λόγω των σημαντικών απειλών που σχετίζονται με αυτά τα συστήματα.

Λέξεις ευρετηρίου: *Διεπαφή Εγκεφάλου – Η/Υ, Συστήματα BCI, Κυβερνοασφάλεια, Ιδιωτικότητα, Νευροασφάλεια, Νευροεμπιστευτικότητα,*

Εισαγωγή

Τα συστήματα διεπαφής εγκεφάλου-υπολογιστή (BCI) έκαναν την αρχική τους εμφάνιση τη δεκαετία του 1970, με στόχο τη συλλογή και επεξεργασία της ηλεκτρικής δραστηριότητας του εγκεφάλου που εκτίθενται από τους χρήστες, προκειμένου στη συνέχεια να εκτελέσουν καθορισμένες ενέργειες μέσω εξωτερικών μηχανών ή συσκευών.[1] Το σύστημα διεπαφής εγκεφάλου-υπολογιστή (BCI), το οποίο είναι επίσης γνωστό ως σύστημα Brain-Machine Interface (BMI), αποτελεί ένα ολοκληρωμένο σύστημα που συγχωνεύει τόσο υλικό όσο και λογισμικό, επιτρέποντας έτσι την ανθρώπινη αλληλεπίδραση με το περιβάλλον τους χωρίς εξάρτηση από περιφερικά νεύρα και μύες, μέσω της χρήσης σημάτων ελέγχου που προέρχονται από ηλεκτροεγκεφαλογραφική δραστηριότητα.[2] Οι δυνατότητες των συστημάτων BCI έχουν διευρυνθεί, επιτρέποντας όχι μόνο την καταγραφή της νευρικής δραστηριότητας αλλά και τη διέγερση του εγκεφάλου.[3]

Στον τομέα της ασφάλειας, τα συστήματα διεπαφής εγκεφάλου-υπολογιστή (BCI) παραμένουν σε μια πρώιμη φάση ανάπτυξης. Ο ακαδημαϊκός λόγος δεν θεωρούσε την ασφάλεια ως ουσιαστική διάσταση των συστημάτων BCI μέχρι την έλευση των τελευταίων ετών, κατά τη διάρκεια των οποίων έχουν προκύψει ορολογίες όπως η νευροασφάλεια, η νευρο ιδιωτικότητα, η νευροεμπιστευτικότητα, η παραβίαση του εγκεφάλου και η νευροηθική.[4] Η βιβλιογραφία έχει οριοθετήσει συγκεκριμένες κατηγορίες απειλών ασφαλείας που θέτουν σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα, τη διαθεσιμότητα και τη συνολική ασφάλεια των συστημάτων BCI. Ωστόσο, αυτές οι έρευνες αποτυγχάνουν να διεξάγουν διεξοδική εξέταση και παραμελούν τις σχετικές υπάρχουσες ανησυχίες που σχετίζονται με αυτά τα κρίσιμα ζητήματα.[5,6]

Επιπλέον, ο πολλαπλασιασμός των συστημάτων διεπαφής εγκεφάλου-υπολογιστή (BCI) σε αναδυόμενους τομείς, όπως τα βιντεοπαιχνίδια και η ψυχαγωγία, δημιουργεί σημαντικούς κινδύνους όσον αφορά την εμπιστευτικότητα των δεδομένων.[5,6] Μέσα σε αυτό το πλαίσιο, η διασφάλιση των προσωπικών δεδομένων των χρηστών, που περιλαμβάνουν σκέψεις, συναισθήματα, σεξουαλικό προσανατολισμό ή θρησκευτικές πεποιθήσεις, διακυβεύεται εκτός εάν εφαρμοστούν κατάλληλα πρωτόκολλα ασφαλείας.[5,6] Επιπλέον, σύγχρονες μεθοδολογίες που σχετίζονται με συστήματα BCI, συμπεριλαμβανομένης της ενσωμάτωσης διεπαφών ολοκληρωμένων κυκλωμάτων, παρουσιάζουν πρόσθετες προκλήσεις ασφαλείας που αποδίδονται στην κλιμάκωση του όγκου δεδομένων και στη χρήση δυνητικά ευαίσθητων τεχνολογιών.[7]

Σκοπός

Σκοπός της παρούσας βιβλιογραφικής ανασκόπησης

είναι η περιγραφή των πιθανών επιθέσεων ασφαλείας που επηρεάζουν την κάθε φάση του κύκλου ενός συστήματος BCI. Επίσης, η ανάλυση των επιπτώσεων των επιθέσεων αυτών καθώς και τα πιθανά αντίμετρα που μπορούν να χρησιμοποιηθούν και πώς αυτά τεκμηριώνονται βάσει της διεθνούς βιβλιογραφίας

Υλικό και Μέθοδος

Πραγματοποιήθηκε αφηγηματική βιβλιογραφική ανασκόπηση βασισμένη σε άρθρα από επιστημονικές βάσεις δεδομένων (PubMed /Medline, Google Scholar) με τη χρήση συγκεκριμένων λέξεων- κλειδιών στην ελληνική και αγγλική γλώσσα, σε έντυπα βιβλία και αναφορές στο διαδίκτυο.

Αποτελέσματα

Πολλές ξεχωριστές διαμορφώσεις του κύκλου (BCI) έχουν οριοθετηθεί στην ακαδημαϊκή βιβλιογραφία. Παρ' όλα αυτά, οι επικρατούσες επαναλήψεις επικεντρώνονται αποκλειστικά στη λήψη σημάτων, παραμελώντας τη διέγερση των νευρώνων. Αυτές οι μεθοδολογίες παρουσιάζουν διάφορες ταξινομήσεις του κύκλου BCI; συγκεκριμένα, ορισμένοι δεν ενσωματώνουν τη δημιουργία εγκεφαλικών σημάτων ως ξεχωριστή φάση, ενώ άλλοι συγχωνεύουν πολλαπλές φάσεις σε μια μοναδική κατηγορία, αποτυγχάνοντας να διευκρινίσουν τις αντίστοιχες λειτουργίες τους.[8] Πρόσθετα πλαίσια, όπως διατυπώνονται στις αναφορές,6 παρουσιάζουν έναν βαθμό ασάφειας, καθώς κατηγοριοποιούν τις μεταβάσεις και τις ανταλλαγές δεδομένων μεταξύ διαφορετικών φάσεων ως νέες φάσεις. Στον τομέα των εφαρμογών, ορισμένοι μελετητές οριοθετούν ένα γενικευμένο στάδιο για εφαρμογές.[9] Αντίθετα, άλλοι ασχολούνται με την έννοια των εντολών που αποστέλλονται σε εξωτερικές συσκευές[10,11] και μόνο ένας περιορισμένος αριθμός εξετάζει τους μηχανισμούς ανάδρασης που παρέχουν οι εφαρμογές στους χρήστες.[11] Για να τυποποιηθεί ο κύκλος BCI και να διορθωθούν τα στοιχεία ή οι πηγές σύγχυσης που είχαν παραβλεφθεί προηγουμένως, προτείνεται μια αναθεωρημένη επανάληψη του κύκλου BCI, που περιλαμβάνει πέντε ξεχωριστές φάσεις (καθεμία με ρητά καθορισμένες εργασίες, εισόδους και εξόδους) που αναγνωρίζουν δεόντως τόσο τις δυνατότητες απόκτησης όσο και τις δυνατότητες διέγερσης.

