

Θέμα: Ανίχνευση επιθέσεων σε IoT περιβάλλοντα με τη χρήση τεχνικών anomaly detection	
Επιβλέπων: Γεώργιος Σπαθούλας	Στοιχεία επικοινωνίας: gspathoulas@uth.gr
Σκοπός και στόχοι <p>Η παρούσα πτυχιακή εργασία αποσκοπεί στη μελέτη, ανάπτυξη και αξιολόγηση τεχνικών ανίχνευσης επιθέσεων (Intrusion Detection) σε περιβάλλοντα Internet of Things (IoT), με βάση μεθόδους ανίχνευσης ανωμαλιών (anomaly detection). Στόχος είναι η διερεύνηση αλγορίθμων που μπορούν να αναγνωρίζουν ασυνήθιστες ή ύποπτες συμπεριφορές δικτυακής ή συσκευαστικής δραστηριότητας, συμβάλλοντας στην έγκαιρη αναγνώριση επιθέσεων και στη βελτίωση της ασφάλειας των IoT συστημάτων.</p>	
Αντικείμενο <p>Τα περιβάλλοντα IoT αποτελούνται από πολυάριθμες και ετερογενείς συσκευές που επικοινωνούν συνεχώς και λειτουργούν σε κατανεμημένα δίκτυα. Η περιορισμένη υπολογιστική ισχύς και οι συχνά ανεπαρκείς μηχανισμοί ασφαλείας καθιστούν τα συστήματα IoT ευάλωτα σε ποικίλες επιθέσεις, όπως DoS/DDoS, spoofing, malware injection ή data exfiltration. Η ανίχνευση επιθέσεων με βάση τεχνικές anomaly detection στοχεύει στον εντοπισμό μη φυσιολογικών προτύπων δικτυακής ροής, συσκευαστικής δραστηριότητας ή κατανάλωσης πόρων. Η εργασία θα εξετάσει και θα συγκρίνει μεθόδους όπως:</p> <ul style="list-style-type: none">• Statistical anomaly detection,• Machine Learning-based• Deep Learning-based <p>για την ανάλυση δεδομένων από πραγματικά ή προσομοιωμένα IoT datasets</p>	
Η εργασία περιλαμβάνει <ul style="list-style-type: none">• Ανάλυση των προκλήσεων ασφαλείας και των τύπων επιθέσεων στο IoT.• Επισκόπηση των μεθόδων anomaly detection και των εφαρμογών τους στην κυβερνοασφάλεια.• Επιλογή ή συλλογή κατάλληλου IoT dataset.• Προεπεξεργασία δεδομένων και εξαγωγή χαρακτηριστικών (feature engineering).• Εφαρμογή και σύγκριση αλγορίθμων anomaly detection για ανίχνευση επιθέσεων.• Αξιολόγηση της απόδοσης των μοντέλων	
Σχετιζόμενα μαθήματα <ul style="list-style-type: none">• Ασφάλεια συστημάτων υπολογιστών• Κρυπτογραφία• Τεχνητή νοημοσύνη	

Προτεινόμενη μεθοδολογία έρευνας

<p>Η εργασία θα βασιστεί στη Design Science Research Methodology (DSRM) και θα περιλαμβάνει:</p> <ul style="list-style-type: none">• Βιβλιογραφική ανασκόπηση για τις τεχνικές anomaly detection και τις εφαρμογές τους στο IoT security.• Ανάλυση απαιτήσεων και επιλογή κατάλληλων αλγορίθμων και δεδομένων.• Σχεδιασμό και υλοποίηση πειραματικού πλαισίου για ανίχνευση ανωμαλιών σε IoT περιβάλλον.• Πειραματική αξιολόγηση της ακρίβειας και της αποδοτικότητας των μοντέλων.• Εξαγωγή συμπερασμάτων και προτάσεις για βελτιστοποίηση ή ανάπτυξη ελαφριών (lightweight) λύσεων κατάλληλων για edge συσκευές.

Προσδοκώμενα αποτελέσματα

<ul style="list-style-type: none">• Κατανόηση των βασικών απειλών και αναγκών ασφαλείας στα IoT συστήματα.• Σύγκριση και αξιολόγηση διαφορετικών τεχνικών anomaly detection για την ανίχνευση επιθέσεων.• Ανάπτυξη πειραματικού πλαισίου ή πρωτοτύπου συστήματος IDS για IoT.• Συμβολή στη βελτίωση της ασφάλειας και αξιοπιστίας των IoT περιβαλλόντων.

Ενδεικτικές πηγές

<ul style="list-style-type: none">• S. Moustafa et al., "BoT-IoT: A Realistic Dataset for Evaluating IoT Network Intrusion Detection Systems," IEEE Access, 2023.• T. Ferrag et al., "Deep Learning for Cybersecurity in IoT: Recent Advances and Future Trends," IEEE Internet of Things Journal, 2024.• M. Thamilarasu, S. Chawla, "Anomaly Detection Models for IoT Security: A Review," Computer Communications, 2023.
