 **ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**

**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**

**ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΙΑΤΡΙΚΗ**

**ΣΧΕΔΙΑΣΗ ΣΥΣΤΗΜΑΤΟΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΦΥΣΙΚΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ IoT ΣΥΣΚΕΥΩΝ**

**ΕΛΕΝΗ ΣΟΥΛΙΔΟΥ**

**ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ**

**Υπεύθυνος**

**Αθανάσιος Κακαρούντας**

**Αναπληρωτής Καθηγητής**

**Λαμία, 2024**

****

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**

**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ**

**ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΙΑΤΡΙΚΗ**

**ΣΧΕΔΙΑΣΗ ΣΥΣΤΗΜΑΤΟΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΦΥΣΙΚΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ IoT ΣΥΣΚΕΥΩΝ**

**ΕΛΕΝΗ ΣΟΥΛΙΔΟΥ**

**ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ**

**Επιβλέπων**

**Αθανάσιος Κακαρούντας**

**Αναπληρωτής Καθηγητής**

**Λαμία, 2024**

|  |
| --- |
| Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις (1), που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι: |
| *1.    Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί* ***χωρίς να τα περικλείω σε εισαγωγικά*** *και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*  *2.    Δέχομαι ότι η αυτολεξεί* ***παράθεση χωρίς εισαγωγικά****, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*  *3.    Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια*  *4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.* |

Ημερομηνία: ……/..…/20……

Ο – Η Δηλ.

(Υπογραφή)

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.

**Σχεδίαση Συστήματος Παρακολούθησης Φυσικών Χαρακτηριστικών για την Ασφάλεια IoT Συσκευών**

**Ελένη Σουλίδου**

**Τριμελής Επιτροπή:**

Αθανάσιος Κακαρούντας, Αναπληρωτής Καθηγητής (επιβλέπων/σα)

Ονοματεπώνυμο, Βαθμίδα……

Ονοματεπώνυμο, Βαθμίδα…….

**Περίληψη**

**Abstract**

Περιεχόμενα

[Κεφάλαιο 1. Εισαγωγή 11](#_Toc166790403)

[1.1. Βιβλιογραφική ανασκόπηση 12](#_Toc166790404)

[1.2. Διάρθρωση Πτυχιακής 13](#_Toc166790405)

[Κεφάλαιο 2. Διαδίκτυο των Πραγμάτων 15](#_Toc166790406)

[2.1. Ορισμός 15](#_Toc166790407)

[2.1.1. Χαρακτηριστικά του Διαδικτύου των Πραγμάτων 15](#_Toc166790408)

[2.1.2. Μερίδιο της Αγοράς 16](#_Toc166790409)

[2.1.3. Σύγχρονες Εφαρμογές του Διαδικτύου των Πραγμάτων 17](#_Toc166790410)

[2.2. Τεχνολογίες και Συστήματα 18](#_Toc166790411)

[2.2.1. Συστήματα υλικού 18](#_Toc166790412)

[2.2.2. Συνδεσιμότητα 18](#_Toc166790413)

[2.2.3. Διαστρωμάτωση Διαδικτύου των Πραγμάτων 18](#_Toc166790414)

[Κεφάλαιο 3. Ασφάλεια Συσκευών στο Διαδίκτυο των Πραγμάτων 20](#_Toc166790415)

[3.1. Ζητήματα ασφαλείας 20](#_Toc166790416)

[3.2. Επιθέσεις 20](#_Toc166790417)

[3.3. Προδιαγραφές ασφαλείας 20](#_Toc166790418)

[3.4. Συστήματα ανίχνευσης 20](#_Toc166790419)

[Κεφάλαιο 4. Σχεδίαση, Υλοποίηση και Αξιολόγηση Συστήματος 21](#_Toc166790420)

[4.1. Αρχιτεκτονική συστήματος 21](#_Toc166790421)

[4.2. Χαρακτηριστικά συστήματος 21](#_Toc166790422)

[4.2.1. Raspberry Pi Zero W 21](#_Toc166790423)

[4.2.2. Arduino UNO R3 22](#_Toc166790424)

[4.2.3. MCP9808 22](#_Toc166790425)

[4.3. Υλοποίηση συστήματος 22](#_Toc166790426)

[4.3.1. Παρουσίαση συστήματος 22](#_Toc166790427)

[4.3.2. Κώδικας υλοποίησης 23](#_Toc166790428)

[4.4. Μετρήσεις και πειραματική αξιολόγηση 24](#_Toc166790429)

[Κεφάλαιο 5. Συμπεράσματα και Μελλοντικές Επεκτάσεις 25](#_Toc166790430)

[Παραρτήματα 26](#_Toc166790431)

[Παράρτημα Α: Κώδικες Arduino 26](#_Toc166790432)

[Ι. Κώδικας αισθητήρα θερμοκρασίας MCP9808 26](#_Toc166790433)

[Παράρτημα B: Σενάρια κελύφους Raspberry Pi 26](#_Toc166790434)

[Ι. Κώδικας καταγραφής θερμοκρασίας συστήματος 26](#_Toc166790435)

[Παράρτημα Γ: Κώδικες Matlab 27](#_Toc166790436)

[Ι. Κώδικας μονών γραφημάτων τιμών θερμοκρασίας 27](#_Toc166790437)

[ΙΙ. Κώδικας πολλαπλών γραφημάτων τιμών θερμοκρασίας 27](#_Toc166790438)

# Κεφάλαιο 1. Εισαγωγή

Η ευρεία ενσωμάτωση των τεχνολογιών έξυπνων συσκευών και του Διαδικτύου των Πραγμάτων (Internet of Things – IoT) έχει επιφέρει πολλά θετικά αποτελέσματα, τόσο στον βιομηχανικό όσο και στον καταναλωτικό κόσμο. Ήδη ο αριθμός των έξυπνων συσκευών που έχουν πρόσβαση στο διαδίκτυο εκτιμάται στην τάξη του δισεκατομμυρίου, και αναμένεται να αυξηθεί στο μέλλον. Από αυτά γεννάται το εξής ερώτημα, «*Πόσο ασφαλείς είναι οι έξυπνες συσκευές όταν έχουν πρόσβαση στο διαδίκτυο;*». Συσκευές όπως έξυπνες οικιακές συσκευές (Smart TVs, Smart Appliances, Smart Alarm κ.α.), φορητές συσκευές (wearables) καθώς και βιομηχανικά συστήματα ελέγχου σχεδιάζονται με κύριο στόχο το χαμηλό κόστος και την ευκολία χρήσης, θυσιάζοντας αρκετά χαρακτηριστικά ασφαλείας. Ως εκ τούτου, ο συνδυασμός της περιορισμένης ισχύος, η έλλειψη προδιαγραφών ασφαλείας και η έκθεση σε διαδικτυακούς κινδύνους, καθιστά τις συσκευές IoT ιδανικούς στόχους προς επίθεση [1].