Σύμφωνα με τη διαδικασία νευρικής απόκτησης, η φάση 1 περιλαμβάνει τη δημιουργία νευρικών σημάτων. Τα προκύπτοντα δεδομένα αντικατοπτρίζουν την πρόθεση του χρήστη να εκτελέσει συγκεκριμένες ενέργειες, όπως η λειτουργία μιας εξωτερικής συσκευής. Στη φάση 2, τα εγκεφαλικά κύματα συλλέγονται μέσω διαφόρων τεχνολογιών, συμπεριλαμβανομένης της ηλεκτροεγκεφαλογραφίας (EEG) και της λειτουργικής απεικόνισης μαγνητικού συντονισμού (fMRI). Τα ακατέργαστα αναλογικά σήματα που ενσωματώνουν την πρόθεση του χρήστη μεταδίδονται στη συνέχεια στη φάση 3, απαιτώντας επεξεργασία δεδομένων και μετατροπή. Συγκεκριμένα, αυτή η φάση συνεπάγεται τη μετατροπή αναλογικών σημάτων σε ψηφιακές μορφές για τη διευκόλυνση της επακόλουθης επεξεργασίας δεδομένων.

Ένας από τους πρωταρχικούς στόχους αυτής της συγκεκριμένης φάσης είναι η βελτιστοποίηση του λόγου σήματος προς θόρυβο (SNR), ο οποίος χρησιμεύει για την αξιολόγηση της έντασης του σήματος στόχου σε σχέση με το επίπεδο θορύβου περιβάλλοντος, διασφαλίζοντας έτσι ότι το αρχικό σήμα αποκτάται με μέγιστη ακρίβεια, ενώ ταυτόχρονα προσπαθεί να διατηρήσει αυτόν τον υψηλό βαθμό ακρίβειας για παρατεταμένη διάρκεια. Η φάση 4 συνεπάγεται την επεξεργασία ψηφιακών νευρωνικών δεδομένων για την ερμηνεία της αναμενόμενης ενέργειας του χρήστη, όπου τα σχετικά χαρακτηριστικά εξάγονται και επιλέγονται από τα νευρικά δεδομένα. Στη συνέχεια, μια ποικιλία μοντέλων (π.χ. ταξινομητές, αλγόριθμοι πρόβλεψης και αναλύσεις παλινδρόμησης) ή συστήματα που βασίζονται σε κανόνες χρησιμοποιούνται για την εξακρίβωση της προβλεπόμενης δράσης.[11,12] Η ενέργεια τελικά κορυφώνεται στις εφαρμογές κατά τη φάση 5, οι οποίες εκτελούν τις ενεργειακές λειτουργίες. Επιπλέον, οι εφαρμογές είναι ικανές να μεταδίδουν προαιρετική ανάδραση στον χρήστη για να προκαλέσουν εγκεφαλικά σήματα, διευκολύνοντας έτσι νέες επαναλήψεις του κύκλου.

Όσον αφορά τη διαδικασία διέγερσης, ο κύκλος ξεκινά στη φάση 5, όπου η ενέργεια διέγερσης οριοθετείται με ευρύ τρόπο, για παράδειγμα, η διέγερση μιας καθορισμένης περιοχής του εγκεφάλου για τη βελτίωση των συμπτωμάτων της νόσου του Alzheimer. Αυτή η προτεινόμενη παρέμβαση μεταφέρεται στη συνέχεια στη φάση 4, όπου υφίσταται επεξεργασία χρησιμοποιώντας μια ποικιλία μεθοδολογιών, συμπεριλαμβανομένης της μηχανικής μάθησης (ML), με στόχο την παραγωγή ενός μοτίβου πυροδότησης που ενσωματώνει εξελιγμένες πληροφορίες σχετικά με τις συσκευές διέγερσης που έχουν προγραμματιστεί για ενεργοποίηση, τις συχνότητες που χρησιμοποιούνται και τον χρονικό προγραμματισμό. Η φάση 3 ασχολείται με τον μετασχηματισμό του μοτίβου πυροδότησης που αποκτήθηκε, το οποίο περιγράφεται με γενική έννοια, σε συγκεκριμένες παραμέτρους που σχετίζονται άμεσα με την τεχνολογία που

χρησιμοποιείται στο σύστημα διεπαφής εγκεφάλου-υπολογιστή (BCI).

Για παράδειγμα, η διαδικασία προσδιορισμού περιλαμβάνει τον εντοπισμό συγκεκριμένων νευρώνων που απαιτούν διέγερση, καθώς και τα απαιτούμενα επίπεδα έντασης και τάσης που είναι απαραίτητα για την εκτέλεση της διαδικασίας. Η φάση 2 μεταφέρει αυτές τις παραμέτρους διέγερσης στο σύστημα διέγερσης, το οποίο είναι επιφορτισμένο με τη φυσική διέγερση του εγκεφαλικού φλοιού. Μετά από αυτήν την παρέμβαση, ο εγκέφαλος δημιουργεί νευρωνική δραστηριότητα ως απόκριση, η οποία μπορεί στη συνέχεια να συλληφθεί από το σύστημα BCI για να αξιολογήσει την εγκεφαλική κατάσταση μετά από κάθε συμβάν διέγερσης.

