Ανακοίνωση Τύπου
προς δημοσίευση

Πανεπιστήμιο Κύπρου
ΚΟΙΟΣ Research and Innovation Center of Excellence

Γραφείο Επικοινωνίας και Δημοσίων Σχέσεων
Τομέας Προώθησης και Προβολής

Τηλέφωνο: **22894304**
Ηλ. Διεύθυνση: **prinfo@ucy.ac.cy**
Ιστοσελίδα: **www.ucy.ac.cy/pr**

10 Δεκεμβρίου 2024

GuardAI: Νέο έργο για την ενίσχυση της ευρωστίας, ανθεκτικότητας και ασφάλειας των Συστημάτων Τεχνητής Νοημοσύνης

Ξεκίνησε επίσημα το ευρωπαϊκό ερευνητικό έργο **GuardAI** (Enhancing Robustness and Security of Edge AI Systems for Safety-Critical Applications), με χρηματοδότηση από το Πρόγραμμα Ορίζοντας Ευρώπη και συντονιστή το Κέντρο Αριστείας για Έρευνα και Καινοτομία «Κοίος» του Πανεπιστημίου Κύπρου.

Το έργο στοχεύει στην ενίσχυση της ευρωστίας, ανθεκτικότητας και ασφάλειας συστημάτων τεχνητής νοημοσύνης στα οποία η επεξεργασία δεδομένων γίνεται τοπικά (edge AI systems). Παραδείγματα τέτοιων συστημάτων αποτελούν τα μη επανδρωμένα αεροσκάφη, τα αυτόνομα συνδεδεμένα οχήματα και οι τοπικοί κόμβοι δικτύου τηλεπικοινωνιών. Αυτά τα συστήματα λαμβάνουν αποφάσεις σε πραγματικό χρόνο με τη χρήση τεχνητής νοημοσύνης, επηρεάζοντας το περιβάλλον τους, οπότε είναι αναγκαία η προστασία των τρωτών τους σημείων που σχετίζονται με παραποίηση δεδομένων, απειλές ασφάλειας και κακόβουλες επιθέσεις.

Αυτό θα επιτευχθεί με την ανάπτυξη καινοτόμων αλγορίθμων και τεχνολογιών για να διασφαλιστεί η ακεραιότητα, η ασφάλεια και ανθεκτικότητα αυτών των συστημάτων. Μέσω της ενσωμάτωσης δεικτών σε αλγόριθμους τεχνητής νοημοσύνης, τα συστήματα θα μπορούν να προσαρμόζονται και να λαμβάνουν αποφάσεις σε δυναμικά περιβάλλοντα. Επιπρόσθετα, μέσω της συνεργασίας ερευνητών, ειδικών σε θέματα τεχνητής νοημοσύνης, κυβερνητικών φορέων και της βιομηχανίας, θα τεθούν οι βάσεις για περεταίρω προώθηση μεθόδων αξιόπιστης και ασφαλούς τεχνητής νοημοσύνης σε διάφορα πεδία/τομείς, καθώς και πιστοποίηση της ασφάλειας τέτοιων συστημάτων. Το έργο GuardAI θα αναπτύξει πρωτοποριακές, τεχνολογικές λύσεις προσαρμοσμένες στις ανάγκες των συστημάτων τεχνητής νοημοσύνης, προστατεύοντας κρίσιμες υποδομές και άλλα συστήματα.

Στο έργο συμμετέχουν 10 εταίροι από την Ευρώπη (Κύπρος, Ελλάδα, Ιταλία, Αυστρία) και το Ηνωμένο Βασίλειο, με εμπειρία και γνώση σε θέματα τεχνητής νοημοσύνης.

Η ερευνητική ομάδα του Κέντρου Αριστείας «Κοίος», αποτελούμενη από τον Αναπληρωτή Καθηγητή, Θεοχάρη Θεοχαρίδη, τον Ερευνητή Λέκτορα, Δρ. Χρίστο Κύρκου και τον Ερευνητικό Συνεργάτη, Δρ. Αντώνη Σάββα, θα αναπτύξει αλγόριθμους με στόχο την ενίσχυση της ανθεκτικότητας μοντέλων μηχανικής μάθησης. Επιπρόσθετα, θα ηγηθεί των δραστηριοτήτων

για δοκιμές των αλγορίθμων σε εφαρμογές επιτήρησης και παρακολούθησης με χρήση μη επανδρωμένων αεροσκαφών.

Σύμφωνα με το Συντονιστή του έργου, εκ μέρους του Κέντρου Αριστείας «Κοίος», Αναπλ. Καθηγητή Θεοχάρη Θεοχαρίδη, **«**Τ*ο έργο GuardAI ευθυγραμμίζεται με τους στόχους που θέτει ο Ευρωπαϊκός Κανονισμός για την Τεχνητή Νοημοσύνη (EU AI Act), το πρώτο νομικό πλαίσιο για την τεχνητή νοημοσύνη, που υποστηρίζει την ανάπτυξη αξιόπιστης τεχνητής νοημοσύνης. Με την ανάπτυξη καινοτόμων μηχανισμών προστασίας για την τεχνητή νοημοσύνη, το έργο θα ενισχύσει την ανθεκτικότητα έναντι ψηφιακών επιθέσεων και παραποίησης δεδομένων σε συστήματα τεχνητής νοημοσύνης με δυνατότητα τοπικής και αυτόνομης επεξεργασίας δεδομένων»*.

Η εναρκτήρια συνάντηση του έργου πραγματοποιήθηκε στις 10 Οκτωβρίου 2024 στο Πανεπιστήμιο Κύπρου, με την παρουσία όλων των εταίρων.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101168067.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Τέλος ανακοίνωσης