Σκοπός των συσκευών IoT αποτελεί η παροχή υπηρεσιών, είτε αυτή αφορά την ασφάλεια, την διευκόλυνση ή την ψυχαγωγία. Όμως, η φύση τους αυτή τις κάνει ευάλωτες σε επιθέσεις που στοχεύουν στην διατάραξη της παροχής υπηρεσιών. Σε αυτές περιλαμβάνονται οι επιθέσεις DoS (Denial of Service) και DDoS (Distributed DoS), οι οποίες αποτελούν και τις πιο συχνές. Πράγματι, ένα από τα σημαντικότερα χαρακτηριστικά των έξυπνων συσκευών είναι η ικανότητα τους να αυτοματοποιούν εργασίες, βελτιστοποιώντας τις για την αύξηση της αποδοτικότητας, να συλλέγουν δεδομένα και να τα διακινούν μέσω του δικτύου για την εξ αποστάσεως διαχείριση τους. Έτσι, η αποτυχία παροχής μιας υπηρεσίας μπορεί να προκαλέσει πληθώρα ζητημάτων για τις εφαρμογές που βασίζονται σε αυτήν, ειδικά στην περίπτωση κρίσιμων συστημάτων IoT πραγματικού χρόνου

Συνεπώς η έγκαιρη ανίχνευση επιθέσεων στα συστήματα IoT είναι μείζονος σημασίας. Συστήματα που είναι σχεδιασμένα για την ανίχνευση συγκεκριμένων ειδών επιθέσεων έχουν μεγάλη απήχηση, τόσο στην ερευνητική όσο και στην βιομηχανική κοινότητα. Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα συστήματα παρακολούθησης φυσικών χαρακτηριστικών, καθώς μπορούν να παρομοιαστούν με την παρακολούθηση ασθενών σε κλινικές. Θεωρώντας το κύκλωμα ως «ασθενή» παρακολουθούμε διάφορες παραμέτρους όπως η θερμοκρασία, η κατανάλωση ρεύματος και η τηλεπικοινωνιακή κίνηση.

Η παρούσα πτυχιακή εργασία, έχει ως αρχικό στόχο την μελέτη συστημάτων IoT, ευπαθειών και επιθέσεων που σχετίζονται με την διακοπή παροχής υπηρεσιών και συστημάτων παρακολούθησης φυσικών χαρακτηριστικών για την ανίχνευση επιθέσεων. Ως ειδικότερο σκοπό, η πτυχιακή έχει να προτείνει και να υλοποιήσει ένα πρότυπο σύστημα παρακολούθησης φυσικών χαρακτηριστικών με βάση την θερμοκρασία της κεντρικής μονάδας επεξεργασίας (CPU – Central Processing Unit) μιας έξυπνης συσκευής για την έγκαιρη ανίχνευση επιθέσεων DoS.

## Βιβλιογραφική ανασκόπηση

Η ασφάλεια των IoT συσκευών απασχολεί ιδιαίτερα την ερευνητική και επιστημονική κοινότητα. Στην πορεία θα αναφερθούμε σε μερικές ερευνητικές εργασίες που αφορούν τη θεματολογία αυτή.

Οι Berguiga et al. [2] δημιούργησαν έναν αλγόριθμο για την ανίχνευση επιθέσεων πλημμύρας με TCP SYN πακέτα. Στο συγκεκριμένο είδος επίθεσης, ο επιτιθέμενος στέλνει πολλαπλά πακέτα αίτησης TCP επιβραδύνοντας έτσι τη συσκευή ή ακόμα και την απόδοση του δικτύου. Πρότειναν λοιπόν, έναν νέο αλγόριθμο ως σύστημα ανίχνευσης εισβολών (Intrusion Detection System - IDS) ο οποίος δοκιμάστηκε με διαφορετικές πιθανότητες επιθέσεων ώστε να επιβεβαιωθεί η ορθή λειτουργία του.

Αντίστοιχα, οι Roopak et al. [3] πρότειναν ένα σύστημα ανίχνευσής εισβολών βασισμένο στο συνδυασμό βαθιάς μάθησης και της μεθόδου βελτιστοποίησης πολλαπλών στόχων για την ανίχνευση επιθέσεων DDoS σε δίκτυα IoT. Για την σχεδίαση του συστήματος έγινε χρήση συνελικτικού νευρωνικού δικτύου (Convolutional Neural Network – CNN) και της μεθόδου βελτιστοποίησης πολλαπλών στόχων Jumping Gene NSGA-II. Μέσω πειραματισμών οι ερευνητές απέδειξαν ότι το προτεινόμενο σύστημα παρουσίασε ακρίβεια 99.03%.

Επίσης, οι Shurman et al. [4] προτείνουν δύο διαφορετικούς τρόπους για την ανίχνευση κατανεμημένων επιθέσεων άρνησης υπηρεσιών με ανάκλαση (Distributed reflection Denial of Service – DrDoS). Ο πρώτος τρόπος χρησιμοποιεί μοντέλα βαθιάς μάθησης βασισμένα στα δίκτυα μακράς βραχύχρονης μνήμης ( Long Short-Term Memory – LSTM) εκπαιδευμένο στο σύνολο δεδομένων CICDDoS2019 ενώ ο δεύτερος χρησιμοποιεί υβριδικό σύστημα ανίχνευσης εισβολών. Στις DrDoS επιθέσεις οι επιτιθέμενοι στέλνουν πακέτα αιτήματος σε διακομιστές ανάκλασης και θέτουν την διεύθυνση IP του θύματος ως διεύθυνση παραλήπτη ώστε να εξουδετερωθεί από τα μεγάλα πακέτα απάντησης.