Η βιβλιογραφία έχει καταγράψει εκτενώς περιπτώσεις παραπλανητικών ερεθισμάτων,[13] έναν μηχανισμό που τροποποιεί τα νευρικά σήματα εξόδου μέσω της σκόπιμης παρουσίασης χειραγωγημένων ερεθισμάτων σε χρήστες που ασχολούνται με ένα σύστημα BCI. Τα δυναμικά που σχετίζονται με συμβάντα (ERP) αντιπροσωπεύουν νευροφυσιολογικές αποκρίσεις που προκαλούνται από γνωστικά, αισθητηριακά ή κινητικά ερεθίσματα, αναγνωρίσιμα ως ένα διακριτικό μοτίβο διακύμανσης τάσης.[8]

Από τη μία πλευρά, οι Martinovic et al.[14] χρησιμοποίησαν το δυναμικό P300 για την εξαγωγή εμπιστευτικών πληροφοριών από πειραματικά άτομα και απεικόνισαν την αποτελεσματικότητα των παραπλανητικών επιθέσεων ερεθίσματος. Τα οπτικά ερεθίσματα χορηγήθηκαν με τη μορφή εικόνων, κατηγοριοποιημένες ως εξής: τετραψήφιοι προσωπικοί αριθμοί αναγνώρισης, αυτόματες ταμειακές μηχανές, πιστωτικές κάρτες, μήνες γέννησης και φωτογραφίες ατόμων. Ο στόχος του πειράματος ήταν να αποδείξει ότι οι συμμετέχοντες εμφανίζουν αυξημένη κορυφή στο δυναμικό P300 όταν έρχονται αντιμέτωποι με ένα οικείο ερέθισμα, επιτρέποντας έτσι την εξαγωγή ιδιωτικών πληροφοριών.

Σε σχέση με τις ακουστικές προκληθείσες δυνατότητες (AEP), υπάρχει έλλειψη συγκεκριμένων εργασιών που οριοθετούν επιθέσεις που χρησιμοποιούν ακουστικά ερεθίσματα. Παρ' όλα αυτά, οι Fukushima et al.[15] διευκρίνισαν ότι οι ανεπαίσθητοι ήχοι υψηλής συχνότητας μπορεί να επηρεάσουν σημαντικά την εγκεφαλική δραστηριότητα. Αυτή η συγκεκριμένη περίσταση δημιουργεί νέες προοπτικές για εισβολείς στον κυβερνοχώρο, καθώς η διατύπωση μη ακουστικών ερεθισμάτων δεν απαιτεί στενή εμπλοκή με τον στόχο, διευκολύνοντας έτσι την ικανότητα του δράστη να παραμείνει αδιευκρίνιστος.

Στο πλαίσιο της νευρικής διέγερσης, αυτή η φάση σημαίνει το αποτέλεσμα της διαδικασίας διέγερσης που συμβαίνει στον εγκεφαλικό φλοιό. Δύο κύριες ταξινομήσεις επιθέσεων μπορούν να εντοπιστούν κατά τη διάρκεια της διαδικασίας νευροδιέγερσης. Η αρχική κατηγορία περιλαμβάνει τον σφετερισμό του μηχανισμού διέγερσης με σκοπό να προκαλέσει βλάβη στον νευρικό ιστό. Τέτοιες επιθέσεις μπορεί να μιμούνται ή να εντείνουν τις ανεπιθύμητες δευτερογενείς επιδράσεις που συνήθως σχετίζονται με τη θεραπευτική αντιμετώπιση νευρολογικών διαταραχών, συμπεριλαμβανομένης της νόσου του Πάρκινσον, είτε μέσω μηχανισμών υπερδιέγερσης είτε μέσω της αναστολής των τυπικών τρόπων θεραπείας.[16,17] Η επόμενη κατηγορία επιθέσεων αφορά την πρόκληση ενός συγκεκριμένου αποτελέσματος ή αντίληψης στον χρήστη. Η νευροδιέγερση μπορεί να προκαλέσει μια ποικιλία ψυχιατρικών και ψυχολογικών εκδηλώσεων, όπως διακυμάνσεις της διάθεσης, καταθλιπτικά επεισόδια, άγχος ή αυτοκτονικό ιδεασμό. Ένας εισβολέας θα μπορούσε να ενισχύσει αυτές τις εκδηλώσεις μέσω του χειρισμού επιβλαβών παραμέτρων διέγερσης για να εκμεταλλευτεί τις ευπάθειες του χρήστη.

Συγκεκριμένα, οι Landau et al.[13] διευκρίνισαν ότι η παρουσία παραπλανητικών ερεθισμάτων κατά τη διαδικασία της ιατρικής διάγνωσης, που παραδειγματίζεται από μια φωτοευαίσθητη αξιολόγηση επιληψίας που περιλαμβάνει την παρουσίαση πληθώρας οπτικών ερεθισμάτων, έχει τη δυνατότητα να οδηγήσει σε λανθασμένες διαγνώσεις, θέτοντας έτσι σε κίνδυνο την ασφάλεια των χρηστών. Επιπλέον, παρατηρήθηκε ότι η ψυχολογική διάθεση των ατόμων μπορεί να διαμορφωθεί μέσω οπτικών ερεθισμάτων, είτε συνειδητά αντιληπτών είτε υποσυνείδητα επεξεργασμένων.

Επιδιώκοντας αντίμετρα που αποσκοπούν στη μείωση του αντίκτυπου των επιθέσεων παραπλανητικών ερεθισμάτων, πολυάριθμες μελέτες[13,18] έχουν οριοθετήσει ολοκληρωμένες στρατηγικές για την ενίσχυση της ευαισθητοποίησης των ατόμων που χρησιμοποιούν συστήματα Brain-Computer Interface (BCI), που περιλαμβάνουν (i) τη διάδοση πληροφοριών σε κλινικούς ιατρούς και ασθενείς σχετικά με τους εγγενείς κινδύνους που σχετίζονται με αυτές τις τεχνολογίες και (ii) την ολοκληρωμένη εκπαίδευση των χρηστών σχετικά με τις λειτουργίες αυτών των συστημάτων. Η παρατήρηση αυτή είναι ιδιαίτερα αξιοσημείωτη, δεδομένου ότι οι ανθρώπινοι χειριστές αποτελούν συνήθως το πιο ευάλωτο στοιχείο σε ένα πλαίσιο ασφαλείας. Συγκεκριμένα, ο Ienca[19] έχει διατυπώσει ότι οι προσαρμοσμένες εκπαιδευτικές συνεδρίες μπορεί να αποδειχθούν επω-

φελείς για την προστασία των χρηστών από ερεθίσματα που έχουν τη δυνατότητα να είναι επικίνδυνα, ιδιαίτερα σε σχέση με τα πρωτόκολλα ελέγχου ταυτότητας και τις οικονομικές πληροφορίες.

