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.

Ελένη Σουλίδου

(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)

Χαράλαμπος Καρανίκας, Επίκουρος Καθηγητής

Παναγιώτης Τσαρούχας, Καθηγητής

Ευχαριστίες

Με την ολοκλήρωση της παρούσας πτυχιακής εργασίας θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή, Αθανάσιο Κακαρούντα για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα.

Επιπλέον, θα ήθελα να ευχαριστήσω τον μεταδιδακτορικό ερευνητή του τμήματος, κύριο Μυριδάκη Δημήτριο, για την συνεχή υποστήριξη και καθοδήγηση καθ' όλη την διάρκεια εκπόνησης της παρούσας εργασίας.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου και τους κοντινούς μου ανθρώπους, για την υποστήριξη και την βοήθεια τους καθ' όλη την διάρκεια των σπουδών μου.

Περίληψη

Το Διαδίκτυο των Πραγμάτων βασίζεται στη σύνδεση συσκευών μέσω διαδικτύου, επιτρέποντας τη συλλογή και ανταλλαγή δεδομένων. Η συνεχής και ταχεία αύξηση των IoT συσκευών, από έξυπνες οικιακές συσκευές, όπως θερμοστάτες και ψυγεία, μέχρι βιομηχανικούς αισθητήρες και ιατρικές συσκευές, δημιουργεί νέες προκλήσεις ασφαλείας. Καθώς ο αριθμός των διασυνδεδεμένων συσκευών αυξάνεται, αυξάνεται και το έδαφος που κερδίζουν οι κακόβουλοι χρήστες. Οι επιθέσεις σε IoT συσκευές μπορεί να οδηγήσουν σε σοβαρές συνέπειες, όπως διακοπή υπηρεσιών, απώλεια δεδομένων και παραβίαση προσωπικών πληροφοριών. Η ανάγκη προστασίας των IoT συσκευών από επιθέσεις είναι επιτακτική. Στη παρούσα εργασία σχεδιάστηκε ένα σύστημα παρακολούθησης φυσικών χαρακτηριστικών για την έγκαιρη ανίχνευση επιθέσεων. Το προτεινόμενο σύστημα παρακολουθεί τις μεταβολές θερμοκρασίας της CPU μιας συσκευής IoT. Το ρόλο της IoT συσκευής πήρε ο μικροϋπολογιστής Raspberry Pi Zero W, ο οποίος λειτουργεί ως IP κάμερα, και με την βοήθεια ενός μικροελεγκτή Arduino UNO και ενός αισθητήρα θερμοκρασίας υψηλής ακρίβειας, πραγματοποιείται η λήψη των τιμών θερμοκρασίας. Τα ευρήματα της πειραματικής αξιολόγησης επιβεβαίωσαν την αποτελεσματικότητα της θερμοκρασίας ως μέτρο για την ανίχνευση επιθέσεων, με τον ρυθμό μεταβολής της θερμοκρασίας να παρέχει ουσιαστικές πληροφορίες σχετικά με την παρουσία επίθεσης. Συγκεκριμένα, στο πλαίσιο της λειτουργίας της κάμερας IP, διαπιστώθηκε ότι ο φωτισμός του περιβάλλοντος έχει ελάχιστη επίδραση στη θερμοκρασία, με την υψηλότερη φωτεινότητα να προκαλεί μικρή αύξηση της θερμοκρασίας σε σύγκριση με τις συνθήκες συσκότισης. Επιπλέον, η κίνηση εντός της ροής εικόνας της κάμερας δεν είχε ως αποτέλεσμα σημαντικές μεταβολές της θερμοκρασίας, γεγονός που επιβεβαιώθηκε από τις αντίστοιχες τιμές του ρυθμού μεταβολής. Παρόμοιες παρατηρήσεις έγιναν όσον αφορά τις μεταβολές της θερμοκρασίας λόγω της εκτέλεσης σεναρίου κελύφους στο παρασκήνιο της συσκευής. Η ύπαρξη επιθέσεων συσχετίστηκε με υψηλότερες τιμές ρυθμού μεταβολής της θερμοκρασίας.

Λέξεις κλειδιά: Arduino, Raspberry Pi, Διαδίκτυο των Πραγμάτων, Ανίχνευση επιθέσεων, Αισθητήρας θερμοκρασίας, Ασφάλεια, Φυσικά χαρακτηριστικά, Έξυπνη συσκευή

Abstract

The Internet of Things is based on connecting devices over the internet, enabling the collection and exchange of data. The continuous and rapid growth of IoT devices, from smart home appliances such as thermostats and refrigerators to industrial sensors and medical devices, creates new security challenges. As the number of interconnected devices increases, so does the ground gained by malicious users. Attacks on IoT devices can lead to serious consequences such as service disruption, data loss and breach of personal information. The need to protect IoT devices from attacks is imperative. In this paper, a physical feature monitoring system is designed for early detection of attacks. The proposed system monitors the temperature changes of the CPU of an IoT device. The role of the IoT device was taken by the Raspberry Pi Zero W microcomputer, which acts as an IP camera, and by using an Arduino UNO microcontroller and a high precision temperature sensor, the temperature values are obtained. The findings of the experimental evaluation confirmed the effectiveness of temperature as a measure for detecting attacks, with the rate of temperature change providing meaningful information about the presence of an attack. Specifically, in the context of IP camera operation, it was found that ambient lighting has minimal effect on temperature, with higher brightness causing a small increase in temperature compared to blackout conditions. Furthermore, movement within the camera image stream did not result in significant temperature changes, which was confirmed by the corresponding rate of change values. Similar observations were made regarding the temperature changes due to the execution of a shell scenario in the background of the device. The presence of attacks was associated with higher values of temperature rate of change.

Keywords: Arduino, Raspberry Pi, Internet of Things, Attack detection, Temperature sensor, Security, Physical characteristics, Smart device

Περιεχόμενα

Ευρετήριο Πινάκων

Ευρετήριο Εικόνων

Αρκτικόλεξο

ANN	Artificial Neural Networks
ARP	Address Resolution Protocol
CNN	Convolutional Neural Network
CPU	Central Processing Unit
CSI	Camera Serial Interface
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
DCNN	Distributed Convolutional Neural Network
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DrDoS	Distributed reflection Denial of Service
EEPROM	Electrically Erasable Programmable Read-Only Memory
FTP	File Transfer Protocol
HIDS	Host-based Intrusion Detection Systems
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
I^2C	Inter-Integrated Circuit
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LAN	Local Area Network
LLC	Logical Link Control
LSTM	Long Short-Term Memory
MAC	Media Access Control
MIMO	Multiple-Input and Multiple-Output
MITM	Man-In-The-Middle

ML	Machine Learning
MLP	MultiLayer Perceptron
MQTT	Message Queuing Telemetry Transport
NIDS	Network Intrusion Detection Systems
OSI	Open Systems Interconnection
POP	Post Office Protocol
PWM	Pulse-width modulation
QoS	Quality of Service
RAM	Random Access Memory
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
SCL	Serial Clock Line
SDA	Serial Data Line
SDN	Software-Defined Networks
SMTP	Simple Mail Transfer Protocol
SPI	Serial Peripheral Interface
SQL	Structured Query Language
SRAM	Static Random Access Memory
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
ΔτΠ	Διαδίκτυο των Πραγμάτων

Κεφάλαιο 1. Εισαγωγή

Η ευρεία ενσωμάτωση των τεχνολογιών έξυπνων συσκευών και του Διαδικτύου των Πραγμάτων (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 και DDoS, 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) μιας έξυπνης συσκευής για την έγκαιρη ανίχνευση επιθέσεων DoS.

1.1. Βιβλιογραφική ανασκόπηση

Η ασφάλεια των IoT συσκευών απασχολεί ιδιαίτερα την ερευνητική και επιστημονική κοινότητα. Στην συνέχεια 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 (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 (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 (DrDoS). Ο πρώτος τρόπος χρησιμοποιεί μοντέλα βαθιάς μάθησης βασισμένα στα δίκτυα μακράς βραχύχρονης μνήμης (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 (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 (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%.

Αξιοποιώντας τεχνικές μηχανικής μάθησης (ML) για την ταξινόμηση της κίνησης του δικτύου, οι Fernandes Silveira et al. [7] προτείνουν έναν ολοκληρωμένο μηχανισμό ανίχνευσης που ονομάζεται σύστημα Smart Detection-IoT (SD-IoT) για την καταπολέμηση των επιθέσεων DDoS σε περιβάλλοντα δικτύων IoT, βασισμένη στην δικτύωση που ορίζεται από λογισμικό (SDN). Η αρχιτεκτονική του συστήματος έχει σχεδιαστεί για την έγκαιρη ανίχνευση επιθέσεων DDoS στο δίκτυο προέλευσης, χρησιμοποιώντας έναν αισθητήρα εγκατεστημένο στο σημείο πρόσβασης του δικτύου IoT, ο οποίος ταξινομεί τη διαδικτυακή κυκλοφορία χρησιμοποιώντας μια στρατηγική βασισμένη στη μηχανική μάθηση. Η πειραματική αξιολόγηση βασίστηκε στα σύνολα δεδομένων CIC-DOS και CICIDS2017 όπως επίσης και σε δείγματα κίνησης δικτύου που συλλέχθηκαν από έναν μεταγωγέα OpenFlow.

Οι Hussain et al. [8] ανέπτυξαν μια μεθοδολογία για τον μετασχηματισμό δεδομένων δικτυακής κίνησης σε μορφή εικόνας και εκπαίδευσαν το ResNet, ένα σύγχρονο μοντέλο CNN, στα μετασχηματισμένα δεδομένα για την ανίχνευση DoS και DDoS επιθέσεων. Για την απόκτηση των δεδομένων κίνησης χρησιμοποίησαν το σύνολο δεδομένων CICDDoS2019, το οποίο περιέχει εισερχόμενη και εξερχόμενη κίνηση των πιο πρόσφατων DoS και DDoS επιθέσεων. Μέσω της αξιολόγησης παρατηρήθηκε ότι σε περίπτωση δυαδικής ταξινόμησης,

η προτεινόμενη μεθοδολογία επιτυγχάνει ακρίβεια 99.99% ενώ σε περίπτωση ταξινόμησης πολλαπλών κατηγοριών επιτυγχάνει ακρίβεια 87.06%.

Τέλος, οι Myridakis et al. [9] πρότειναν μια μέθοδο ανίχνευσης επιθέσεων βασισμένη τα φυσικά χαρακτηριστικά του συστήματος. Συγκεκριμένα παρακολουθείται η αυξομείωση του ρεύματος τροφοδοσίας της συσκευής. Το προτεινόμενο σύστημα αποτελείται από έναν μικροελεγκτή, που παρεμβάλλεται μεταξύ του ρεύματος τροφοδοσίας της συσκευής και της ίδιας της συσκευής. Χρησιμοποιώντας τον νόμο του Ohm πραγματοποιείται ο υπολογισμός της απόκλισης του ρεύματος τροφοδοσίας του συστήματος [10]. Μέσω μετρήσεων που πάρθηκαν σε διάφορες καταστάσεις της IoT συσκευής, παρατηρήθηκε ότι όντως υπάρχει αύξηση της τάσης του ρεύματος τροφοδοσίας κατά την διάρκεια επίθεσης.

1.2. 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

2.1. 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 [11]. 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 [12]. Πρακτικά όμως, ως Διαδίκτυο των Πραγμάτων μπορούμε να αναφερόμαστε σε δίκτυα από αντικείμενα, καθένα εξοπλισμένο με ενσωματωμένους αισθητήρες, τα οποία συνδέονται με το Διαδίκτυο.