Οι Syed et al. [5] προτείνουν ένα framework ανίχνευσης επιθέσεων DoS σε επίπεδο εφαρμογής για το πρωτόκολλο επικοινωνίας MQTT, βασισμένο στην μηχανική μάθηση που αναπτύχθηκε για το συγκεκριμένο πρωτόκολλο. Συγκεκριμένα, χρησιμοποίησαν τρείς διαφορετικούς αλγορίθμους μηχανικής μάθησης, τον AODE ο οποίος είναι βασισμένος στον Naive Bayes, τον C4.5 βασισμένο στα Δένδρα Απόφασης ( Decision Trees) και τον MLP με βάση το Τεχνητό Νευρωνικό Δίκτυο (Artificial Neural Networks – ANN). Η εκπαίδευση έγινε με βάση δύο σύνολα δεδομένων, ένα με πακέτα κανονικής δικτυακής κίνησης και ένα με πακέτα κατά τη διάρκεια κάποιας επίθεσης. Συμπερασματικά, ο ταξινομητής AODE πέτυχε την υψηλότερη ακρίβεια ταξινόμησης στην ανίχνευση της κίνησης επίθεσης ενώ ο ταξινομητής MLP πέτυχε ακρίβεια ταξινόμησης 84% και στην πορεία επαναξιολογήθηκε με διάφορες παραμέτρους βελτιστοποίησης ώστε να αυξηθεί η απόδοση του στην ανίχνευση της κίνησης επιθέσεων.

Για το επίπεδο εφαρμογής αντίστοιχα, πρότειναν οι De La Tore Parra et al. [6] ένα framework κατανεμημένης βαθιάς μάθησης βασισμένο στο cloud για την ανίχνευση και τον περιορισμό επιθέσεων που πραγματοποιούνται από ομάδες συσκευών συνδεδεμένες στο διαδίκτυο (Botnet) και επιθέσεων Phishing. Η υλοποίηση τους περιλαμβάνει δύο συνεργατικούς μηχανισμούς ασφαλείας οι οποίοι βασίζονται στο κατανεμημένο συνελικτικό νευρωνικό δίκτυο (Distributed Convolutional Neural Network – DCNN) και στη μακρά βραχύχρονη μνήμη. Για την εκπαίδευση των μοντέλων δημιούργησαν ένα σύνολο δεδομένων διευθύνσεων URL, τόσο phishing όσο και μη phishing. Μέσω τον πειραμάτων έδειξαν ότι το μοντέλο DCNN μπορεί να ανιχνεύσει επιθέσεις phishing με ακρίβεια 94.3% και το μοντέλο LSTM μπορεί να ανιχνεύσει επιθέσεις Botnet με ακρίβεια 94.8%.

## Διάρθρωση Πτυχιακής

Ως δομή της πτυχιακής ορίζονται τα παρακάτω:

* Στο κεφάλαιο 1 εκτελέσαμε μια σύντομη εισαγωγή στη θεματολογία και στους στόχους της παρούσας εργασίας, καθώς και μια ανασκόπηση της σύγχρονης βιβλιογραφίας.
* Στο κεφάλαιο 2 αναλύουμε βασικές έννοιες του διαδικτύου των πραγμάτων, αναφερόμαστε στα εγγενή του χαρακτηριστικά και στην σημαντικότητα αφομοίωσης του από τη σύγχρονη βιομηχανία. Παράλληλα, παραθέτουμε οικονομικά στοιχεία, που υποστηρίζουν την στάση μας.
* Στο κεφάλαιο 3 επικεντρωνόμαστε στα ζητήματα και τις τεχνικές ασφαλείας των συσκευών και πρωτοκόλλων που χρησιμοποιούνται στα συστήματα IoT.
* Στο κεφάλαιο 4 παρουσιάζουμε ένα πρότυπο σύστημα παρακολούθησης φυσικών χαρακτηριστικών και ανίχνευσης ανωμαλιών με βάση αυτά, και αναφερόμαστε στις τεχνολογίες που χρησιμοποιήθηκαν για την υλοποίηση του. Μέσω του συστήματος εκτελείται πειραματική αξιολόγηση, ενώ ακολούθως γίνεται και σχολιασμός των ευρημάτων.
* Στο κεφάλαιο 5 παραθέτουμε τα συμπεράσματα που αντλήσαμε κατά την εκπόνηση της εν λόγω πτυχιακής εργασίας.

# Κεφάλαιο 2. Διαδίκτυο των Πραγμάτων

## Ορισμός

Σύμφωνα με την Ευρωπαϊκή Ένωση, ως Διαδίκτυο των Πραγμάτων ορίζεται μια καθολική υποδομή δικτύου, η οποία διασυνδέει φυσικά και εικονικά αντικείμενα εκμεταλλευόμενη την συλλογή δεδομένων και τις δυνατότητες επικοινωνίας. Με την σειρά της, η ITU ορίζει το Διαδίκτυο των Πραγμάτων ως μια καθολική υποδομή της κοινωνίας της πληροφορίας, η οποία επιτρέπει προηγμένες υπηρεσίες μέσω διασύνδεσης «Πραγμάτων». Η διασύνδεση φυσικών και ψηφιακών πραγμάτων βασίζεται στις αναπτυσσόμενες και διαλειτουργικές τεχνολογίες της πληροφορίας και των επικοινωνιών. Πρακτικά όμως, ως Διαδίκτυο των Πραγμάτων μπορούμε να αναφερόμαστε σε δίκτυα από αντικείμενα, καθένα εξοπλισμένο με ενσωματωμένους αισθητήρες, τα οποία συνδέονται με το Διαδίκτυο (ΙΕΕΕ).