Η φάση που σχετίζεται με την απόκτηση και διέγερση νευρωνικών δεδομένων δίνει έμφαση στη δέσμευση συστημάτων Brain-Computer Interface (BCI) με εγκεφαλικές δομές για την απόκτηση νευρικών δεδομένων ή την εκτέλεση της διέγερσής τους. Όσον αφορά την απόκτηση δεδομένων, οι μελετητές έχουν διακρίνει την εφαρμογή μιας συνεργιστικής προσέγγισης που περιλαμβάνει επιθέσεις επανάληψης και πλαστογραφίας, όπου προηγούμενα σήματα από τον χρήστη του συστήματος BCI, σήματα από εναλλακτικούς χρήστες ή περίπλοκα σήματα μπορεί να εκπροσωπούνται λανθασμένα ως κανονιστικά εγκεφαλικά κύματα.[13] Επιπλέον, υπάρχει η δυνατότητα για την εφαρμογή αυτών των επιθέσεων εντός συστημάτων διέγερσης, σύμφωνα με τα οποία ένας επιτιθέμενος θα μπορούσε να επιβάλει συγκεκριμένους τρόπους διέγερσης που βασίζονται σε προηγούμενες συμπεριφορές. Ένα πιθανό αποτέλεσμα τέτοιου χειρισμού θα μπορούσε να είναι η αύξηση της τάσης που χορηγείται στον εγκεφαλικό φλοιό του ασθενούς.[20]

Όσον αφορά τις επιπτώσεις που προκλήθηκαν από προηγούμενες επιθέσεις, οι Li et al.[6] διευκρίνισαν ότι τόσο οι επιθέσεις επανάληψης όσο και οι επιθέσεις πλαστοπροσωπίας θέτουν σε κίνδυνο την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, εμποδίζοντας έτσι τις διαδικασίες που είναι απαραίτητες για την απόκτησή τους. Επιπλέον, οι Landau et al.[13] υπογράμμισαν ότι τέτοιες επιθέσεις έχουν τη δυνατότητα να διαταράξουν τις κλινικές διαγνωστικές διαδικασίες αντικαθιστώντας αυθεντικά εγκεφαλικά σήματα με κακά αντίστοιχα, οδηγώντας κατά συνέπεια σε λανθασμένες διαγνώσεις, οι οποίες μπορεί να οδηγήσουν στην αποτυχία παροχής κατάλληλης θεραπείας ή τη χορήγηση ακατάλληλων παρεμβάσεων σε ασθενείς με καλή υγεία.

Είναι σημαντικό να αναγνωρίσουμε ότι οι επιθέσεις σε προηγμένες τεχνολογίες όπως η λειτουργική απεικόνιση μαγνητικού συντονισμού (fMRI) ή η μαγνητοεγκεφαλογραφία (MEG) μπορεί να έχουν πιο σημαντική οικονομική επίπτωση λόγω του υπερβολικού κόστους που σχετίζεται με αυτές τις μεθόδους σε αντίθεση με εναλλακτικές λύσεις όπως η ηλεκτροεγκεφαλογραφία (EEG).[21] Ωστόσο, το EEG παραμένει η πιο εκτενώς ερευνημένη τεχνολογία απόκτησης σε σχέση με την ασφάλεια, που αποδίδεται στην ευρεία προσβασιμότητά του πέρα από τα κλινικά περιβάλλοντα, υπογραμμίζοντας έτσι τη δυνατότητα συμβιβασμών όπως επιθέσεις παραπλανητικών ερεθισμάτων ή επιθέσεις παρεμβολών.

Σε σχέση με αντίμετρα που αποσκοπούν στον εντοπισμό και την ανακούφιση των επιθέσεων επανάληψης και εξαπάτησης, οι Landau et al.[13] υποστήριξαν την εφαρμογή μηχανισμών ανίχνευσης ανωμαλιών για την απόκτηση δεδομένων, ειδικά για τον εντοπισμό τροποποιημένων εισόδων, παράλληλα με την ενίσχυση της ακρίβειας των συσκευών απόκτησης. Κατά συνέπεια, προτείνεται ένας μηχανισμός που θα επέτρεπε την απενεργοποίηση ηλεκτροδίων που θεωρούνται περιττά για το τρέχον λειτουργικό πλαίσιο, μετριάζοντας έτσι τους πιθανούς κινδύνους, συμπεριλαμβανομένης της απόκτησης σημάτων P300 εντός της εγκεφαλικής δραστηριότητας. Συγκεκριμένα, οι Landau et al.[13] συνέστησαν τη χρήση μιας συλλογής ταξινομητών για να διακρίνει την προσθήκη θορύβου στα τυπικά (μη κακόβουλα) δεδομένα εισόδου. Ως προτεινόμενο σύνολο αντιμέτρων, οι Vadlamani et al.[22] οριοθέτησαν τη χρήση της μετάδοσης χαμηλής ισχύος ως βιώσιμη στρατηγική για την περιπλοκή της ανίχνευσης νόμιμων μεταδόσεων από αντιπάλους, παράλληλα με την ανάπτυξη κατευθυντικών κεραιών προσανατολισμένων στον εγκέφαλο για την παράκαμψη των εμποδίων επικοινωνίας.

Η φάση επεξεργασίας και μετατροπής δεδομένων περιλαμβάνει τις βασικές εργασίες που είναι απαραίτητες για την επαρκή προετοιμασία των νευρικών δεδομένων και των ενεργειών διέγερσης για τα επόμενα στάδια. Αν και η υπάρχουσα βιβλιογραφία δεν έχει οριοθετήσει ρητά τις ευπάθειες ασφαλείας κατά τη διάρκεια αυτής της φάσης, οι Bonaci et al.[23] ισχυρίζονται ότι αυτή η φάση είναι ευαίσθητη σε πιθανές επιθέσεις κακόβουλου λογισμικού, οι οποίες μπορεί να επιτρέψουν στους αντιπάλους να αποκτήσουν ολοκληρωμένο έλεγχο του συστήματος Brain-Computer Interface (BCI).

Όσον αφορά τα αντίμετρα που στοχεύουν στον μετριασμό των επιθέσεων που θέτουν σε κίνδυνο την εμπιστευτικότητα των δεδομένων, οι Chizeck et al.[23] έχουν καινοτομήσει μια νέα τεχνολογία που ονομάζεται «Ανώνυμη διασύνδεση εγκεφάλου-υπολογιστή», η οποία διαθέτει την ικανότητα να επεξεργάζεται νευρικά σήματα με τρόπο που εξαλείφει όλες τις μη απαραίτητες ιδιωτικές πληροφορίες.[24] Κατά συνέπεια, ευαίσθητα δεδομένα δεν διατηρούνται εντός του συστήματος BCI ούτε μεταδίδονται εξωτερικά. Επιπλέον, οι Ienca et al.[25] έχουν προτείνει την εφαρμογή διαφορικού απορρήτου για την ενίσχυση τόσο της ασφάλειας όσο και της διαφάνειας εντός του παραδείγματος επεξεργασίας δεδομένων. Επιπλέον, η ανάπτυξη λογισμικού προστασίας από ιούς και συστημάτων ανίχνευσης εισβολών (IDS) ως προστατευτικά