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 [13].

2.1.1. Χαρακτηριστικά του Διαδικτύου των Πραγμάτων

Το Διαδίκτυο των Πραγμάτων αποτελείται από τέσσερα βασικά χαρακτηριστικά.

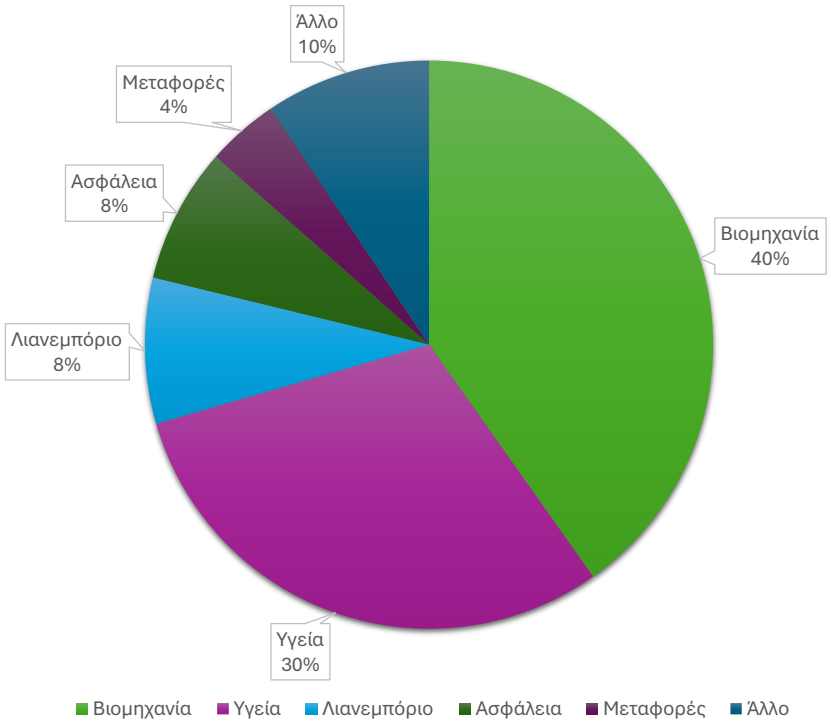
- Πρώτο χαρακτηριστικό αποτελεί η αποδοτική και ικανή προς κλιμάκωση αρχιτεκτονική του συστήματος. Τα συστήματα του IoT οφείλουν να είναι αποδοτικά ως προς την κατανάλωση ενέργειας, αλλά και ως προς την παρεχόμενη υπηρεσία, ενώ πρέπει να έχουν και τη δυνατότητα να επεκταθούν κατ’ απαίτηση.
- Δεύτερο χαρακτηριστικό των συστημάτων του IoT 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 [14].

2.1.2. 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 [15].

2.1.3. Σύγχρονες Εφαρμογές του Διαδικτύου των Πραγμάτων

Οι εφαρμογή των ιδεών του ΔτΠ ξεκίνησε με απλές εφαρμογές, όπου πρώτος στόχος ήταν η διασύνδεση συσκευών. Η ανάπτυξη του διαδικτύου επέτρεψε την διασύνδεση, αρχικά υπολογιστών και ύστερα συσκευών, ανεξάρτητα από την γεωγραφική τους εγγύτητα. 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.

2.2. 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.

2.2.1. Συστήματα υλικού

Τα συστήματα υλικού που απαιτούνται σε ένα σύστημα IoT 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. Κύριος στόχος των gateways είναι η μετάφραση δεδομένων μεταξύ διαφορετικών πρωτοκόλλων επικοινωνίας (π.χ. από Wi-Fi σε IP).

2.2.2. Επικοινωνία

Η επικοινωνία των συσκευών σε ένα σύστημα είναι από τα πιο σημαντικά μέρη του συστήματος. Οι τρόποι επικοινωνίας μπορούν να διακριθούν σε δύο κατηγορίες, την τοπική συνδεσιμότητα και την καθολική συνδεσιμότητα. Η τοπική συνδεσιμότητα επιτυγχάνεται από τεχνολογίες όπως το Wi-Fi (IEEE 802.11), το LoRa, το NB-IoT το ZigBee, 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 [16].

Η κυριότερη τεχνολογία που χρησιμοποιείται για την επικοινωνία των συσκευών στο IoT είναι τα WLANs με τη χρήση Wi-Fi. Το Wi-Fi λειτουργεί πάνω από την οικογένεια προτύπων IEEE 802.11, προσφέροντας πολλαπλές εκδόσεις τους όπως το 802.11b/g/n/ac/ax [17]. Τα πρότυπα αυτά καθορίζουν τον ρυθμό δεδομένων, τις συχνότητες λειτουργίας και άλλα τεχνικά χαρακτηριστικά. Οι συχνότητες λειτουργίας του Wi-Fi είναι είτε τα 2.4 GHz είτε τα 5 GHz. Στη συχνότητα των 2.4 GHz παρέχεται μεγαλύτερο εύρος ζώνης, αλλά μικρότερες ταχύτητες και η επικοινωνία είναι πιο ευάλωτη σε παρεμβολές από γειτονικές συσκευές. Από την άλλη, η συχνότητα των 5 GHz παρέχει μεγαλύτερους ρυθμούς μετάδοσης δεδομένων, αλλά με κόστος την μικρότερη εμβέλεια και περιορισμένες δυνατότητες διάθλασης.

Όσον αφορά την ασφάλεια του, το Wi-Fi συνοδεύεται από διάφορα πρωτόκολλα ασφαλείας όπως τα WPA2/3 για την αυθεντικοποίηση και την κρυπτογράφηση της μεταδιδόμενης πληροφορίες από μη εξουσιοδοτημένη πρόσβαση.

Όλα τα πρότυπα Wi-Fi χρησιμοποιούν το CSMA/CA πρωτόκολλο για πρόσβαση στο μέσο, ενώ χρησιμοποιούν και ίδια δομή πλαισίου για τα πλαίσια του επιπέδου ζεύξης δεδομένων. Σημαντικό πλεονέκτημα των προϊόντων 802.11 είναι πως έχουν καθοδική συμβατότητα, δηλαδή μια συσκευή που χρησιμοποιεί το πρωτόκολλο 802.11g είναι συμβατή για επικοινωνία με ένα σημείο πρόσβασης 802.11ac [17]. Κάθε πρότυπο διαφοροποιείται στο φυσικό επίπεδο, λειτουργώντας σε διαφορετικές περιοχές συχνοτήτων και επιτυγχάνοντας διαφορετικούς ρυθμούς δεδομένων. Επιπλέον, τα πρότυπα 802.11n και 802.11ac χρησιμοποιούν τεχνολογία MIMO για την εκπομπή και λήψη πολλαπλών σημάτων. Συγκεκριμένα, ένας σταθμός βάσης 802.11ac μπορεί να μεταδίδει προς πολλαπλούς σταθμούς ταυτόχρονα χρησιμοποιώντας «έξυπνες κεραίες» [17]. Οι «έξυπνες κεραίες» στρέφουν τους λοβούς εκπομπής των πολλαπλών κεραιών έτσι ώστε να προσανατολίζονται πάντα προς την κατεύθυνση

του δέκτη. Η τεχνική αυτή μειώνει σημαντικά τις παρεμβολές από γειτονικές συσκευές και αυξάνει την εμβέλεια για ένα προκαθορισμένο ρυθμό μετάδοσης δεδομένων. Το πιο πρόσφατο πρότυπο, 802.11ax προσφέρει ακόμη υψηλότερους ρυθμούς δεδομένων (έως 9,6 Gbps), βελτιωμένη αποδοτικότητα για το χειρισμό πολλαπλών συσκευών και βελτιωμένα χαρακτηριστικά ασφαλείας [18].

Πίνακας 1: Πίνακας χαρακτηριστικών προτύπων IEEE 802.11

Πρότυπο	Περιοχή συχνοτήτων (Η.Π.Α)	Ρυθμός δεδομένων
802.11b	2.4 GHz	< 11 Mbps
802.11a	5 GHz	< 54 Mbps
802.11g	2.4 GHz	< 54 Mbps
802.11n	2.5 GHz και 5 GHz	< 450 Mbps
802.11ac	5 GHz	< 1300 Mbps
802.11ax	2.4 GHz και 5 GHz	< 9.6 Gbps

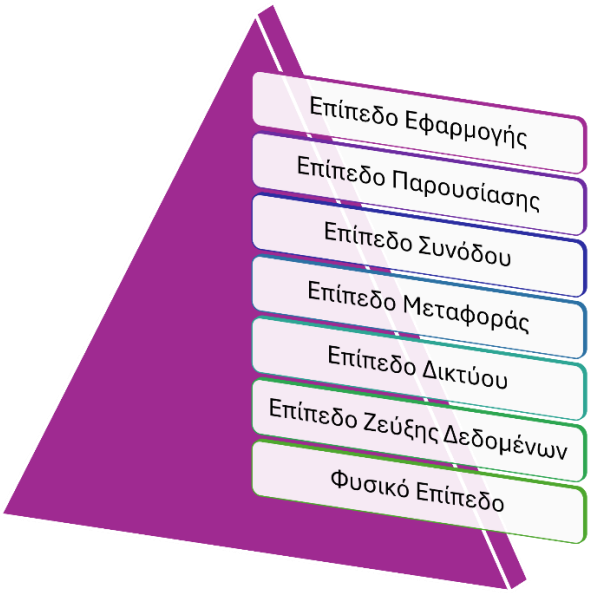
Το IoT και το Wi-Fi είναι δύο τεχνολογίες που είναι στενά συνυφασμένες, οδηγώντας στην ανάπτυξη και τις δυνατότητες των συνδεδεμένων συσκευών σε διάφορους τομείς [19]. Το Wi-Fi χρησιμεύει ως κρίσιμος καταλύτης για το IoT, παρέχοντας την ασύρματη συνδεσιμότητα που επιτρέπει σε δισεκατομμύρια συσκευές να επικοινωνούν και να μοιράζονται δεδομένα. Υπάρχουν αρκετά πλεονεκτήματα από τη χρήση του Wi-Fi ως τεχνολογία διασύνδεσης των συσκευών IoT. Η υποδομή Wi-Fi είναι πανταχού παρούσα, άμεσα διαθέσιμη σε σπίτια, γραφεία και δημόσιους χώρους, εξαλείφοντας την ανάγκη για πρόσθετη υποδομή δικτύου για πολλές εφαρμογές IoT. Τα νεότερα πρότυπα Wi-Fi, όπως τα 802.11ac και ax, προσφέρουν υψηλούς ρυθμούς δεδομένων, κατάλληλους για εφαρμογές που απαιτούν μετάδοση δεδομένων σε πραγματικό χρόνο, όπως η ροή βίντεο από κάμερες ασφαλείας ή βιομηχανικούς αισθητήρες. Σε σύγκριση με άλλες επιλογές συνδεσιμότητας, όπως τα δίκτυα κινητής τηλεφωνίας, το Wi-Fi προσφέρει μια οικονομικά αποδοτική λύση για πολλές εφαρμογές IoT, ιδίως σε μια τοπική περιοχή [20]. Τέλος, η δημιουργία και η διαχείριση των συνδέσεων Wi-Fi είναι σχετικά απλή, καθιστώντας τη φιλική προς το χρήστη τόσο για τους προγραμματιστές όσο και για τους καταναλωτές.