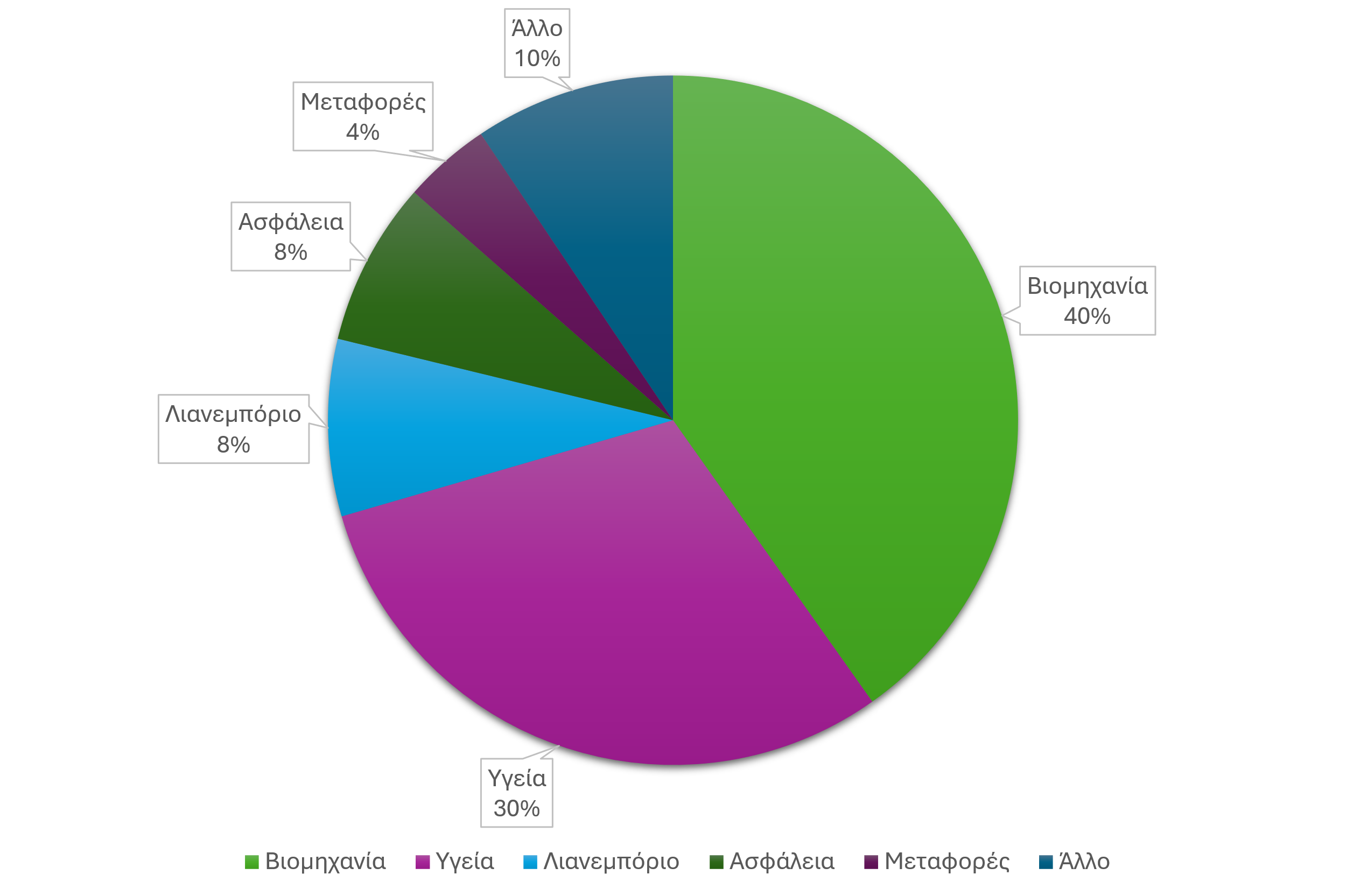
Από τη δεκαετία του 2000, η τεχνολογία οδεύει προς την εποχή του πανταχού παρόντος υπολογισμού (Ubiquitous Computing), όπου οι χρήστες του Διαδικτύου θα απαριθμούνται σε δισεκατομμύρια και θα αποτελούν την μειονότητα ως απλά πηγές και αποδέκτες πληροφορίας. Το μεγαλύτερο μέρος της κίνησης του Διαδικτύου ήδη οφείλεται σε συσκευές και «Πράγματα», τα οποία ανταλλάσσουν συνεχόμενα πληροφορία.

### Χαρακτηριστικά του Διαδικτύου των Πραγμάτων

Το Διαδίκτυο των Πραγμάτων μπορεί να χαρακτηριστεί από τέσσερεις βασικές ιδιότητες. Πρώτη ιδιότητα αποτελεί η αποδοτική και ικανή προς κλιμάκωση αρχιτεκτονική του συστήματος. Τα συστήματα του ΔτΠ οφείλουν να είναι αποδοτικά ως προς την κατανάλωση ενέργειας, αλλά και ως προς την παρεχόμενη υπηρεσία, ενώ πρέπει να έχουν και τη δυνατότητα να επεκταθούν κατ’ απαίτηση. Δεύτερη ιδιότητα των συστημάτων του ΔτΠ αποτελεί η μη διφορούμενη ονοματοδοσία και διευθυνσιοδότηση των συσκευών του. Κάθε συσκευή που συμμετέχει σε ένα δίκτυο πρέπει να αποκτά μοναδική διεύθυνση και να είναι προσβάσιμη από κάθε άλλο κόμβο του. Το τρίτο χαρακτηριστικό που εμφανίζουν τα συστήματα αυτά είναι η αφθονία από αδρανείς κόμβους, κινητές συσκευές και συσκευές που δεν υλοποιούν το πρωτόκολλο IP. Ως εκ τούτου, τα συστήματα αυτά οφείλουν να μεριμνούν για κάθε είδος κόμβου που βρίσκεται σε αυτά και να εξασφαλίζει την διαλειτουργικότητα και την επικοινωνία. Τέλος, το τέταρτο χαρακτηριστικό είναι η διακοπτόμενη συνδεσιμότητα. Όλα τα παραπάνω χαρακτηριστικά καθιστούν δυνατή την συνύπαρξη πολλαπλών ετερογενών συσκευών σε ένα δίκτυο.

### Μερίδιο της Αγοράς

Ο όρος «Διαδίκτυο των Πραγμάτων» σημαίνει πολλά, τόσο για τον ερευνητικό τομέα όσο και για τη σύγχρονη αγορά. Η δυνατότητα εφαρμογής των συστημάτων του Διαδικτύου των Πραγμάτων σε πληθώρα τομέων έχει επιτρέψει τη δημιουργία ενός νέου τοπίου ανταγωνιστικότητας.



Εικόνα 1: Κατανομή των τομέων εφαρμογής του Διαδικτύου των Πραγμάτων.

Κυριότερος τομέας εφαρμογής αποτελεί η βιομηχανία, καταλαμβάνοντας το 40.2% της αγοράς. Όροι όπως το βιομηχανικό διαδίκτυο των πραγμάτων και τα κυβερνοφυσικά συστήματα γίνονται όλο και πιο διαδεδομένοι, ενώ αυξάνονται και οι επενδύσεις των βιομηχανιών σε σύγχρονες τεχνολογίες (π.χ. αυτοκινητοβιομηχανία). Δεύτερος κυριότερος τομέας μετά τη βιομηχανία αποτελεί ο τομέας της υγείας, καταλαμβάνοντας το 30.3%. Ιδιαίτερο ενδιαφέρον παρουσιάζεται στον τομέα της έξυπνης υγείας, με κυριότερη εφαρμογή την παρακολούθηση βιομετρικών χαρακτηριστικών των ασθενών.