μέτρα για μεμονωμένες συσκευές αποδεικνύεται σημαντικά πλεονεκτική.[13] Άλλοι μελετητές υποστηρίζουν την εφαρμογή μηχανισμών περιμετρικής ασφάλειας, όπως τα τείχη προστασίας, τα οποία είναι επιφορτισμένα με τον έλεγχο όλων των εισερχόμενων και εξερχόμενων επικοινωνιών κάθε συσκευής. Επιπλέον, ένα άλλο αντίμετρο περιλαμβάνει την εφαρμογή μηχανικής μάθησης (ML) σε συστήματα ανίχνευσης ανωμαλιών για τη διάκριση πιθανών απειλών που προέρχονται από κακόβουλο λογισμικό.[26]

Οι διαδικασίες κωδικοποίησης και αποκωδικοποίησης αντιπροσωπεύουν την κρίσιμη φάση που δίνει έμφαση στην ταυτοποίηση της ενέργειας που επιθυμούν οι χρήστες στο πλαίσιο της απόκτησης νευρωνικών δεδομένων ή της εξακρίβωσης των μοτίβων νευρωνικής πυροδότησης στη νευροδιέγερση. Οι εισβολές κακόβουλου λογισμικού που στοχεύουν στη λήψη αυτών των σημάτων έχουν διευκρινιστεί από τους Bonaci et al.[23], οι οποίοι διευκρίνισαν ότι οι δράστες θα μπορούσαν να εκμεταλλευτούν κακόβουλο λογισμικό για να παρακάμψουν τη λειτουργικότητα αυτής της φάσης ή να ενσωματώσουν πρόσθετους επιβλαβείς αλγόριθμους. Επιπλέον, οι εισβολές κακόβουλου λογισμικού μπορούν να κατευθυνθούν προς τη ροή διέγερσης, διακόπτοντας έτσι ή σταματώντας τον σχηματισμό ενός μοτίβου πυροδότησης, αξιοποιώντας τους αλγόριθμους ταξινόμησης που χρησιμοποιούνται. Τέτοιες εισβολές έχουν επιπτώσεις σε όλες τις ποικιλίες μοντέλων μηχανικής μάθησης (ML) και κατά συνέπεια, παρουσιάζουν ένα συνεχιζόμενο ερευνητικό δίλημμα.[12]

Οι προαναφερθείσες επιθέσεις έχουν ξεχωριστές επιπτώσεις στο σύστημα διασύνδεσης εγκεφάλου-υπολογιστή (BCI). Από τη μία πλευρά, το κακόβουλο λογισμικό ασκεί επιρροή στην ακεραιότητα και τη διαθεσιμότητα των δεδομένων, καθώς έχει την ικανότητα να τροποποιεί ή να αντικαθιστά τα δεδομένα που αποκτήθηκαν από προηγούμενα στάδια και να παρακάμψει την έξοδο της τρέχουσας φάσης, διακόπτοντας έτσι τις επιδιωκόμενες ενέργειες που αποστέλλονται στις εφαρμογές του συστήματος BCI κατά τη διαδικασία απόκτησης, όπως παρεμπόδιση του ελέγχου μιας αναπηρικής πολυθρόνας ή αλλαγή της τροχιάς της ή επηρεάζοντας την ενεργοποίηση ακολουθίας για νευρωνική διέγερση, γεγονός που διευκολύνει ένα ευρύ φάσμα δυνατοτήτων επιθέσεις, όπως έχει τεκμηριωθεί προηγουμένως. Επιπλέον, το κακόβουλο λογισμικό θέτει σε κίνδυνο τη διαθεσιμότητα λειτουργιών μηχανικής μάθησης (ML) τροποποιώντας το μοντέλο που δημιουργείται από τον αλγόριθμο εκπαίδευσης ή μηχανικής μάθησης (ML). Όσον αφορά την εμπιστευτικότητα των δεδομένων, το κακόβουλο λογισμικό έχει τη δυνατότητα να διεισδύσει στις δυνατότητες που χρησιμοποιούνται στη φάση εκπαίδευσης του αλγορίθμου μηχανικής μάθησης (ML), καθώς και να συλλέξει πληροφορίες σχετικά με το μοντέλο και τον αλγόριθμο που χρησιμοποιείται. Επιπλέον, το κακόβουλο λογισμικό θέτει σε κίνδυνο την ασφάλεια των χρηστών, καθώς οι προηγούμενες επιπτώσεις στην ακεραιότητα και τη διαθεσιμότητα καταλήγουν σε κακόβουλες ενέργειες και ακολουθίες ενεργοποίησης που θέτουν σε κίνδυνο την ακεραιότητα του χρήστη, ενδεχομένως με αποτέλεσμα νευρική βλάβη ή εμφάνιση συγκεκριμένων ψυχολογικών διαταραχών.

Προκειμένου να μετριαστούν οι επιπτώσεις των επιθέσεων κατά τη φάση εκπαίδευσης του αλγορίθμου μηχανικής μάθησης (ML), οι οποίες θέτουν σε κίνδυνο την ακεραιότητα και τη διαθεσιμότητα, μια ποικιλία τεχνικών που στοχεύουν στην αντιμετώπιση των αντίστοιχων επιθέσεων έχουν προταθεί στην επιστημονική βιβλιογραφία. Αρχικά, συνιστάται η απολύμανση των δεδομένων που θεωρούνται ευεργετικά για την εξάλειψη δειγμάτων που περιέχουν κακόβουλες πληροφορίες, διαταράσσοντας έτσι το μοντέλο. Οι Jagielski et al.[27] παρουσίασαν μια συγκρίσιμη στρατηγική κατά των επιθέσεων δηλητηρίασης που εφαρμόζονται σε μεθοδολογίες παλινδρόμησης, όπου ο θόρυβος και οι ακραίες τιμές διαγράφονται από το σύνολο δεδομένων εκπαίδευσης.

Οι Landau et al.[13] οριοθέτησαν πολλούς κινδύνους που σχετίζονται με εφαρμογές συστημάτων BCI. Συγκεκριμένα, διευκρινίζουν ότι ένας εισβολέας θα μπορούσε να διαταράξει την ικανότητα του χρήστη να χρησιμοποιεί τη συσκευή, θέτοντας έτσι σε κίνδυνο τη διαθεσιμότητά της. Εξέφρασαν επίσης ανησυχίες σχετικά με την εμπιστευτικότητα, ειδικά σε σχέση με την ταυτοποίηση των χρηστών μέσω των νευρωνικών δεδομένων τους, θέτοντας ένα σενάριο στο οποίο ένας εισβολέας εξάγει δεδομένα ηλεκτροεγκεφαλογράφου (EEG) από την εφαρμογή και τα συσχετίζει με τη βάση δεδομένων ΗΕΓ ενός νοσοκομείου, επιτρέποντας έτσι την αναγνώριση του χρήστη και την μη εξουσιοδοτημένη πρόσβαση στα ιατρικά αρχεία του. Μια τέτοια ταυτοποίηση θα μπορούσε να προκαλέσει περιπτώσεις διακρίσεων βάσει σχέσης με συγκεκριμένα δημογραφικά στοιχεία, συμπεριλαμβανομένων θρησκευτικών πεποιθήσεων[28] ή ιατρικών ιστορικών.