Όπως κάθε τεχνολογία, έτσι και το Wi-Fi εμφανίζει κάποιες αδυναμίες. Βασική αδυναμία του Wi-Fi είναι η περιορισμένη εμβέλεια. Τα εκπεμπόμενα σήματα έχουν

περιορισμένη εμβέλεια, ιδίως στη ζώνη των 5 GHz, γεγονός που το καθιστά ακατάλληλο για συνδέσεις μεγάλων αποστάσεων ή εφαρμογές που απαιτούν ευρεία κάλυψη περιοχής [17] [21]. Από την πλευρά της ασφάλειας, τα δίκτυα Wi-Fi είναι ευάλωτα σε παραβιάσεις ασφαλείας, εάν δεν έχουν ρυθμιστεί και ασφαλιστεί σωστά. Αυτό μπορεί να αποτελέσει σημαντικό πρόβλημα για ευαίσθητες εφαρμογές IoT, ιδίως εκείνες που διαχειρίζονται κρίσιμα δεδομένα όπως βιομετρικά χαρακτηριστικά ή κρίσιμες παραμέτρους βιομηχανικών μονάδων. Τέλος, σημαντικό μειονέκτημα των προτύπων της οικογένειας 802.11 είναι η υψηλή κατανάλωση ενέργειας, το οποίο είναι κρίσιμο χαρακτηριστικό για όλα τα συστήματα IoT. Μεγάλο μέρος των συσκευών που μετέχουν σε ένα σύστημα IoT λειτουργούν με μπαταρία, γεγονός που περιορίζει τις δυνατότητες τους, τόσο σε υπολογιστική ισχύ, όσο και σε αξιοποίηση πρωτοκόλλων επικοινωνίας.

2.2.3. Διαστρωμάτωση Διαδικτύου των Πραγμάτων

Όπως κάθε σύνθετο σύστημα, έτσι και τα συστήματα IoT απαιτούν μια αυστηρά καθορισμένη διαστρωμάτωση των επιπέδων λειτουργίας τους, για την βέλτιστη ανάπτυξη και τον προγραμματισμό τους. Το πιο γνωστό μοντέλο στρωματοποιημένης αρχιτεκτονικής δικτύου είναι το OSI. Το μοντέλο OSI αναπτύχθηκε από τον Διεθνή Οργανισμό Τυποποίησης (ISO) και προδιαγράφει επτά επίπεδα τα οποία υλοποιούν συγκεκριμένες λειτουργίες, ώστε να είναι εφικτή η διασύνδεση διαφορετικών υπολογιστικών συστημάτων (βλ. Εικόνα 2).



Εικόνα 2: Διαστρωμάτωση Επιπέδων Διαδικτύου των Πραγμάτων.

Το ανώτερο επίπεδο του μοντέλου OSI. Που βρίσκεται πιο κοντά στην εφαρμογή του τελικού χρήστη ονομάζεται επίπεδο εφαρμογής. Το λογισμικό που απευθύνεται στον χρήστη αλληλεπιδρά άμεσα με το επίπεδο εφαρμογής μέσω λειτουργιών όπως η κοινή χρήση αρχείων, ο χειρισμός μηνυμάτων ή η πρόσβαση σε βάσεις δεδομένων. Σε αυτό το επίπεδο ανήκουν πρωτόκολλα υψηλού επιπέδου, όπως το HTTP, το POP, το SMTP και το FTP, για την κοινή χρήση πόρων [22]. Αμέσως μετά το επίπεδο εφαρμογής, βρίσκεται το επίπεδο παρουσίασης, που αφορά τη μετάφραση και τη μορφοποίηση δεδομένων. Σε αυτό το επίπεδο, τα πρωτόκολλα χειρίζονται διαδικασίες όπως η κρυπτογράφηση, η αποκρυπτογράφηση, η συμπίεση και η αποσυμπίεση. Ο στόχος του στρώματος παρουσίασης είναι να μετασχηματίσει τα δεδομένα με τέτοιο τρόπο ώστε να μπορούν να σταλούν μέσω ενός δικτύου με σύνταξη που ταιριάζει στις δομές που καθορίζονται από το στρώμα εφαρμογής [23]. Ακολούθως, το επίπεδο συνόδου δημιουργεί κανάλια επικοινωνίας μεταξύ συσκευών. Το συγκεκριμένο επίπεδο χειρίζεται ενέργειες όπως η σύνδεση, η αποσύνδεση και ο τερματισμός μιας συνόδου μεταξύ ενός πελάτη ή διακομιστή. Επίσης, έχει τη δυνατότητα να ορίσει σημεία ελέγχου κατά τη διάρκεια μιας μεταφοράς δεδομένων, έτσι ώστε σε περίπτωση διακοπής , οι συσκευές να μπορούν να συνεχίσουν τη μεταφορά από το τελευταίο σημείο ελέγχου [23].

Με την σειρά του, το επίπεδο μεταφοράς παρέχει όλες τις λειτουργίες και τα μέσα που χρειάζονται ώστε να επιτευχθεί μια από άκρο σε άκρο επικοινωνία μεταξύ

προγραμμάτων ή διεργασιών. Το επίπεδο μεταφοράς λαμβάνει δεδομένα από το επίπεδο συνόδου, τα διασπά σε τμήματα και τα μεταφέρει στο επίπεδο δικτύου, εξασφαλίζοντας ότι όλα τα τμήματα φτάνουν σωστά στο άλλο άκρο. Στα πρωτόκολλα του επιπέδου αυτού ανήκουν τα TCP και UDP [17].

Το επίπεδο δικτύου είναι υπεύθυνο για την δρομολόγηση των πακέτων από τον αποστολέα προς τον παραλήπτη, διασχίζοντας όλου τους ενδιάμεσους κόμβους και ενδέχεται να κατακερματίσει το πακέτο εάν υπερβαίνει το μέγιστο μέγεθος του δικτύου. Τα πιο συνηθισμένα πρωτόκολλα που χρησιμοποιούνται σε αυτό το επίπεδο είναι τα IP, ICMP και RIP [24].

Το επίπεδο σύνδεσης δεδομένων εγκαθιστά και τερματίζει μια σύνδεση μεταξύ δύο φυσικά συνδεδεμένων κόμβων σε ένα δίκτυο. Αποτελείται από δύο μέρη, τον έλεγχο λογικής σύνδεσης (LLC), ο οποίος αναγνωρίζει τα πρωτόκολλα δικτύου, εκτελεί έλεγχο σφαλμάτων και συγχρονίζει τα frames, και τον έλεγχο πρόσβασης στα μέσα (MAC), ο οποίος χρησιμοποιεί διευθύνσεις MAC για τη σύνδεση συσκευών και τον καθορισμό δικαιωμάτων μετάδοσης και λήψης δεδομένων [22].

Τέλος, το φυσικό επίπεδο αποτελεί το χαμηλότερο επίπεδο μετάδοσης δεδομένων μέσω φυσικών μέσων, όπως καλώδια ή ασύρματη μετάδοση, και αναφέρεται σε δυαδικά δεδομένα και στη διαδικασία μετατροπής τους σε ηλεκτρικά σήματα. Το κατώτερο αυτό στρώμα είναι υπεύθυνο για τις διασυνδεδεμένες συσκευές και ο κύριος σκοπός του είναι να εκτελεί την ταυτοποίηση των συσκευών και να παρέχει την ανακάλυψη υπηρεσιών [23]. Οι συσκευές αυτές μπορεί να είναι διαφόρων τύπων (Arduino, Raspberry, ZigBee κ.λπ.), αλλά για να θεωρηθούν ως συσκευές IoT πρέπει να χρησιμοποιούν τεχνολογία επικοινωνίας που να τους επιτρέπει να συνδέονται μεταξύ τους είτε άμεσα είτε έμμεσα μέσω του Διαδικτύου.

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. Επιπλέον, η ευρεία υιοθέτηση και η έντονη εμπορευματοποίηση των τεχνολογιών IoT καθιστούν τις συσκευές του ευάλωτες σε επιθέσεις [25].

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

Η έννοια του IoT καλύπτει ένα μεγάλο εύρος φυσικών αντικειμένων, όπως προσωπικά είδη που χρησιμοποιούμε καθημερινά, βιομηχανικές συσκευές, συσκευές στον τομέα της υγείας και συσκευές στον τομέα της γεωργίας, της κτηνοτροφίας και του περιβάλλοντος γενικότερα. Ένα οικοσύστημα IoT περιλαμβάνει έξυπνες συσκευές με ενσωματωμένους επεξεργαστές, αισθητήρες και τηλεπικοινωνιακό εξοπλισμό που συλλέγουν, αποστέλλουν και επεξεργάζονται δεδομένα από το περιβάλλον τους.

Τα ζητήματα ασφάλειας στο IoT προκύπτουν κυρίως λόγω του τεράστιου αριθμού διασυνδεδεμένων συσκευών, πολλές από τις οποίες είναι ανεξέλεγκτες, δημιουργώντας τρωτά σημεία. Αυτά τα κενά μπορούν να οδηγήσουν σε διαρροή ή απώλεια δεδομένων, ακόμη και μη εξουσιοδοτημένο έλεγχο από τρίτο πρόσωπο ή καταστροφή συσκευών και υποδομών. Καθώς οι διασυνδεδεμένες συσκευές αυξάνονται σε αριθμό και πολυπλοκότητα, αυξάνονται και οι δυνατότητες για κακόβουλες δραστηριότητες. Η αντιμετώπιση αυτών των κενών ασφαλείας είναι απαραίτητη για την ανάπτυξη εφαρμογών του Διαδικτύου των Πραγμάτων. Τα

αποτελεσματικά μέτρα ασφαλείας είναι ζωτικής σημασίας, όπως επίσης και η διασφάλιση της ευρείας υιοθέτησης αυτών από τους τελικούς χρήστες.

Οι συσκευές του IoT ενέχουν σημαντικούς κινδύνους, συμπεριλαμβανομένων πιθανών παραβιάσεων προσωπικών πληροφοριών, μη εξουσιοδοτημένης πρόσβασης σε συσκευές και επιθέσεων σε διάφορα συστήματα. Η ταχεία επέκταση του IoT αυξάνει αυτούς τους κινδύνους, οι οποίοι μπορεί να απειλήσουν όχι μόνο τις συσκευές αλλά και τη σωματική ασφάλεια των χρηστών τους. Με την αυξανόμενη χρήση συσκευών συλλογής δεδομένων στην καθημερινή ζωή, παράγονται, επεξεργάζονται και αποθηκεύονται τεράστιες ποσότητες δεδομένων, γεγονός που τα καθιστά ευάλωτα σε κακόβουλη χρήση από τρίτους. Τα περιστατικά παραβίασης συσκευών και κλοπής δεδομένων αναδεικνύουν την ανάγκη για ισχυρά μέτρα ασφαλείας στα συστήματα IoT. Στα πιο συχνά κενά ασφαλείας περιλαμβάνονται η χρήση παρωχημένου ή μη ασφαλούς λογισμικού, η μετάδοση μη κρυπτογραφημένων δεδομένων και η ανεπαρκής πιστοποίηση και εξουσιοδότηση.

3.2. Επιθέσεις

Στην υποενότητα αυτή θα αναφέρουμε τις επιθέσεις που πραγματοποιούνται ανά επίπεδο του μοντέλου OSI. Οι επιθέσεις που γίνονται στο φυσικό επίπεδο επικεντρώνονται στα φυσικά εξαρτήματα των συστημάτων, καθώς ο επιτιθέμενος πρέπει να βρίσκεται κοντά στο σύστημα. Επιπλέον, στο φυσικό επίπεδο συγκαταλέγονται επιθέσεις που βλάπτουν άμεσα την διάρκεια ζωής και τον κύκλο λειτουργίας μιας συσκευής. Ένα είδος επίθεσης που μπορεί να πραγματοποιηθεί στο κατώτερο επίπεδο του μοντέλου OSI είναι οι επιθέσεις παρεμβολής. Ο επιτιθέμενος στοχεύει την ασύρματη επικοινωνία του συστήματος, παρεμβαίνοντας στις κανονικές συχνότητες που χρησιμοποιούν οι κόμβοι του δικτύου.