Τελευταίοι, αλλά όχι λιγότερο σημαντικοί είναι οι τομείς του λιανεμπορίου και της ασφάλειας με 8.3% και 7.7% της αγοράς αντίστοιχα. Συστήματα έξυπνου ανεφοδιασμού καταστημάτων, συστήματα καταγραφής προϊόντων και προηγμένα συστήματα πληρωμής μπορούν να ενισχύσουν την ανταγωνιστικότητα μιας επιχείρησης. Αντίστοιχα, τα έξυπνα συστήματα παρακολούθησης μέσω της χρήσης αισθητήρων δημιουργούν μια τελείως ξεχωριστή αγορά, αποτελώντας πολλές φορές κομμάτι αυτού που αναφέρεται ως έξυπνο σπίτι. Συγκεκριμένα, μεγάλη ανάπτυξη φαίνεται στον τομέα των έξυπνων καμερών με σύνδεση στο διαδίκτυο (IP Cameras), για την συνεχή παρακολούθηση, τόσο δημόσιων όσο και ιδιωτικών χώρων.

### Σύγχρονες Εφαρμογές του Διαδικτύου των Πραγμάτων

Οι εφαρμογή των ιδεών του Διαδικτύου των Πραγμάτων ξεκίνησε με απλές εφαρμογές, όπου πρώτος στόχος ήταν η διασύνδεση συσκευών. Τα μηχανήματα αυτόματων συναλλαγών (ΑΤΜ) διασυνδέθηκαν για πρώτη φορά στο 1974, ενώ το 1991 ο παγκόσμιος ιστός επίφερε καινοτόμες μεθόδους υπολογισμού και επικοινωνίας. Πλέον, οι εφαρμογές του Διαδικτύου των Πραγμάτων περιορίζονται μόνο από τη φαντασία των σχεδιαστών. Συστήματα έξυπνης στάθμευσης και έξυπνων δρόμων υποστηρίζουν τον χώρο των έξυπνων οχημάτων για την ανάπτυξη των συγκοινωνιών. Τα έξυπνα συστήματα ενέργειας επιτρέπουν την βέλτιστη διαχείριση του συστήματος διανομής ηλεκτρικής ενέργειας, την παρακολούθηση της κατάστασης απομακρυσμένων συστημάτων συλλογής ενέργειας όπως φωτοβολταϊκά και ανεμογεννήτριες. Τα συστήματα παρακολούθησης εφοδιαστικής αλυσίδας, ανεφοδιασμού συλών, διαχείρισης αποβλήτων, παρακολούθησης επιπέδων καυσίμου και ανίχνευσης υγρών/διαρροών αποτελούν σημαντικά μέρη σε πληθώρα τομέων όπως η βιομηχανία και η ναυτιλία.

Τα συστήματα του Διαδικτύου των πραγμάτων μπορούν να χρησιμοποιηθούν για την έγκαιρη ανίχνευση φυσικών καταστροφών και περιβαλλοντικών συνθηκών, όπως η ανίχνευση πυρκαγιών, η παρακολούθηση της μόλυνσης του αέρα, η παρακολούθηση των επιπέδων χιονιού, η πρόληψη κατολισθήσεων και χιονοστιβάδων, η ανίχνευση επιβλαβούς ακτινοβολίας και επικίνδυνων ή εύφλεκτων αερίων.

## Τεχνολογίες και Συστήματα

Η υλοποίηση ενός συστήματος που ανήκει στο Διαδίκτυο των πραγμάτων αποτελείται από συγκεκριμένες τεχνολογίες και υποσυστήματα. Οι τεχνολογίες που επιτρέπουν την υλοποίηση τέτοιων συστημάτων μπορούν να χωριστούν σε τέσσερεις βασικές ομάδες.

* Τεχνολογίες υλικού
* Τεχνολογίες τηλεπικοινωνιών και δικτύων
* Τεχνολογίες διαχείρισης μεγάλου όγκου δεδομένων
* Τεχνητή νοημοσύνη και μηχανική μάθηση

Από τις παραπάνω ομάδες τεχνολογιών, οι απαραίτητες τεχνολογίες που πρέπει να υπάρχουν σε ένα σύστημα Διαδικτύου των Πραγμάτων είναι αυτές που επιτρέπουν τον υπολογισμό και την επικοινωνία.

### Συστήματα υλικού

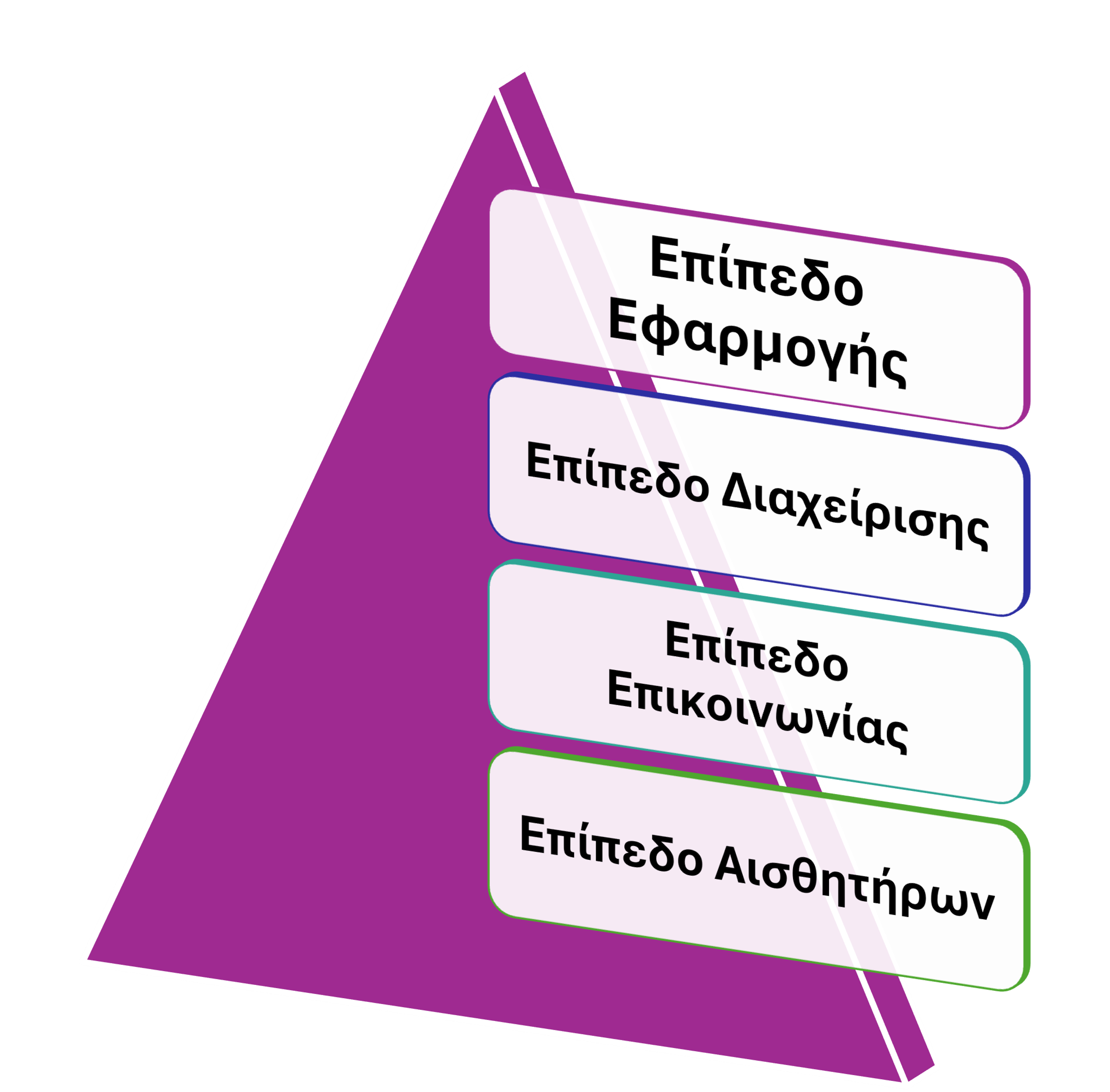
Τα συστήματα υλικού που απαιτούνται σε ένα σύστημα ΔτΠ αποτελούν τους τερματικούς κόμβους του δικτύου, τα gateways και τους κόμβους τοπικής επεξεργασίας. Οι τερματικοί κόμβοι μπορεί να αποτελούν αισθητήρες, ενεργοποιητές ή τηλεπικοινωνιακά στοιχεία όπως RFID Tags. Από την άλλη, τα gateways και οι κόμβοι τοπικής επεξεργασίας μπορεί να αποτελούν κάποιο ενδιάμεσο λογισμικό (middleware), κάποιον δέκτη σήματος ή γενικά πομποδέκτες.