Τελικά, οι επιθέσεις που θέτουν σε κίνδυνο αυτήν τη φάση μπορούν να προκαλέσουν εφαρμογές για τη μετάδοση επιβλαβών ερεθισμάτων ή την εφαρμογή ενεργειών που μπορεί να οδηγήσουν σε σωματικό

τραυματισμό.[29] Λαμβάνοντας υπόψη τις επιπτώσεις προηγούμενων επιθέσεων, οι εφαρμογές που προκύπτουν από επιθέσεις πλαστοπροσωπίας (πλαστογραφία) θέτουν σε κίνδυνο τόσο την ακεραιότητα όσο και την εμπιστευτικότητα των δεδομένων, καθώς μπορεί να εισαγάγουν κακόβουλα ερεθίσματα με σκοπό την εξαγωγή ευαίσθητων πληροφοριών από νευρώνες, όπως γνωστικές διαδικασίες ή πεποιθήσεις.[29] Σε περιπτώσεις νευροδιέγερσης, οι κακές εφαρμογές θα μπορούσαν να αλλάξουν εντελώς τα πρότυπα πυροδότησης που χρησιμοποιούνται για την τόνωση των ασθενών, θέτοντας έτσι σημαντικό κίνδυνο για την ασφάλεια. Πιο συγκεκριμένα, αυτές οι εφαρμογές θα μπορούσαν να υποκινήσουν ψυχολογικές παρεμβάσεις στο θύμα, καθιστώντας το πιο ευαίσθητο σε τυχερά παιχνίδια ή ακόμη και προωθώντας επιβλαβείς ψυχολογικές καταστάσεις, όπως άγχος και κατάθλιψη. Σε αυτό το πλαίσιο, ο εισβολέας θα μπορούσε να εκμεταλλευτεί αυτές τις τροποποιημένες ψυχικές καταστάσεις ενσωματώνοντας διαφημίσεις μέσα στην εφαρμογή, με στόχο τη δημιουργία κέρδους εις βάρος του θύματος.

Μεταβαίνοντας σε επιθέσεις εισαγωγής δεδομένων, αυτές οι κακόβουλες δραστηριότητες μπορούν να προκαλέσουν απώλεια, τροποποίηση και διαφθορά δεδομένων, υπονομεύοντας έτσι την ακεραιότητα των εφαρμογών.[30] Σε σχέση με την εμπιστευτικότητα, τέτοιες επιθέσεις μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών σε οντότητες που δεν διαθέτουν κατάλληλη έγκριση[30], συμπεριλαμβανομένων των ασφαλιστικών παρόχων που επιδιώκουν να εντοπίσουν τους βέλτιστους υποψηφίους για τις προσφορές τους. Η διαθεσιμότητα υπηρεσιών μπορεί να τεθεί σε κίνδυνο από την άρνηση πρόσβασης μέσω πλαισίων ελέγχου ταυτότητας ή με την υποκίνηση σφαλμάτων, εξόδων ή επανεκκινήσεων εφαρμογών, οι οποίες μπορούν να διαταράξουν βασικές λειτουργίες όπως η κλινική νευροδιέγερση.[30]

Είναι επιτακτική ανάγκη να εξακριβωθεί η ορθή λειτουργία των εφαρμογών λογισμικού και να διασφαλιστεί η αποτελεσματική διακυβέρνηση των διαύλων πωλήσεων και διανομής των εφαρμογών ώστε να μειωθεί ο κίνδυνος επιθέσεων πλαστοπροσωπίας. Οι Landau et al.[13] υποστήριξαν τη χρήση εφαρμογών που έχουν σχεδιαστεί από διαπιστευμένες οντότητες για να εξακριβωθεί η αξιοπιστία τους. Όσον αφορά τις εισβολές κακόβουλου λογισμικού, τα ίδια αντίμετρα που συνιστώνται για επιθέσεις επεξεργασίας δεδομένων και μετασχηματισμού ισχύουν εξίσου για εφαρμογές, συμπεριλαμβανομένης της ανάπτυξης λογισμικού προστασίας από ιούς, τείχους προστασίας, συστημάτων ανίχνευσης εισβολών (IDS) και συστημάτων ανίχνευσης ανωμαλιών για τον εντοπισμό επιθέσεων και τη μείωση των εκτεταμένων επιπτώσεων τους. Οι Takabi et al.[5] συνέστησαν την εφαρμογή μηχανισμών ελέγχου πρόσβασης για εισερχόμενα δεδομένα για τον περιορισμό της προσβασιμότητάς τους και έτσι να μετριάσουν τις επιπτώσεις στην εμπιστευτικότητα. Επιπλέον, προτείνεται η χρήση τεχνικών τυχαιοποίησης και διαφορικού απορρήτου, παράλληλα με την ενσωμάτωση ομομορφικής κρυπτογράφησης για τον χειρισμό κρυπτογραφημένων δεδομένων σε συνδυασμό με λειτουργική κρυπτογράφηση για πρόσβαση σε ένα συγκεκριμένο υποσύνολο πληροφοριών. Σε σχέση με τις επιθέσεις υπερχείλισης μνήμης, είναι ζωτικής σημασίας να χρησιμοποιηθούν γλώσσες προγραμματισμού που εγγενώς αμυνθούν έναντι τέτοιων απειλών, εκτός από τη χρήση μεταγλωττιστών εξοπλισμένων με μηχανισμούς ανίχνευσης.[31]

Συμπεράσματα

Η παρούσα βιβλιογραφική ανασκόπηση αφορά στην ασφάλεια και την προστασία των συστημάτων BCI. Ειδικότερα περιγράφονται οι επιθέσεις ασφαλείας, οι επιπτώσεις των επιθέσεων και τα αντίμετρα επιθέσεων. Από τη βιβλιογραφία προτείνεται μια ενοποιημένη εκδοχή του κύκλου ενός συστήματος BCI που περιλαμβάνει τόσο την απόκτηση δεδομένων από τους νευρώνες όσο και τη διαδικασία της διέγερσης των νευρώνων.