Οι επιθέσεις που πραγματοποιούνται στο επίπεδο σύνδεσης δεδομένων είναι τύπου spoofing, δηλαδή ο επιτιθέμενος πλαστογραφεί τη διεύθυνση MAC μιας συσκευής για να υποδυθεί μια άλλη στο δίκτυο. Η ενέργεια αυτή μπορεί να επιτρέψει στον επιτιθέμενο την πρόσβαση σε πόρους του δικτύου ή τη δυνατότητα τροποποίησης και υποκλοπής της κυκλοφορίας του δικτύου που προορίζεται για την νόμιμη πηγή. Σε αυτό το είδος επιθέσεων ανήκουν οι MAC spoofing, ARP spoofing και DHCP spoofing. Το πρωτόκολλο επίλυσης διευθύνσεων (ARP) χρησιμοποιείται για την αντιστοίχιση μιας διεύθυνσης IP σε μια φυσική διεύθυνση μηχανής, αναγνωρίσιμη

στο τοπικό δίκτυο. Όταν μια μηχανή χρειάζεται να βρει την διεύθυνση MAC από μια συγκεκριμένη διεύθυνση IP, στέλνει ένα αίτημα ARP στην μηχανή στην οποία ανήκει η διεύθυνση IP και εκείνη απαντά με ένα μήνυμα απάντησης ARP το οποίο περιέχει την φυσική διεύθυνση και στην συνέχεια, η απάντηση αυτή, καταχωρείται στην προσωρινή μνήμη ARP. Κατά την επίθεση, ο εισβολέας τροποποιεί την προσωρινή μνήμη ARP του στόχου με μια πλαστή καταχώρηση, έχοντας έτσι την δυνατότητα να υποκλέψει frames δεδομένων από το δίκτυο. Το πρωτόκολλο DHCP χρησιμοποιείται για τη δυναμική κατανομή διευθύνσεων IP σε υπολογιστές για μια συγκεκριμένη χρονική περίοδο. Στη επίθεση DHCP spoofing, ο επιτιθέμενος δημιουργεί έναν πλαστό διακομιστή DHCP για να δώσει διευθύνσεις στους υπολογιστές-πελάτες. Επίσης, τους παρέχει και μια ψεύτικη πύλη δικτύου με τις αποκρίσεις DHCP. Έτσι, ο εισβολέας μπορεί να υποκλέψει τα πακέτα που οδηγούνται στην ψεύτικη πύλη δικτύου και να τα απορρίψει ή να απαντήσει στην πραγματική πύλη δικτύου.

Οι επιθέσεις στο τρίτο επίπεδο του μοντέλου OSI πραγματοποιούνται μέσω του διαδικτύου. Στόχος των επιθέσεων αυτών είναι η απόκτηση πρόσβασης σε ένα υπολογιστικό σύστημα που έχει απομονωθεί από το υπόλοιπο δίκτυο. Ανάμεσα στις επιθέσεις αυτού του είδους συγκαταλέγονται οι επιθέσεις ICMP flood, Smurf και MITM. Στην περίπτωση της επίθεσης ICMP ή ping flood, χρησιμοποιείται το πρωτόκολλο μηνυμάτων ελέγχου διαδικτύου (ICMP). Κατά την επίθεση αυτή ο επιτιθέμενος στέλνει έναν μεγάλο αριθμό πακέτων ICMP Echo στον σύστημα-θύμα στοχεύοντας να υπερφορτώσει τη σύνδεση δικτύου με ψευδή κίνηση προκαλώντας άρνηση παροχής υπηρεσιών [1]. Παρόμοια με την ICMP flood επίθεση, είναι και η Smurf επίθεση, με την διαφορά ότι ο επιτιθέμενος στέλνει μεγάλο όγκο κίνησης ICMP με παραποιημένη διεύθυνση IP, δηλαδή έχει ορίσει ως διεύθυνση προέλευσης την διεύθυνση IP του στόχου, πολλαπλασιάζοντας την ποσότητα κίνησης που κατακλύζει το σύστημα- θύμα [26]. Τέλος, σε μια επίθεση MITM ο επιτιθέμενος υποκλέπτει και τροποποιεί την επικοινωνία μεταξύ δύο εμπλεκόμενων, χειραγωγώντας την δρομολόγηση των πακέτων. Στόχος της επίθεσης είναι η απόσπαση προσωπικών πληροφοριών, όπως διαπιστευτήρια σύνδεσης, στοιχεία λογαριασμών και αριθμοί πιστωτικών καρτών.

Οι επιθέσεις που εκτελούνται στο επίπεδο μεταφοράς βασίζονται στη μετάδοση και παραγωγή τεράστιου όγκου κίνησης για την απενεργοποίηση των διαθέσιμων υπηρεσιών του δικτύου στους νόμιμους χρήστες, κάνοντας κατάχρηση των πρωτοκόλλων TCP και UDP, όπως οι επιθέσεις TCP SYN flood και UDP flood.

Η επίθεση SYN flood εκμεταλλεύεται την διαδικασία της τριπλής χειραψίας για την δημιουργία μιας σύνδεσης TCP. Ο επιτιθέμενος στέλνει πολλαπλά πακέτα συγχρονισμού και ο στόχος απαντάει με την αποστολή μηνύματος SYN/ACK για κάθε πακέτο συγχρονισμού που στάλθηκε, προκειμένου να επιβεβαιώσει την επικοινωνία. Στο σημείο αυτό αναμένεται η αποστολή του τελικού πακέτου ACK από τον επιτιθέμενο, για να ολοκληρωθεί η σύνδεση. Η μη αποστολή του τελικού πακέτου δημιουργεί μισάνοιχτες συνεδρίες, οι οποίες οδηγούν στη σταδιακή εξάντληση του διακομιστή και εν τέλη στην κατάρρευσή του [1].

Αντίθετα, η επίθεση UDP flood κατακλύζει την συσκευή του θύματος με πολλά πακέτα UDP σε τυχαίες θύρες. Στην συνέχεια, η συσκευή στόχος θα ελέγξει αν κάποια εφαρμογή χρησιμοποιεί την συγκεκριμένη θύρα και αν όχι, θα απαντήσει με πακέτο ICMP Destination Unreachable. Αυτό έχει ως αποτέλεσμα, όσα περισσότερα πακέτα UDP στείλει ο επιτιθέμενος, τόσα πακέτα απάντησης να στέλνει και η συσκευή στόχος, και συνεπώς καθίσταται μη προσβάσιμη από άλλους χρήστες, οδηγώντας σε άρνηση παροχής υπηρεσιών [27].

Στο επίπεδο συνόδου πραγματοποιείται η επίθεση Session hijacking, όπου ο επιτιθέμενος παραβιάζει το αναγνωριστικό περιόδου σύνδεσης ώστε να αποκτήσει πρόσβαση σε προσωπικές πληροφορίες και κωδικούς πρόσβασης του θύματος.

Στην κατηγορία επιθέσεων hijacking ανήκει και η επίθεση SSL hijacking, που μπορεί να πραγματοποιηθεί στο έκτο επίπεδο. Το SSL είναι ένα πρωτόκολλο ασφαλείας του διαδικτύου που βασίζεται στην κρυπτογράφηση και όσοι ιστότοποι το εφαρμόζουν, έχουν στην διεύθυνση URL τους το «HTTPS». Κατά την επίθεση αυτή, ο επιτιθέμενος δημιουργεί πλαστά πιστοποιητικά για τα domains των ιστότοπων HTTPS που προσπαθεί να επισκεφθεί το θύμα. Ως αποτέλεσμα, το θύμα υποθέτει ότι έχει ασφαλή σύνδεση με τον ιστότοπο-στόχο, αλλά στην πραγματικότητα έχει πραγματοποιήσει σύνδεση με έναν κλωνοποιημένο ιστότοπο που ελέγχεται από τον επιτιθέμενο.

Τέλος, κάποιες από τις επιθέσεις που πραγματοποιούνται στο επίπεδο εφαρμογής είναι οι επιθέσεις phishing, HTTP flood και SQL injection. Οι επιθέσεις phishing χρησιμοποιούν παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα κειμένου, τηλεφωνικές κλήσεις ή ιστότοπους για να εξαπατήσουν τους χρήστες ώστε να μοιραστούν ευαίσθητα δεδομένα ή να κατεβάσουν κακόβουλο λογισμικό.

Στην επίθεση HTTP flood ο επιτιθέμενος υπερφορτώνει τον στόχο με αιτήσεις HTTP και τον οδηγεί σε άρνηση παροχής υπηρεσιών [28]. Κατά την επίθεση SQL injection,

γίνεται εισαγωγή ενός SQL query μέσω τον δεδομένων εισόδου από τον χρήστη στην εφαρμογή με αποτέλεσμα ο επιτιθέμενος να έχει πρόσβαση στην βάση δεδομένων, είτε για να διαβάσει ευαίσθητα δεδομένα είτε για να την τροποποιήσει προς όφελος του.

3.3. Προδιαγραφές ασφαλείας

Στόχος της υποενότητας αυτής είναι η παρουσίαση των βασικών προδιαγραφών ασφαλείας που οφείλουν να τηρούν τα συστήματα IoT. Με βάση την μελέτη των Pal et al. [29] οι προδιαγραφές μπορούν να χωριστούν σε διακριτά σύνολα. Το πρώτο σύνολο αποτελεί την ανάγκη για ελαφριές λύσεις. Κάθε σχεδιαστής συστήματος οφείλει να λαμβάνει υπόψη τον περιορισμό πόρων των συσκευών του IoT, ο οποίος κατ' επέκταση θέτει περιορισμούς στην υλοποίηση κρυπτογραφικών τεχνικών και πρωτοκόλλων. Επιπλέον, συμπεριλαμβάνεται η ανάγκη για ενεργειακή αποδοτικότητα. Συνεπώς, οι λύσεις ασφαλείας πρέπει να είναι επεξεργαστικά ελαφριές, επιτυγχάνοντας ισορροπία μεταξύ των κρυπτογραφικών τεχνικών ασφαλείας και της βελτιωμένης επικοινωνίας των δεδομένων με προσοχή στην κατανάλωση ενέργειας. Το δεύτερο σύνολο προδιαγραφών ορίζει την ανάγκη των συστημάτων IoT να πραγματώνουν την έννοια της αποκεντρωμένης διαχείρισης. Όπως προαναφέραμε, τα συστήματα IoT μπορούν να κλιμακωθούν σε σημαντικά μεγάλο βαθμό. Ως εκ τούτου, οι κεντρικοποιημένες λύσεις ασφαλείας δεν αποτελούν δόκιμη επιλογή. Η ανερχόμενη αξιοποίηση των αποκεντρωμένων αρχιτεκτονικών με τη χρήση edge συσκευών επιφέρει μια κατανεμημένη συμπεριφορά στα συστήματα. Με βάση αυτά, η ασφάλεια των συσκευών πρέπει να βρίσκεται όσο πιο κοντά στην ευάλωτη συσκευή γίνεται, ενώ παράλληλα να υλοποιεί της προδιαγραφές του πρώτου συνόλου, για υπολογιστικά ελαφριά συστήματα. Μια προτεινόμενη αρχιτεκτονική σκιαγραφεί ένα αποκεντρωμένο σύστημα που θα είναι υπεύθυνο για συστάδες συσκευών.