### Συνδεσιμότητα

Η συνδεσιμότητα των συσκευών/πραγμάτων σε ένα σύστημα είναι από τα πιο σημαντικά μέρη του συστήματος. Η συνδεσιμότητα χωρίζεται σε δύο βασικές κατηγορίες, την τοπική συνδεσιμότητα και την καθολική συνδεσιμότητα. Η τοπική συνδεσιμότητα επιτυγχάνεται από τεχνολογίες όπως το ZigBee, το RFID, το Bluetooth (IEEE 802.15.1) και τα δίκτυα 5G/4G. Για την επίτευξη καθολικής συνδεσιμότητας απαιτούνται συστήματα gateway, για την σύνδεση του τοπικού δικτύου με το Διαδίκτυο.

### Διαστρωμάτωση Διαδικτύου των Πραγμάτων

Όπως κάθε σύνθετο σύστημα, έτσι και τα συστήματα ΙοΤ απαιτούν μια αυστηρά καθορισμένη διαστρωμάτωση των επιπέδων λειτουργίας τους, για την βέλτιστη ανάπτυξη και τον προγραμματισμό τους. Παρόμοια με τη διαστρωμάτωση δικτύων OSI, και η αρχιτεκτονική του ΙοΤ διακρίνεται επίσης σε στρώματα (βλ. Εικόνα 2).



Εικόνα 2: Διαστρωμάτωση Επιπέδων Διαδικτύου των Πραγμάτων.

Το επίπεδο εφαρμογής περιέχει τα πεδία εφαρμογών, τόσο σε βιομηχανικό όσο και σε καταναλωτικό τομέα. Το αμέσως επόμενο επίπεδο είναι το επίπεδο διαχείρισης, όπου εκτελείται η ανάλυση, η διαχείριση, η οπτικοποίηση και ο έλεγχος των δεδομένων. Επιπλέον, σε αυτό το επίπεδο υλοποιούνται και οι μηχανισμοί ασφαλείας και ιδιωτικότητας. Κάτω από το επίπεδο διαχείρισης βρίσκεται το επίπεδο επικοινωνίας. Στο επίπεδο αυτό τοποθετούνται συσκευές gateway, μικροελεγκτές, επεξεργαστές σήματος κ.α. Ακόμα, υλοποιούνται μηχανισμοί κρυπτογράφησης και αρχιτεκτονικές συστημάτων αισθητήρων. Τέλος, το επίπεδο αισθητήρων περιλαμβάνει όλες τις συσκευές που είναι υπεύθυνες για τη μέτρηση, συλλογή και επεξεργασία των φυσικών χαρακτηριστικών σε πραγματικό χρόνο.

# Κεφάλαιο 3. Ασφάλεια Συσκευών στο Διαδίκτυο των Πραγμάτων

Με την συνεχή εξέλιξη της τεχνολογίας και συγκεκριμένα των συσκευών IoT, οι δυνατότητες σύνδεσης και λειτουργίας, τόσο των ίδιων των συσκευών όσο και εφαρμογών έχουν επεκταθεί, προκαλώντας σημαντικά ζητήματα όσον αφορά την ασφάλεια [1]. Επιπλέον, η ευρεία υιοθέτηση και η έντονη εμπορευματοποίηση των τεχνολογιών IoT καθιστούν τις συσκευές του ευάλωτες σε επιθέσεις [2].

Ένας από τους λόγους που τέτοιου είδους συσκευές είναι επιρρεπείς σε ευπάθειες είναι η έλλειψη τυποποίησης. Η εμπλοκή διάφορων προμηθευτών στην αγορά των διασυνδεδεμένων συσκευών έχει ως αποτέλεσμα κάθε μια να χρησιμοποιεί διαφορετικό λειτουργικό σύστημα ή πρωτόκολλο επικοινωνίας, με συνέπεια να καθίσταται δύσκολη η ανάπτυξη ενός κοινού συστήματος ασφαλείας.

## 3.1. Ζητήματα ασφαλείας

## 3.2. Επιθέσεις

## 3.3. Προδιαγραφές ασφαλείας

## 3.4. Συστήματα ανίχνευσης

# Κεφάλαιο 4. Σχεδίαση, Υλοποίηση και Αξιολόγηση Συστήματος

Στο παρόν κεφάλαιο θα αναλύσουμε συνοπτικά τα χαρακτηριστικά των συνιστωσών της υλοποίησης μας, τον τρόπο διασύνδεσης και λειτουργίας τους, καθώς και τον κώδικα που απαιτείται για τον προγραμματισμό τους. Αρχικά θα ξεκινήσουμε με μια σύντομη ανάλυση των επιμέρους στοιχείων της υλοποίησης. Στη συνέχεια, θα παρουσιαστεί η κατασκευή και η διασύνδεση των επιμέρους στοιχείων, ο κώδικας και οι μετρήσεις. Τέλος, θα γίνει και μια σύντομη βιβλιογραφική ανασκόπηση, ερευνητικών εργασιών με συναφή θεματολογία

## 4.1. Αρχιτεκτονική συστήματος

## 4.2. Χαρακτηριστικά συστήματος

Το παρόν κύκλωμα αποτελείται από έναν μικροϋπολογιστή Raspberry Pi Zero W, έναν μικροελεγκτή Arduino UNO και έναν αισθητήρα θερμοκρασίας MCP9808, τα οποία και θα αναλύσουμε.