Παρόλο που η έρευνα στα συστήματα BCI είναι σχετικά νέα, σημαντική πρόοδος έχει πραγματοποιηθεί σε περίπου δύο δεκαετίες, γεγονός που κατέστη εφικτό μέσω της αξιοποίησης ήδη ώριμων μεθόδων και αποτελεσμάτων έρευνας στις περιοχές της επεξεργασίας σήματος και της αναγνώρισης προτύπων. Πολλές μελέτες έχουν συνδράμει στην αύξηση της ακρίβειας των συστημάτων BCI και έχουν προτείνει μεθόδους για την απόκτηση πληροφορίας με επαρκή ρυθμό bit, παρά τις εγγενείς σημαντικές δυσκολίες στην επεξεργασία του εγκεφαλικού σήματος. Κατά συνέπεια, ο χρόνος εκπαίδευσης των χρηστών έχει μειωθεί σημαντικά, γεγονός που έχει οδηγήσει σε πιο διαδεδομένες εφαρμογές συστημάτων BCI στην καθημερινή ζωή των ατόμων με αναπηρία, όπως ενδεικτικά η επεξεργασία κειμένου, τα προγράμματα περιήγησης, το ηλεκτρονικό ταχυδρομείο, ο έλεγχος αναπηρικών αμαξιδίων, ο απλός έλεγχος περιβάλλοντος χώρου ή τα νευροπροσθετικά μηχανήματα.

Παρά τις πρόσφατες σημαντικές προόδους στον τομέα των συστημάτων BCI, ορισμένα ζητήματα πρέπει ακόμη να επιλυθούν. Πρώτον, τα σχετικά πλεονεκτήμα-

τα και μειονεκτήματα των διαφόρων μεθόδων λήψης σήματος είναι ακόμη ασαφή. Η αποσαφήνισή τους θα απαιτήσει περαιτέρω μελέτες σε ανθρώπους και ζώα. Δεύτερον, οι επεμβατικές μέθοδοι χρειάζονται περαιτέρω διερεύνηση για την αντιμετώπιση της βλάβης των ιστών, του κινδύνου μόλυνσης και των προβλημάτων μακροπρόθεσμης σταθερότητας. Έχουν ήδη προταθεί ηλεκτρόδια που περιέχουν νευροτροπικά μέσα που προάγουν τη νευρωνική ανάπτυξη και την ασύρματη μετάδοση των καταγεγραμμένων νευρωνικών σημάτων. Τρίτον, θα πρέπει να προσδιοριστούν και να χαρακτηριστούν καλύτερα τα ηλεκτροφυσιολογικά και μεταβολικά σήματα που είναι καλύτερα σε θέση να κωδικοποιήσουν την πρόθεση του χρήστη.

Οι περισσότερες εφαρμογές συστημάτων BCI βρίσκονται ακόμη σε ερευνητικό στάδιο και δεν είναι έτοιμες να εισαχθούν σε ευρεία κλίμακα, για συνεχή χρήση στην καθημερινή ζωή των ανθρώπων. Εκτός από τους χαμηλούς ρυθμούς μεταφοράς πληροφοριών και τη μεταβλητή αξιοπιστία τους, τα περισσότερα τρέχοντα συστήματα BCI είναι άβολα, επειδή τα ηλεκτρόδια πρέπει να υγραίνονται (ενδεικτικά, με τη συχνή εφαρμογή ειδικής γέλης), το λογισμικό μπορεί να απαιτεί ειδικούς χειρισμούς και οι επαφές των ηλεκτροδίων δύνανται να χρειάζονται συνεχή προσαρμογή και διόρθωση της τοποθέτησής τους.

Τέλος, υπάρχουν πολλά αντίμετρα που προτείνονται για την αντιμετώπιση των κινδύνων, απαιτείται ωστόσο αρκετή έρευνα ακόμη, ιδίως λόγω της σοβαρότητας των κινδύνων που εγκυμονούνται από τη χρήση των συστημάτων αυτών. Καθώς οι δυνατότητες των συστημάτων BCI θα αυξάνονται και θα προωθείται και η διαλειτουργία τους, αντίστοιχα θα αυξάνονται και οι πιθανοί κίνδυνοι.

ABSTRACT

Security Issues in Brain – Computer Interfaces (BCI)

John Stathoulis[1], Vissarion Bakalis[2], Costas Vassilakis[3]
[1]Biomedical Engineer PhD, Nursing Department, University of Peloponnese
[2]Nursing Department, University of Thessaly
[3]Professor, Department of Informatics and Telecommunications, University of Peloponnese

Introduction: Brain-computer interface (BCI) systems emerged to harness and interpret the electrical activity of the brain for interaction with external devices. BCI, or Brain-Machine Interface (BMI), integrates hardware and software to facilitate human-environment interaction independent of peripheral nerves and muscles through control signals from electroencephalographic data. In the field of safety, BCI systems remain underdeveloped. The importance of safety in BCI systems has only recently attracted attention, leading to the emergence of terms such as neurosafety and neuroethics. The literature has identified categories of security threats that affect the integrity and confidentiality of BCI, but thorough research on these issues is still lacking.
Purpose: The purpose of this literature review is to describe the potential security attacks that affect each phase of the BCI system cycle. Also, to analyse the impact of these attacks as well as the possible countermeasures that can be used and how they are documented based on the international literature.
Material and Method: A narrative literature review based on articles from scientific databases (PubMed/Medline, Google Scholar) using specific keywords in Greek and English, in printed books and internet references was carried out.
Results: A critical review of the literature reveals that the security field focusing on BCI system technologies is not yet mature, creating opportunities for malicious actors to launch attacks. Even unsophisticated attacks can, however, have a significant impact on both BCI system technologies and user security. In addition, the development of standardisation initiatives to unify BCI systems in terms of information is recognised as an opportunity. Well-studied areas, such as implantable medical devices and the Internet of Things, can provide guidance for the development of robust security mechanisms, and user awareness of security issues in BCI systems is considered crucial.
Conclusions: Significant advances in BCI research have been made in the last two decades, leveraging established methodologies in signal processing and pattern recognition. Many studies have improved the accuracy of BCI and have proposed methods for efficient information transfer despite challenges in brain signal processing. Consequently, the training time for users has been reduced, facilitating wider application of BCI for people with disabilities,

including text processing and neuroprosthetics. Most BCI applications are still in the research phase and are not yet suitable for widespread everyday use. Current limitations include low information transfer rates, variable reliability, and inconvenience due to electrode maintenance and software handling requirements. There are many proposed countermeasures to mitigate the risks, but extensive research is still needed due to the significant threats associated with these systems.