Ένα από τα κύρια χαρακτηριστικά του IoT είναι η ετερογένεια των συσκευών του.

Αυτό σημαίνει πως οι πληροφορίες περνούν από πολλαπλούς τομείς και τεχνολογίες. Λαμβάνοντας υπόψη την παραπάνω πτυχή σχηματίζεται το τρίτο σύνολο προδιαγραφών, που αφορούν την ασφάλεια από άκρο-σε-άκρο. Μέσω αυτού του συνόλου, καλύπτονται τα ζητήματα ασφαλούς αποθήκευσης, ασφαλούς επικοινωνίας, ασφαλούς περιεχομένου και ποιότητας υπηρεσίας (QoS). Συνολικά απαιτούνται

διαλειτουργικές τεχνολογίες ασφαλείας, πολιτικές διαχείρισης της πληροφορίας μεταξύ των διαφορετικών τομέων και δυνατότητες ταυτοποίησης ανάμεσα στα τερματικά σημεία του συστήματος. Παράλληλα, η εξασφάλιση της ποιότητας υπηρεσίας του δικτύου μπορεί να θεωρηθεί ως μια πτυχή, η διασφάλιση της οποίας οδηγεί και στην διασφάλιση της δικτύωσης των συσκευών. Είναι επίσης σημαντικό να προστατεύονται οι κρίσιμες παράμετροι QoS κατά τη διάρκεια της επικοινωνίας και να προστατεύονται τα πακέτα δεδομένων κατά τη μετάδοσή τους.

Το τελευταίο σύνολο προδιαγραφών που προτείνεται στο [29], αφορά την ανθεκτικότητα και την αξιοπιστία της συσκευής. Τα συστήματα IoT πρέπει να είναι εύρωστα απέναντι σε παράγοντες όπως η φορητότητα, ο αυξανόμενος αριθμός επιθέσεων και οι πιθανές δυσλειτουργίες των συσκευών. Αντίστοιχη αντοχή θα πρέπει να επιδεικνύουν τα μέτρα ασφαλείας που προορίζονται για αυτά τα συστήματα. Η ύπαρξη ικανοτήτων αυτοεπιδιόρθωσης επιτρέπει στα συστήματα ασφαλείας να ανιχνεύουν και να αντιμετωπίζουν αυτόματα τις τυχόν βλάβες που έχουν προκληθεί, αξιοποιώντας την συγκέντρωση και ανάλυση δεδομένων σε πραγματικό χρόνο από έξυπνους αισθητήρες. Όλα τα μέτρα ασφαλείας που προτείνονται πρέπει να εξασφαλίζουν την ακεραιότητα μεταξύ των επιμέρους λειτουργικών εξαρτημάτων και των υπηρεσιών σε εφαρμογές IoT ευρείας κλίμακας, όπως οι εμπορικοί τομείς (smart home, smart health, κ.λπ.).

3.4. Συστήματα ανίχνευσης

Λαμβάνοντας υπόψη την σημαντικότητα της ασφάλειας των συσκευών σε ένα δίκτυο IoT, προτείνονται τόσο από την ερευνητική κοινότητα όσο και από την βιομηχανία, συστήματα τα οποία είναι ικανά να ανιχνεύουν επιθέσεις που εκμεταλλεύονται τα κενά ασφαλείας. Πολλά από αυτά τα συστήματα λειτουργούν με βάση μια από τις δύο αρχές, την παρακολούθηση της τηλεπικοινωνιακής κίνησης (πακέτα πρωτοκόλλων) ή την παρακολούθηση των φυσικών χαρακτηριστικών του συστήματος (τάση ρεύματος, θερμοκρασία, κ.λπ.).

Όσον αφορά τα IDS, χωρίζονται σε τρείς κατηγορίες: σε συστήματα ανίχνευσης εισβολών με βάση τον κεντρικό υπολογιστή (HIDS), σε συστήματα ανίχνευσης εισβολών στο δίκτυο (NIDS) και σε υβριδικά συστήματα ανίχνευσης εισβολών.

Η πρώτη κατηγορία IDS είναι αφιερωμένη αποκλειστικά στο σύστημα του κεντρικού υπολογιστή. Ως κεντρικός υπολογιστής μπορεί να θεωρηθεί ένας διακομιστής, ένας

υπολογιστής ή οποιοσδήποτε άλλος τύπος συσκευής που παράγει αρχεία καταγραφής, μετρήσεις και άλλα δεδομένα που μπορούν να παρακολουθούνται για λόγους ασφαλείας. Από την ανάλυση των αρχείων καταγραφής μπορεί να εντοπιστεί κακόβουλη χρήση, παραδείγματος χάριν: τροποποίηση σε αρχεία ζωτικής σημασίας για την λειτουργικότητα του λειτουργικού συστήματος, παραβίαση των ελέγχων πρόσβασης κ.α. Τα HIDS μπορούν να δημιουργήσουν λεπτομερείς και ακριβείς υπογραφές για την ανίχνευση εισβολών στο σύστημα του κεντρικού υπολογιστή, οδηγώντας σε χαμηλά ποσοστά ψευδώς θετικών αποτελεσμάτων λόγω της ακρίβειας αυτών των υπογραφών. Σε περίπτωση που εφαρμοστεί σωστά πλεονεκτεί έναντι του NIDS διότι μπορεί να εντοπίσει ύποπτο περιεχόμενο μέσα σε κρυπτογραφημένα πακέτα. Ως μειονέκτημα του συγκεκριμένου συστήματος ανίχνευσης εισβολών αναφέρεται το υψηλό κόστος συντήρησης [30]. Δύο από τα πιο δημοφιλή συστήματα ανίχνευσης εισβολών με βάση τον κεντρικό υπολογιστή είναι τα OSSEC και Tripwire [31].

Αντίθετα, τα συστήματα ανίχνευσης εισβολών στο δίκτυο πραγματοποιούν ανάλυση δεδομένων κίνησης δικτύου για τον εντοπισμό κακόβουλων δραστηριοτήτων. Αποτελούν αυτόνομες συσκευές που βρίσκονται στο ίδιο δίκτυο με το σύστημα που παρακολουθείται και έχουν την δυνατότητα να επιβλέπουν πολλά ξεχωριστά συστήματα σε ένα κοινό δίκτυο. Η τοποθέτηση μιας τέτοιας συσκευής σε αυτή τη θέση βοηθά στον άμεσο εντοπισμό εισβολών και συχνά περνά απαρατήρητη από τους επιτιθέμενους [32]. Τα NIDS μπορούν να συγκεντρώνουν δεδομένα και να καταγράφουν τις δραστηριότητες των κεντρικών υπολογιστών στα δίκτυα, χρησιμοποιώντας διάφορες μεθοδολογίες για τον εντοπισμό εισβολών. Ωστόσο, η εφαρμογή μιας τέτοιας τεχνολογίας μπορεί να επιβραδύνει το δίκτυο και δεν μπορεί να ανιχνεύσει κακόβουλα πακέτα δεδομένων, εάν αυτά είναι κρυπτογραφημένα. Ένα άλλο συχνό πρόβλημα με τα NIDS είναι το υψηλό ποσοστό ψευδών αρνητικών και ψευδών θετικών αποτελεσμάτων. Τα ψευδώς αρνητικά συμβαίνουν όταν οι απειλές ταξινομούνται εσφαλμένα ως φυσιολογικές, ενώ τα ψευδώς θετικά είναι καλοήθεις δραστηριότητες που αναγνωρίζονται εσφαλμένα ως απειλές [30]. Δύο από τα πιο ευρέως χρησιμοποιούμενα συστήματα ανίχνευσης εισβολών στο δίκτυο είναι τα Snort και Suricata. Το πρώτο προσφέρει ανίχνευση και πρόληψη εισβολών σε πραγματικό χρόνο, μαζί με παρακολούθηση της ασφάλειας δικτύου ενώ το δεύτερο αποτελεί μια σύγχρονη ενναλακτική λύση του Snort, σχεδιασμένο να λειτουργεί πολυνηματικά και αξιοποιεί προηγμένα μοντέλα στατιστικής για την ανίχνευση ανωμαλιών [31].

Η ανάγκη για αποτελεσματική προστασία απέναντι στην συνεχώς αναπτυσσόμενη πληθώρα επιθέσεων, οδήγησε στον συνδυασμό των δύο προαναφερθέντων συστημάτων. Τα υβριδικά IDS παρακολουθούν ταυτόχρονα τους κεντρικούς υπολογιστές και το δίκτυο, βελτιώνοντας την ασφάλεια του δικτύου και καθιστώντας τα δεδομένα πιο ασφαλή και λιγότερο επιρρεπή σε επιθέσεις ή κλοπή [33].

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.

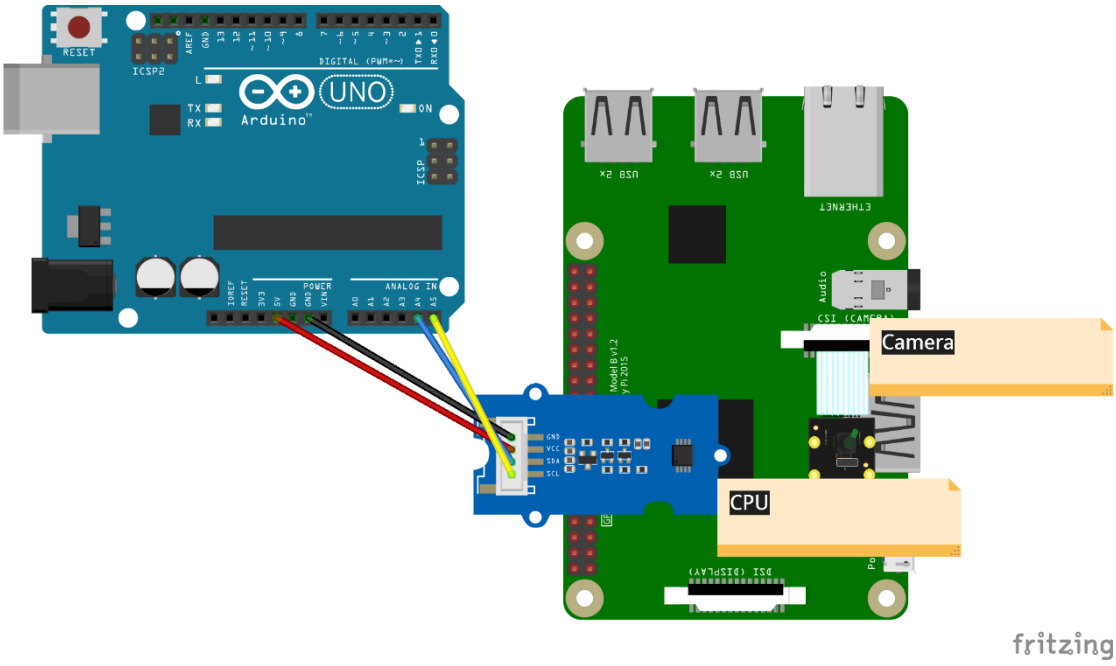
4.1. Μοντέλο συστήματος

Για την υλοποίηση του συστήματος πρέπει πρώτα να προηγηθεί η μοντελοποίηση του. Ως πρώτο στάδιο δημιουργούμε ένα αφαιρετικό μοντέλο που απλά περιγράφει τις σχέσεις μεταξύ των συνιστωσών του. Το αφηρημένο μοντέλο (Εικόνα 3) παρέχει μια γενική ιδέα για τον τρόπο συναρμολόγησης του συστήματος.