### 4.2.1. Raspberry Pi Zero W

Ο μικροϋπολογιστής συνοδεύεται από έναν μονοπύρηνο επεξεργαστή BCM2835, αρχιτεκτονικής 32 bit, χρονισμένο στο 1GHz και από μνήμη RAM χωρητικότητας 512MB. Χρησιμοποιώντας την θύρα CSI που μας παρέχει ο μικρουπολογιστής, έχουμε συνδέσει μια κάμερα ανάλυσης 5MP ώστε να λειτουργεί σαν IP κάμερα για τις ανάγκες της υλοποίησης μας. Για την διασύνδεση της υλοποίησης με το υπόλοιπο δίκτυο, ο μικροϋπολογιστής διαθέτει διεπαφή πρωτοκόλλου IEEE 802.11b/g/n (WiFi) με συχνότητα λειτουργίας στα 2.4 GHz.

Η εκτέλεση των προγραμμάτων πάνω στο Raspberry Pi Zero W υποστηρίζεται από το λειτουργικό σύστημα Raspberry Pi OS Legacy Lite 32-bit. Η έκδοση Lite του λειτουργικού συστήματος αποτελεί μια μινιμαλιστική εικόνα λογισμικού, αποτελούμενη από 493 πακέτα, από την οποία λείπει ο διαχειριστής X-window. Λόγω αυτού, το σύστημα είναι ταχύτερο και πιο συμβατό με περιβάλλοντα εξυπηρετητών και Internet of Things. (paper me RPi).

### 4.2.2. Arduino UNO R3

Το σύστημα του Arduino βασίζεται στον μικροελεγκτή ATmega328P, ο οποίος λειτουργεί ως κύριος επεξεργαστής χρονισμένος στα 16MHz, ενώ χρησιμοποιεί και τον επεξεργαστή ATmega16U2 για τη μετατροπή των σημάτων USB από τον υπολογιστή σε σειριακά σήματα που μπορεί να κατανοήσει ο ATmega328P. Ουσιαστικά, λειτουργεί ως γέφυρα μεταξύ της θύρας USB του υπολογιστή και του μικροελεγκτή. Επίσης, περιέχει μνήμες SRAM χωρητικότητας 2KB, FLASH χωρητικότητας 32KB και EEPROM χωρητικότητας 1KB.

Ως κομμάτι της υλοποίησης, το σύστημα του Arduino πραγματώνει το σύστημα παρακολούθησης (monitor system) σε σύνδεση με τον αισθητήρα θερμοκρασίας MCP9808. Κύρια εργασία του Arduino είναι η συλλογή των δεδομένων από τον αισθητήρα. Οι μετρήσεις που λαμβάνονται από το Arduino, καταγράφονται από το πρόγραμμα RealTerm σε αρχεία κειμένου.

### 4.2.3. MCP9808

Είναι ένας ψηφιακός αισθητήρας θερμοκρασίας ο οποίος μετατρέπει θερμοκρασίες μεταξύ - 20℃ έως +100℃ σε μια ψηφιακή λέξη με ακρίβεια ±0,5℃. Επίσης διαθέτει τέσσερις διαφορετικές αναλύσεις μέτρησης (+0,5℃, +0,25℃, +0,125℃ και +0,0625℃). Ο MCP9808 είναι συμβατός με το πρωτόκολλο επικοινωνίας I2C, το οποίο χρησιμοποιεί μόνο δύο ακροδέκτες του μικροελεγκτή για την μεταφορά δεδομένων, πέραν των ακροδεκτών για το ρεύμα και την γείωση, τον Serial Data Line (SDA) ο οποίος είναι ο Α4 και τον Serial Clock Line (SCL) ο οποίος είναι ο Α5.

## 4.3. Υλοποίηση συστήματος

### 4.3.1. Παρουσίαση συστήματος

Το σύστημα της υλοποίησης, καθώς και η διασύνδεση των επιμέρους στοιχείων φαίνονται στην παρακάτω εικόνα.

Εικόνα που περιέχει κύκλωμα, ηλεκτρονικός μηχανικός, ηλεκτρονικό εξάρτημα, στοιχείο κυκλώματος

Περιγραφή που δημιουργήθηκε αυτόματα

Εικόνα 3: Απεικόνιση συστήματος παρακολούθησης θερμοκρασίας.

Το σύστημα κατασκευάζεται με βάση την λήψη μετρήσεων θερμοκρασίας από την ΚΜΕ του Raspberry Pi (1). Ο αισθητήρας θερμοκρασίας MCP9808 (2) έχει τοποθετηθεί πάνω από τον επεξεργαστή του Raspberry Pi με τη βοήθεια θερμοαγώγιμης πάστας, για την ανίχνευση των μεταβολών της θερμοκρασίας κατά την λειτουργία του. Με την σειρά του, ο αισθητήρας συνδέεται στους ακροδέκτες A4 και A5 του Arduino UNO R3 (4) για την μεταφορά των μετρήσεων στον μικροελεγκτή. Το Raspberry Pi συνδέεται με την κάμερα (3), λειτουργώντας ως IP Camera.

### 4.3.2. Κώδικας υλοποίησης

Η παραπάνω διασύνδεση (Εικόνα 3) υποστηρίζεται από τον μικροελεγκτή, πάνω στον οποίο γράφεται ο κώδικας ελέγχου του συστήματος. Συγκεκριμένα, ο κώδικας αφορά την λειτουργία του αισθητήρα θερμοκρασίας.