Key-words: *Brain-Computer Interface, BCI systems, Cybersecurity, Privacy, Neurosecurity, Neuroconfidentiality.*
✉ **Corresponding Author:** Ioannis Stathoulis, Email: johnstathoulis@yahoo.gr, johnstathoulis@hotmail.com

Βιβλιογραφία

1. Bernal SL, Celdrán AH, Pérez GM, Barros MT, Balasubramaniam S. Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges. ACM Comput Surv. 2021 Jan;54.
2. Khalid MB, Rao NI, Rizwan-i-Haque I, Munir S, Tahir F. Towards a brain computer interface using wavelet transform with averaged and time segmented adapted wavelets. In: 2009 2nd International Conference on Computer, Control and Communication, IC4 2009. 2009.
3. Tyler WJ, Sanguinetti JL, Fini M, Hool N. Non-invasive neural stimulation. In: Micro- and Nanotechnology Sensors, Systems, and Applications IX. SPIE; 2017. p. 101941L.
4. Denning T, Matsuoka Y, Kohno T. Neurosecurity: Security and privacy for neural devices. Neurosurg Focus. 2009;27.
5. Takabi H, Bhalotiya A, Alohaly M. Brain Computer Interface (BCI) Applications: Privacy Threats and Countermeasures. In Institute of Electrical and Electronics Engineers (IEEE); 2017. p. 102–11.
6. Li Q, Ding D, Conti M. Brain-Computer Interface applications: Security and privacy challenges. In: 2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015. Institute of Electrical and Electronics Engineers Inc.; 2015. p. 663–6.
7. Obaid A, Hanna ME, Wu YW, Kollo M, Racz R, Angle MR, et al. Massively parallel microwire arrays integrated with CMOS chips for neural recording. Sci Adv. 2020;6.
8. Bonaci T, Calo R, Chizeck H. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2788104. 2014. App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces.
9. Amara N, Zhiqui H, Ali A. Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. In: Proceedings - 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2017. Institute of Electrical and Electronics Engineers Inc.; 2017. p. 244–51.
10. Bentabet N, Berrached NE. Synchronous P300 based BCI to control home appliances. In: Proceedings of 2016 8th International Conference on Modelling, Identification and Control, ICMIC 2016. Institute of Electrical and Electronics Engineers Inc.; 2017. p. 835–8.
11. Natural Computing for Unsupervised Learning. Springer International Publishing; 2019.
12. Finlayson SG, Bowers JD, Ito J, Zittrain JL, Beam AL, Kohane IS. Adversarial attacks on medical machine learning. Science (1979). 2019 Mar;363:1287–9.
13. Landau O, Puzis R, Nissim N. Mind your mind: EEG-based brain-computer interfaces and their security in cyber space. ACM Comput Surv. 2020 Jan;53.
14. Martinovic I, Davies D, Frank M, Perito D, Ros T, Song D. On the feasibility of side-channel attacks with brain-computer interfaces. In 2012. p. 34.
15. Fukushima A, Yagi R, Kawai N, Honda M, Nishina E, Oohashi T. Frequencies of inaudible high-frequency sounds differentially affect brain activity: Positive and negative hypersonic effects. PLoS One. 2014 Apr;9.
16. Hartmann CJ, Fliegen S, Groiss SJ, Wojtecki L, Schnitzler A. An update on best practice of deep brain stimulation in Parkinson's disease. Ther Adv Neurol Disord. 2019;12:1756286419838096.
17. Parastarfeizabadi M, Kouzani AZ. Advances in closed-loop deep brain stimulation devices. Vol. 14, Journal of neuroengineering and rehabilitation. 2017. p. 79.
18. Camara C, Peris-Lopez P, Tapiador JE. Security and privacy issues in implantable medical devices: A comprehensive survey. Vol. 55, Journal of Biomedical Informatics. Academic Press Inc.; 2015. p. 272–89.
19. Ienca M. Neuroprivacy, neurosecurity and brain-hacking: Emerging issues in neural engineering. Bioethica Forum. 2015;
20. Marin E, Singelée D, Yang B, Volski V, Vandenbosch GAE, Nuttin B, et al. Securing wireless neurostimulators. In: CODASPY 2018 - Proceedings of the 8th ACM Conference on Data and Application Security and Privacy. Association for Computing Machinery; 2018. p. 287–98.
21. Lebedev MA, Nicolelis MAL. Brain-machine interfaces: From basic science to neuroprostheses and neurorehabilitation. Physiol Rev. 2017 Apr;97:767–837.
22. Vadlamani S, Eksioglu B, Medal H, Nandi A. Jamming attacks on wireless networks: A taxonomic survey. Vol. 172, International Journal of Production Economics. Elsevier; 2016. p. 76–94.
23. Bonaci T, Herron J, Matlack C, Chizeck HJ. Securing the exocortex: A twenty-first century cybernetics challenge. In: 2014 IEEE Conference on Norbert Wiener in the 21st Century: Driving Technology's Future, 21CW 2014 - Incorporating the Proceedings of the 2014 North American Fuzzy Information

Processing Society Conference, NAFIPS 2014, Conference Proceedings. Institute of Electrical and Electronics Engineers Inc.; 2014.
24. Bikson M, Brunoni AR, Charvet LE, Clark VP, Cohen LG, Deng Z De, et al. Rigor and reproducibility in research with transcranial electrical stimulation: An NIMH-sponsored workshop. Vol. 11, Brain Stimulation. Elsevier Inc.; 2018. p. 465–80.
25. Ienca M, Haselager P, Emanuel EJ. Brain leaks and consumer neurotechnology. Vol. 36, Nature Biotechnology. Nature Publishing Group; 2018. p. 805–10.
26. Camara C, Peris-Lopez P, Tapiador JE. Security and privacy issues in implantable medical devices: A comprehensive survey. Vol. 55, Journal of Biomedical Informatics. Academic Press Inc.; 2015. p. 272–89.
27. Jagielski M, Oprea A, Biggio B, Liu C, Nita-Rotaru C, Li B. Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning. In: Proceedings - IEEE Symposium on Security and Privacy. Institute of Electrical and Electronics Engineers Inc.; 2018. p. 19–35.
28. Frank M, Hwu T, Jain S, Knight RT, Martinovic I, Mittal P, et al. Using EEG-based BCI devices to subliminally probe for private information. In: WPES 2017 - Proceedings of the 2017 Workshop on Privacy in the Electronic Society, co-located with CCS 2017. Association for Computing Machinery, Inc; 2017. p. 133–6.
29. https://www.bitbrain.com/blog/cybersecurity-brain-computer-interface [Internet]. Cybersecurity and brain-computer interfaces | Bitbrain.
30. Gupta S, Singhal A, Kapoor A. A literature survey on social engineering attacks: Phishing attack. In: Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016. Institute of Electrical and Electronics Engineers Inc.; 2017. p. 537–40.
31. Saito T, Yokoyama M, Sugawara S, Suzaki K. Safe Trans Loader: Mitigation and Prevention of Memory Corruption Attacks for Released Binaries. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag; 2018. p. 68–83.