Εικόνα 3: Αφηρημένο σχήμα μοντέλου συστήματος

Στην γενική περίπτωση, το σύστημα προσαρμόζεται σε μια συσκευή IoT, και συγκεκριμένα έχουμε τοποθέτηση του αισθητήρα θερμοκρασίας πάνω στην CPU (Εικόνα 3). Ο αισθητήρας επικοινωνεί τις μετρήσεις θερμοκρασίας μέσω του μικροελεγκτή και της σειριακής του διεπαφής στο κεντρικό υπολογιστικό σύστημα. Το κεντρικό υπολογιστικό σύστημα μπορεί να είναι οποιοδήποτε υπολογιστικό ή και μικροϋπολογιστικό σύστημα. Στο κεντρικό υπολογιστικό σύστημα εκτελείται η ανάλυση των μετρήσεων και η γραφική τους απεικόνιση.

Η συσκευή IoT που θα χρησιμοποιηθεί για την πειραματική αξιολόγηση της υλοποίησης είναι μια IP κάμερα. Η IP κάμερα υλοποιήθηκε με την χρήση ενός μικροϋπολογιστή Raspberry Pi Zero W και ένα εξάρτημα κάμερας. Ο αισθητήρας θερμοκρασίας στερεώνεται πάνω στην CPU του μικροϋπολογιστή με τη χρήση θερμοαγώγιμου επιθέματος. Το σύστημα κατασκευάζεται με βάση το παρακάτω αναλυτικό διάγραμμα σχεδίασης (Εικόνα 4).



Εικόνα 4: Αναλυτικό σχεδιαστικό διάγραμμα συστήματος.

4.2. Χαρακτηριστικά συστήματος

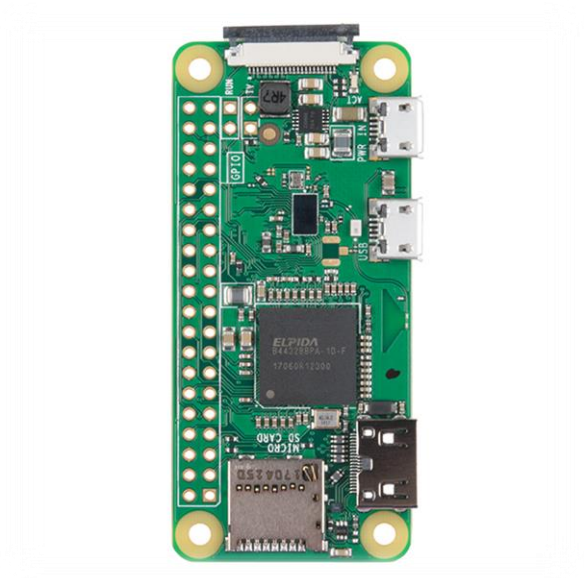
Το παρόν κύκλωμα αποτελείται από έναν μικροϋπολογιστή Raspberry Pi Zero W, έναν μικροελεγκτή Arduino UNO και έναν αισθητήρα θερμοκρασίας MCP9808, τα οποία και θα αναλύσουμε.

4.2.1. Raspberry Pi Zero W

Το Raspberry Pi Zero W είναι ένας μικροϋπολογιστής βασισμένος στον μονοπύρηνο επεξεργαστή Broadcom BCM2835 με συχνότητα λειτουργίας 1GHz. Διαθέτει 512MB μνήμης SDRAM και υποδοχή microSD για την εγκατάσταση και εκτέλεση του λειτουργικού συστήματος. Το συγκεκριμένο μοντέλο περιέχει ενσωματωμένη

ασύρματη δικτύωση Wi-Fi 802.11n καθώς και δυνατότητες συνδεσιμότητας μέσω Bluetooth 4.1 και υποδοχής mini HDMI. Επίσης, περιέχει δύο θύρες micro USB για την τροφοδοσία και την σύνδεση περιφερειακών, όπως πληκτρολόγιο, ποντίκι κ.λπ. Επιπλέον, μέσω της υποδοχής CSI επιτρέπεται η σύνδεση με Raspberry Pi Camera Module για την καταγραφή βίντεο ή την λήψη φωτογραφιών.

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 [34].



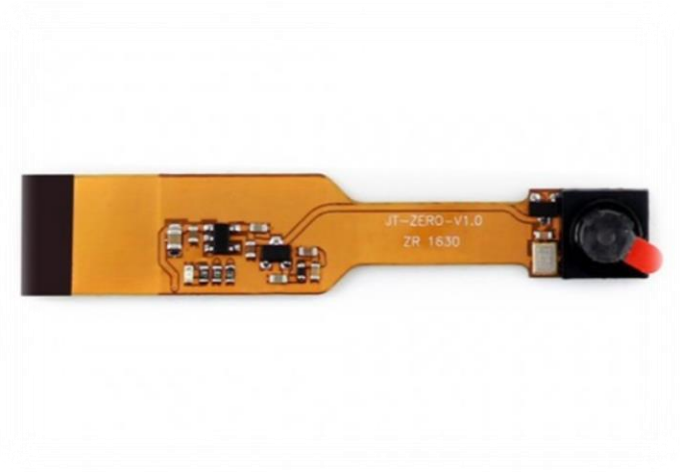
Εικόνα 5: Αναπαράσταση του μικροϋπολογιστή Raspberry Pi Zero W. Πηγή: https://www.hellasdigital.gr/go-create/raspberry-and-accessories/raspberry-pi/raspberry-pi-zero-w-dev-14277/

4.2.1.1 Raspberry Pi Zero Κάμερα V1

Για τις ανάγκες της παρούσας υλοποίησης ο μικρουπολογιστής λειτουργεί ως IoT συσκευή, συγκεκριμένα ως IP κάμερα. Αξιοποιώντας την θύρα CSI που παρέχει το Raspberry Pi Zero W, συνδέσαμε μονάδα κάμερας με ανάλυση 5MP για την καταγραφή βίντεο συνεχούς ροής εικόνας. Η κάμερα ενεργοποιείται εκτελώντας την εντολή

```
raspivid -o - -t 0 -hf -w 800 -h 400 -fps 24 |cvlc -vvv
stream:///dev/stdin --sout '#standard{access=http,mux=ts,dst=:8160}'
:demux=h264
```

στο τερματικό του μικροϋπολογιστή και μέσω της εφαρμογής VLC μπορούμε να παρακολουθήσουμε την καταγραφή. Η εντολή δύναται να λάβει διάφορες παραμέτρους (Πίνακας 2).



Εικόνα 6: Απεικόνιση Raspberry Pi Zero κάμερας V1.3. Πηγή: https://grobotronics.com/raspberry-zero-v1.3-mini-camera.html?gad_source=1&gclid=CjwKCAjw65-zBhBkEiwAjrqRMGg6KnFQqeSsPQHuuaSjNN6Z58sOa4kqWZNXYme-Mk_fNmaCe5AsexoCl_QQAvD_BwE#group_10756666830fd41a5d-4

Πίνακας 2: Παράμετροι εντολής καταγραφής συνεχούς ροής εικόνας.

ΠΑΡΑΜΕΤΡΟΙ	ΕΝΝΟΙΑ
-o	Καθορίζει το όνομα του αρχείου εξόδου, το '-' δίπλα δηλώνει ότι δεν υπάρχει όνομα αρχείου.
-t	Καθορίζει τη διάρκεια καταγραφής, με το 0 να σημαίνει άπειρο.
-hf	Ανατροπή ως προς τον οριζόντιο άξονα.
-w	Καθορίζει την ανάλυση για το πλάτος.
-h	Καθορίζει την ανάλυση για το ύψος.
-fps	Καθορίζει την συχνότητα καταγραφής της εικόνας.

Οι υπόλοιποι παράμετροι σημαίνουν ότι τα δεδομένα θα αποστέλλονται χρησιμοποιώντας το πρωτόκολλο επικοινωνίας http στη θύρα 8160 με μορφή κωδικοποίησης βίντεο το h264 ως την προεπιλεγμένη ροή εξόδου.

4.2.2. Arduino UNO R3

Ο μικροελεγκτής Arduino Uno αποτελεί μια από τις πιο δημοφιλείς πλατφόρμες ανοικτού κώδικα. Πρόκειται για ένα ηλεκτρονικό κύκλωμα που βασίζεται στον

μικροελεγκτή ATmega328P της Atmel και διαθέτει 32KB μνήμης FLASH για την αποθήκευση των προγραμμάτων και του bootloader, 2KB μνήμης SRAM, για την αποθήκευση μεταβλητών, πινάκων κ.λπ. κατά την εκτέλεση των προγραμμάτων, και 1KB μνήμης EEPROM, για μόνιμη αποθήκευση δεδομένων. Ο επεξεργαστής του λειτουργεί στα 16MHz, προσφέροντας επαρκή υπολογιστική ισχύ.
Η πλακέτα Arduino Uno παρέχει 14 ψηφιακούς ακροδέκτες εισόδου/εξόδου, εκ των οποίων οι 6 μπορούν να χρησιμοποιηθούν και ως PWM έξοδοι για την αναλογική διαμόρφωση σήματος, καθώς και 6 αναλογικές εισόδους. Η τροφοδοσία του μπορεί να πραγματοποιηθεί μέσω σύνδεσης USB ή εξωτερικής πηγής τάσης από 7 έως 12V.
Για την επικοινωνία του μικροελεγκτή με τον υπολογιστή, ενσωματώνει τον μικροελεγκτή ATmega16U2, ο οποίος δημιουργεί μια σειριακή επικοινωνία μέσω θύρας USB και εμφανίζεται στον υπολογιστή ως εικονική θύρα COM. Επίσης, ο ATmega328 υποστηρίζει το πρωτόκολλο I2C και επικοινωνία με SPI [35].

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.

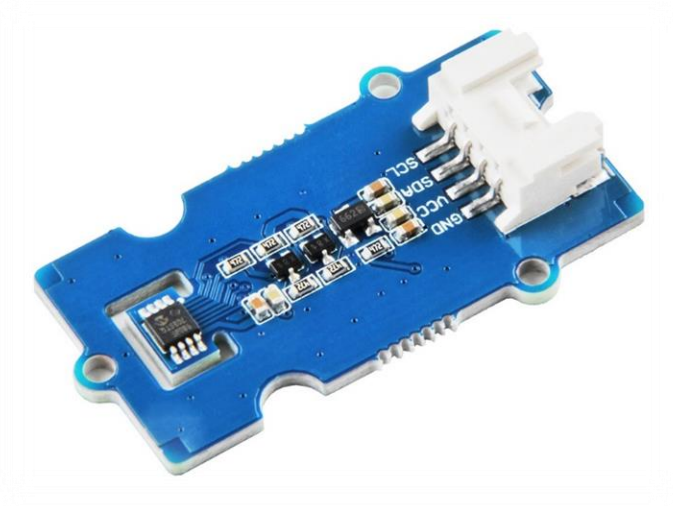
Εικόνα 7: Αναπαράσταση του μικροελεγκτή Arduino Uno. Πηγή: https://grobotronics.com/arduino-uno-rev3.html#group_24666638098d65bd-2

4.2.3. Αισθητήρες Θερμοκρασίας

4.2.3.1 MCP9808

Ο MCP9808 είναι ένας ψηφιακός αισθητήρας θερμοκρασίας χαμηλής ενεργειακής κατανάλωσης και υψηλής ακρίβειας. Παρέχει τυπική ακρίβεια $\pm 0.25℃$ από τους $-40℃$ έως τους $+125℃$ και μέγιστη ακρίβεια $\pm 0.5℃$ στην πιο συχνά χρησιμοποιούμενη περιοχή, από $-20℃$ έως $+100℃$. Επιπλέον, ο αισθητήρας προσφέρει τέσσερις επιλογές ανάλυσης, $0.5℃$, $0.25℃$, $0.125℃$ και $0.0625℃$, επιτρέποντας εξαιρετικά λεπτομερείς μετρήσεις θερμοκρασίας.