Η βιβλιοθήκη Wire.h αξιοποιείται για την επικοινωνία του μικροελεγκτή με συσκευές που χρησιμοποιούν το I2C πρωτόκολλο. Με την σειρά της, η βιβλιοθήκη Adafruit\_MCP9808.h περιέχει όλες τις συναρτήσεις που είναι απαραίτητες για να διαβάσουμε δεδομένα από τον αισθητήρα. Για την αναπαράσταση του αισθητήρα στον κώδικα δημιουργούμε ένα αντικείμενο κλάσης Adafruit\_MCP9808(), το οποίο και θα χρησιμοποιούμε από εδώ και στο εξής. Μέσα στη συνάρτηση setup() δηλώνουμε ότι θα χρησιμοποιήσουμε το Serial terminal με ρυθμό baud 9600 και περιμένουμε να ξεκινήσει η μετάδοση, ενημερώνοντας με κατάλληλο μήνυμα.

Επειδή ο αισθητήρας χρησιμοποιεί το I2C πρωτόκολλο, χρειάζεται να του υποδείξουμε σε ποια διεύθυνση θα συνδεθεί, διότι παρέχεται η δυνατότητα να συνδεθούν πολλοί αισθητήρες στον ίδιο δίαυλο I2C χρησιμοποιώντας διαφορετική διεύθυνση ο καθένας. Έτσι, οι διευθύνσεις που μπορούν να χρησιμοποιηθούν είναι από το 0x18 μέχρι το 0x1F, με την διεύθυνση 0x18 να είναι η προεπιλεγμένη. Έπειτα, θέτουμε την ανάλυση μέτρησης του αισθητήρα, η οποία μπορεί να είναι μια από τις εξής επιλογές:

|  |  |  |
| --- | --- | --- |
| **Λειτουργία** | **Ανάλυση** | **Περίοδος δειγματοληψίας** |
| 0 | 0.5℃ | 30 ms |
| 1 | 0.25℃ | 65 ms |
| 2 | 0.125℃ | 130 ms |
| 3 | 0.0625℃ | 250 ms |

Τέλος, στη συνάρτηση loop() διαβάζουμε τις μετρήσεις από τον αισθητήρα σε βαθμούς Κελσίου και τις εμφανίζουμε στο Serial terminal ανά 100 ms.

## 4.4. Μετρήσεις και πειραματική αξιολόγηση

# Κεφάλαιο 5. Συμπεράσματα και Μελλοντικές Επεκτάσεις

# Παραρτήματα

## Παράρτημα Α: Κώδικες Arduino

### Ι. Κώδικας αισθητήρα θερμοκρασίας MCP9808

#include <Wire.h>

#include "Adafruit\_MCP9808.h"

Adafruit\_MCP9808 tempsensor = Adafruit\_MCP9808();

void setup() {

  Serial.begin(9600);

  while (!Serial);

  Serial.println("MCP9808 temp sensor");

  if (!tempsensor.begin(0x18)) {

    Serial.println("Couldn't find MCP9808! Check your connections and verify the address is correct.");

    while (1);

  }

   Serial.println("Found MCP9808!");

  tempsensor.setResolution(0);

}

void loop() {

  float c = tempsensor.readTempC();

  Serial.print(c, 2);

  Serial.println("\t");

  delay(100);

}

## Παράρτημα B: Σενάρια κελύφους Raspberry Pi

### Ι. Κώδικας καταγραφής θερμοκρασίας συστήματος

import **os**

import **time**

def **measure\_temp**():

    temp = **os**.**popen**("vcgencmd measure\_temp").**readline**()

    return (temp.**replace**("temp=",""))

while True:

**print**(**measure\_temp**())

**time**.**sleep**(0.1)

## Παράρτημα Γ: Κώδικες Matlab

### Ι. Κώδικας μονών γραφημάτων τιμών θερμοκρασίας

clear all;

clc;

file1 = load(['../files/without attack/night\_with\_movement\_with\_script.txt']);

Ts = 0.1;

t1 = (0:length(file1)-1)\*Ts/60;

figure;

plot(t1,file1);

title('Night (with movement, with script)');

[min\_val,idx\_min] = min(file1);

[max\_val,idx\_max] = max(file1);

hold on;

yline(mean(file1), 'm', 'LineWidth',1.5);

plot(t1(idx\_max),file1(idx\_max),'\*r', 'LineWidth',2);

plot(t1(idx\_min),file1(idx\_min),'\*g','LineWidth',2);

hold off;

xlim([0 26]);

xlabel('time (seconds)');

ylabel('temperature (celcius)');

legend('Measurement', sprintf('Mean: %g°C', mean(file1)),sprintf('Max: %g°C, Time: %g sec',max\_val, t1(idx\_max)),sprintf('Min: %g°C, Time: %g', min\_val, t1(idx\_min)), 'Location','southeast');

### ΙΙ. Κώδικας πολλαπλών γραφημάτων τιμών θερμοκρασίας

clear all; clc;

meas = load('../files/without attack/without\_movement\_with\_script2.txt')';

Ts = 0.1; % sampling period

fs = 1/Ts; % sampling frequency

samples\_per\_25min = 15000;

sampling\_parts = ceil(length(meas)/samples\_per\_25min);

figure;

t = (0:length(meas)-1)\*Ts/60;

plot(t,meas);

title('Measurements');

xlabel('time (seconds)');

ylabel('temperature (celcius)');

grid on;

%

% break measurements per 25 minutes

x = ceil(sampling\_parts);

bins = x\*samples\_per\_25min-length(meas);

new\_meas = [meas zeros(1,bins)];

R2 = reshape(new\_meas,samples\_per\_25min,[]);

titles = {"Boot", "Idle", "Normal"};

for ii=1:3

figure;

if ii == sampling\_parts

y = R2(1:length(R2(:,ii))-bins, ii)';

else

y = R2(:,ii)';

end

t = (0:length(y)-1)\*Ts/60;

plot(t, y);

[min\_val,idx\_min] = min(y);

[max\_val,idx\_max] = max(y);

hold on;

yline(mean(y), 'm', 'LineWidth',1.5);

% text(0, mean(y), ['Mean: ' num2str(mean(y))]);

plot(t(idx\_max),y(idx\_max),'\*r', 'LineWidth',2);

plot(t(idx\_min),y(idx\_min),'\*g','LineWidth',2);

% text(t(idx\_min), min\_val, ['min: ' num2str(min\_val) 'time: ' num2str(t(idx\_min))]);

% text(t(idx\_max), max\_val, ['max: ' num2str(max\_val) 'time: ' num2str(t(idx\_max))]);

hold off;

title(titles(ii));

xlabel('time (seconds)');

ylabel('temperature (celcius)');

legend('Measurement', sprintf('Mean: %g°C', mean(y)),sprintf('Max: %g°C, Time: %g sec',max\_val, t(idx\_max)),sprintf('Min: %g°C, Time: %g', min\_val, t(idx\_min)), 'Location','southeast');

grid on;

end