Για την διασύνδεση του αξιοποιείται το πρωτόκολλο επικοινωνίας I^2C, το οποίο επιτρέπει επικοινωνία μεταξύ πολλαπλών συσκευών χρησιμοποιώντας μόνο δύο καλώδια. Συγκεκριμένα, χρησιμοποιεί τους ακροδέκτες SDA (A4) και SCL (A5) του μικροελεγκτή. Όσον αφορά την τάση τροφοδοσίας, λειτουργεί σε εύρος 2.7V έως 5.5V. Τέλος, ενσωματώνει προγραμματιζόμενες εξόδους που ενεργοποιούνται όταν η θερμοκρασία μεταβληθεί από ένα προκαθορισμένο όριο [36].



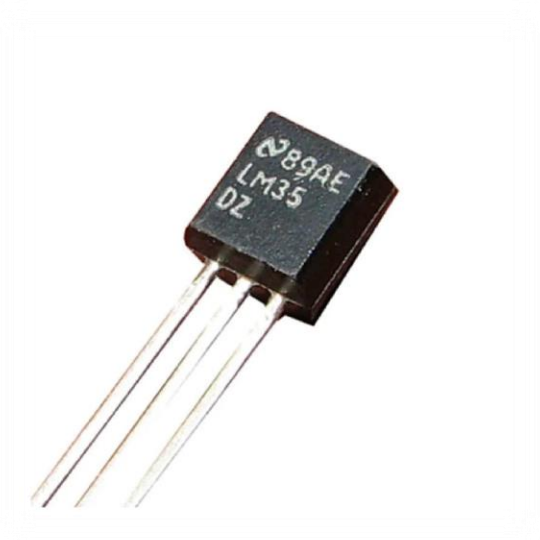
Εικόνα 8: Απεικόνιση του αισθητήρα θερμοκρασίας MCP9808. Πηγή:https://wiki.seeedstudio.com/Grove-I2C_High_Accuracy_Temperature_Sensor-MCP9808/

4.2.3.2 Εναλλακτικοί Αισθητήρες Θερμοκρασίας

Για τη εύρεση του κατάλληλου αισθητήρα θερμοκρασίας για τις ανάγκες της παρούσας υλοποίησης εξετάστηκαν και οι παρακάτω:

4.2.3.2.1 LM35

Ο LM35 αποτελεί αισθητήρα θερμοκρασίας ακριβείας που παράγει τάση εξόδου ευθέως ανάλογη της θερμοκρασίας σε βαθμούς Κελσίου. Για κάθε βαθμό αύξησης της θερμοκρασίας, η τάση εξόδου αυξάνεται κατά περίπου 10 millivolts. Δεν απαιτεί εξωτερική βαθμονόμηση και προσφέρει τυπική ακρίβεια ±0.5°C σε θερμοκρασία δωματίου (περίπου 25°C), όμως η ακρίβεια αυτή υποβαθμίζεται ελαφρώς στα άκρα του εύρους λειτουργίας του, από $-55℃$ έως $+150℃$ [37].



Εικόνα 9: Απεικόνιση του αισθητήρα θερμοκρασίας LM35. Πηγή: https://zinbal.com/product/temperature-sensor-lm35/

4.2.3.2.2 TMP36

Ο TMP36 είναι ένας αισθητήρας θερμοκρασίας χαμηλής τάσης και υψηλής ακριβείας που εξάγει τάση γραμμικά ανάλογη της θερμοκρασίας σε βαθμούς Κελσίου. Δεν απαιτεί εξωτερική βαθμονόμηση και παρέχει τυπικές ακρίβειες ±1°C στους 25°C και ±2°C σε εύρος από -40°C έως +125°C. Όπως στον LM35 έτσι και στον TMP36, για κάθε βαθμό αύξησης της θερμοκρασίας, η τάση εξόδου αυξάνεται κατά περίπου 10 millivolts [38].

Εικόνα 10: Απεικόνιση του αισθητήρα θερμοκρασίας TMP36. Πηγή: https://www.sparkfun.com/products/10988

4.2.4 Θερμοαγώγιμο επίθεμα

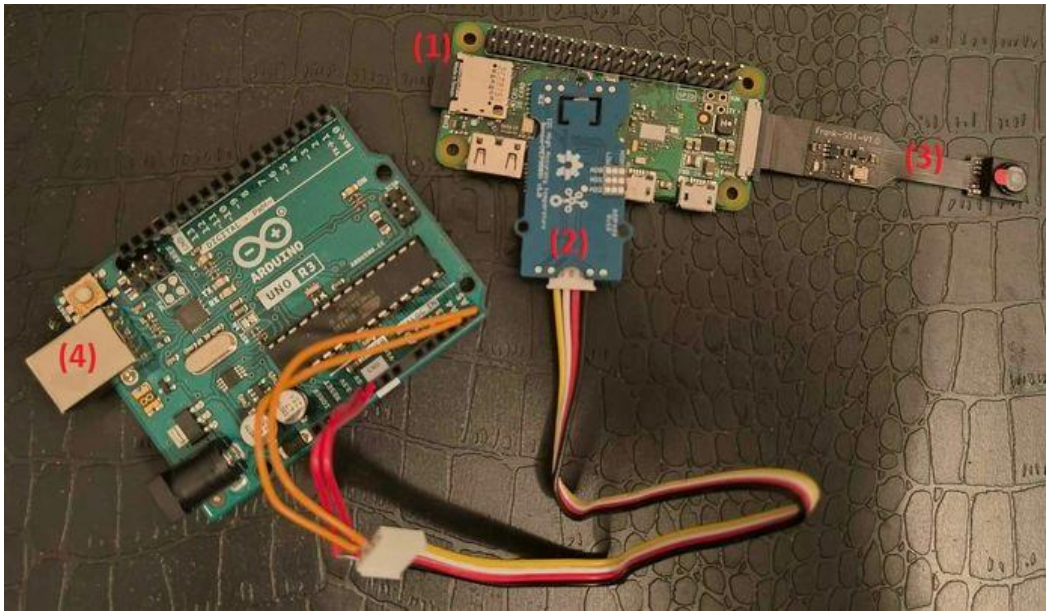
Τα θερμικά επιθέματα λειτουργούν με τον ίδιο τρόπο όπως και τα υπόλοιπα υλικά θερμικής διεπαφής. Τοποθετούνται ανάμεσα σε δύο εξαρτήματα για να μεταφέρουν θερμότητα από το ένα στο άλλο. Συνήθως, αυτό σημαίνει την απομάκρυνση της θερμότητας από μια πηγή θερμότητας, όπως η CPU ή η κάρτα γραφικών, προς μια ψύκτρα, προκειμένου να προστατεύσουν τη συσκευή από την υπερθέρμανση. Τα υλικά που χρησιμοποιούνται για την δημιουργία των επιθεμάτων είναι ως επί το πλείστον η σιλικόνη και ο γραφίτης. Ωστόσο, υπάρχουν κι άλλες επιλογές όπως ακρυλικό, αλουμίνιο και πολυεστέρας [39]. Στην παρούσα υλοποίηση, το θερμοαγώγιμο επίθεμα μεταφέρει τη θερμότητα από τη CPU προς τον αισθητήρα θερμοκρασίας MCP9808.

Εικόνα 11: Απεικόνιση θερμικού επιθέματος. Πηγή: https://grobotronics.com/heat-sink-thermal-tape-80x80mm.html#group_13687666846a003604-2

4.3. Υλοποίηση συστήματος

4.3.1. Παρουσίαση συστήματος

Το σύστημα κατασκευάζεται με βάση το σχεδιαστικό διάγραμμα (Εικόνα 4).



Εικόνα 12: Απεικόνιση συστήματος παρακολούθησης θερμοκρασίας.

Ο αισθητήρας θερμοκρασίας MCP9808 (Εικόνα 12, (2)) τοποθετείται με την όψη προς τα κάτω, πάνω από τον επεξεργαστή του Raspberry Pi (Εικόνα 12,(1)) με τη βοήθεια θερμοαγώγιμου επιθέματος, για την καλύτερη 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 (Εικόνα 12, (4)) για την μεταφορά των μετρήσεων στον μικροελεγκτή. Τέλος, στο Raspberry Pi συνδέεται κάμερα (Εικόνα 12, (3)), επιτρέποντας στον μικροϋπολογιστή να λειτουργεί ως IP Camera.

4.3.2. Κώδικας υλοποίησης

Η παραπάνω διασύνδεση (Εικόνα 12) υποστηρίζεται από τον μικροελεγκτή, πάνω στον οποίο γράφεται ο κώδικας ελέγχου του συστήματος. Συγκεκριμένα, ο κώδικας

αφορά την λειτουργία του αισθητήρα θερμοκρασίας (βλ. Παράρτημα Α: Κώδικες Arduino, I, σελ.56).

Η βιβλιοθήκη Wire.h αξιοποιείται για την επικοινωνία του μικροελεγκτή με συσκευές που χρησιμοποιούν το I^2C 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 I^2C πρωτόκολλο, χρειάζεται να του υποδείξουμε σε ποια διεύθυνση θα συνδεθεί, διότι παρέχεται η δυνατότητα να συνδεθούν πολλοί αισθητήρες στον ίδιο δίαυλο I^2C 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 του Πίνακας 3.

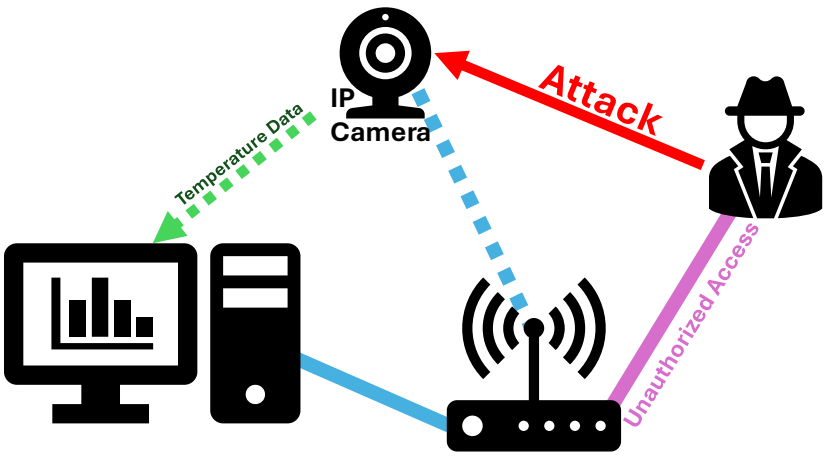
Πίνακας 3: Πίνακας επιλογών ανάλυσης αισθητήρα θερμοκρασίας MCP9808

Λειτουργία	**Ανάλυση**	**Περίοδος δειγματοληψίας**
0	0.5°C	30 ms
1	0.25°C	65 ms
2	0.125°C	130 ms
3	0.0625°C	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. Μοντέλο προσομοίωσης

Για την λήψη των μετρήσεων σχεδιάστηκε ένα μοντέλο προσομοίωσης (), το οποίο περιλαμβάνει το μοντέλο συστήματος (Εικόνα 4).



Εικόνα 13: Μοντέλο προσομοίωσης

Στο μοντέλο προσομοίωσης διακρίνονται τέσσερεις βασικές οντότητες. Αρχικά έχουμε το υπολογιστικό σύστημα καταγραφής και γραφικής απεικόνισης των μετρήσεων θερμοκρασίας από την οντότητα IP Camera. Η οντότητα IP Camera σχεδιάζεται με βάση την (Εικόνα 4) και δέχεται επίθεση από ένα δεύτερο υπολογιστικό σύστημα που ορίζεται ως ο επιτιθέμενος. Και οι τρείς οντότητες επικοινωνούν με βάση το LAN που δημιουργείται από τον δρομολογητή. Ο επιτιθέμενος θεωρείται πως έχει αποκτήσει πρόσβαση στο LAN ή πως γνωρίζει την IP διεύθυνση της κάμερας από κάποια διαδικασία εξερεύνησης δικτύου.

Για την εκτέλεση της προσομοίωσης, χρησιμοποιήσαμε έναν δρομολογητή χωρίς σύνδεση στο διαδίκτυο, ώστε να δημιουργήσουμε ένα LAN, όπου συνδέσαμε την IP Camera (Raspberry Pi Zero W), το υπολογιστικό σύστημα καταγραφής (Laptop 1) και το υπολογιστικό σύστημα του επιτιθέμενου (Laptop 2). Το υπολογιστικό σύστημα καταγραφής λειτουργεί σε Windows, ενώ το σύστημα του επιτιθέμενου σε Linux.

4.5. Μετρήσεις και πειραματική αξιολόγηση

Η αξιολόγηση του συστήματος πραγματοποιήθηκε καταγράφοντας την θερμοκρασία του συστήματος σε διάφορες καταστάσεις διάρκειας 32 λεπτών, όπως κατά την διάρκεια εκκίνησης, σε κατάσταση αδράνειας και σε κανονική λειτουργία. Ως κατάσταση αδράνειας (idle state) θεωρήθηκε η καταγραφή συνεχούς ροής εικόνας είτε με κίνηση είτε χωρίς και ως κανονική λειτουργία (normal state) θεωρήθηκε η παράλληλη εκτέλεση καταγραφής συνεχούς ροής εικόνας, είτε με κίνηση είτε χωρίς,

και ενός σεναρίου κελύφους στον μικροϋπολογιστή για την καταγραφή της εσωτερικής θερμοκρασίας του συστήματος. Επίσης, πάρθηκαν μετρήσεις κατά τη διάρκεια ημέρας και νύχτας σε τέσσερις διαφορετικές καταστάσεις: χωρίς κίνηση και χωρίς εκτέλεση σεναρίου κελύφους, χωρίς κίνηση και με εκτέλεση σεναρίου κελύφους, με κίνηση και χωρίς εκτέλεση σεναρίου κελύφους, με κίνηση και με εκτέλεση σεναρίου κελύφους.

Σε όλες τις καταστάσεις πάρθηκε και η αντίστοιχη μέτρηση με επίθεση. Σε κάθε περίπτωση μελέτης εκτελέστηκαν δύο επιθέσεις διάρκειας τριών λεπτών η κάθε μία. Συγκεκριμένα η πρώτη επίθεση αρχίζει μετά τα πρώτα πέντε λεπτά της καταγραφής των τιμών θερμοκρασίας και η δεύτερη αρχίζει δέκα λεπτά μετά την λήξη της πρώτης.

Για την πραγματοποίηση της επίθεσης χρησιμοποιήθηκε το εργαλείο hping3 και εκτελέστηκε η επίθεση TCP SYN flood με την εντολή,

```
hping3 -S -c 10000 -p 8160 --flood --rand-source [Target IP Address]
```

Οι παράμετροι της εντολής παρουσιάζονται αναλυτικά στον Πίνακας 4.

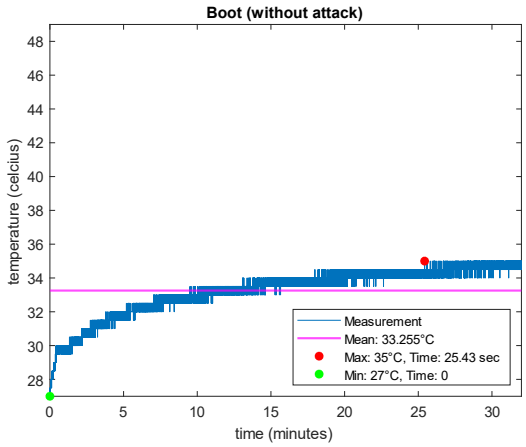
Πίνακας 4: Παράμετροι εντολής TCP SYN flood επίθεσης.

ΠΑΡΑΜΕΤΡΟΙ	ΕΝΝΟΙΑ
-S	Καθορίζει τα πακέτα που στέλνονται να είναι πακέτα συγχρονισμού.
-c	Καθορίζει το πλήθος των πακέτων που στέλνονται.
-p	Καθορίζει τη θύρα στην οποία θα γίνει η επίθεση.
--flood	Στέλνει τα πακέτα όσο πιο γρήγορα γίνεται.
--rand-source	Θέτει τυχαία διεύθυνση IP αποστολέα.

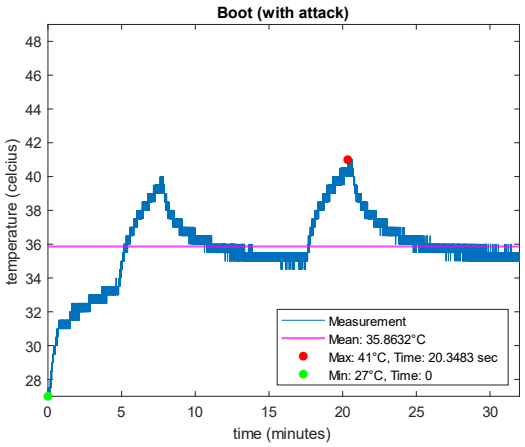
Η επιλογή της επίθεσης TCP SYN flood έγινε με γνώμονα το πρωτόκολλο που χρησιμοποιεί η εντολή `raspivid`, δηλαδή το HTTP. Το πρωτόκολλο HTTP βασίζεται στο πρωτόκολλο TCP για τη μεταφορά των δεδομένων, συνεπώς οι επιθέσεις που απευθύνονται σε αυτό το πρωτόκολλο αναμένεται να προκαλέσουν μεγαλύτερο αντίκτυπο στις επιδόσεις του συστήματος.

Τα διαγράμματα των μεταβολών της θερμοκρασίας από την πειραματική αξιολόγηση εξάχθηκαν μέσω του λογισμικού MATLAB (Παράρτημα Γ: Κώδικες Matlab, I, σελ.59). Κάθε μελέτη περίπτωσης αντιστοιχεί σε ξεχωριστό αρχείο καταγραφής, το οποίο δίνεται ως είσοδος στο σενάριο γραφικής απεικόνισης MATLAB. Κάθε

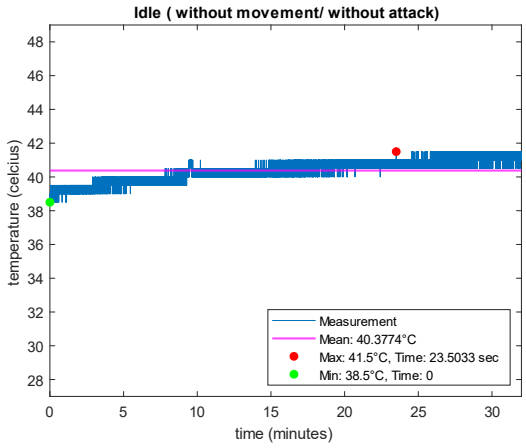
διάγραμμα αποτελεί μια χρονοσειρά των τιμών θερμοκρασίας για διάστημα 32 λεπτών, ενώ στο καθένα απεικονίζονται η μέση, η μέγιστη και η ελάχιστη τιμή θερμοκρασίας.



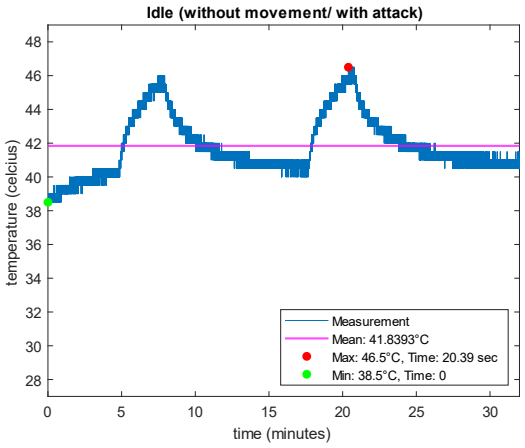
Εικόνα 14: Boot without attack



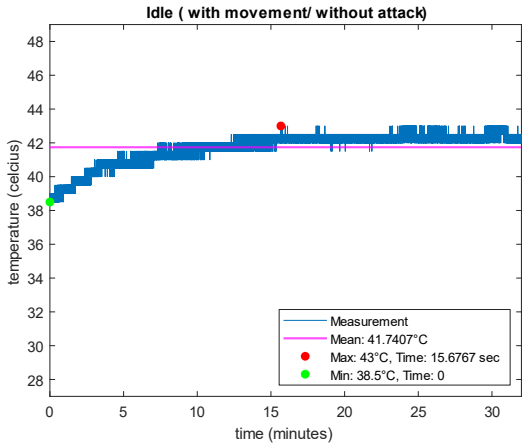
Εικόνα 15: Boot with attack



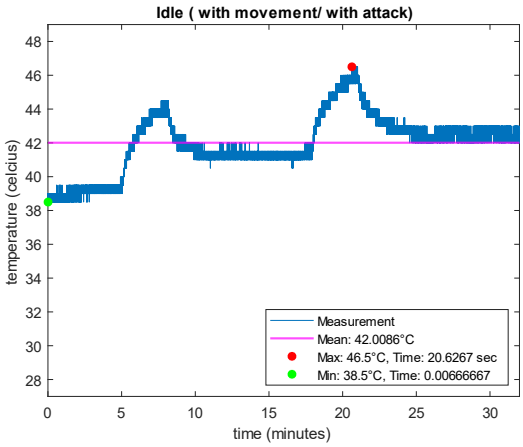
Εικόνα 16: Idle without movement, without attack



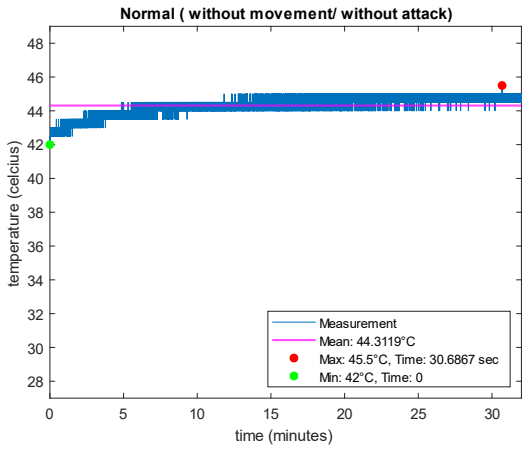
Εικόνα 17: Idle without movement, with attack



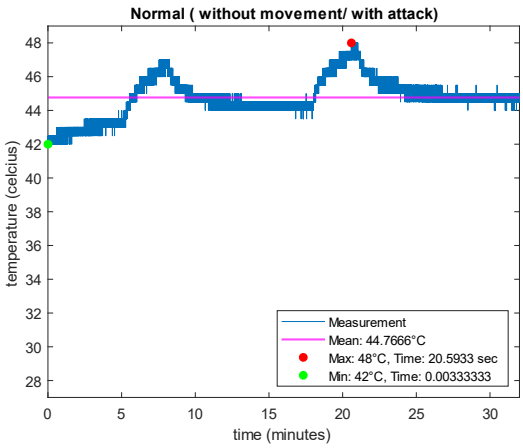
Εικόνα 18: Idle with movement, without attack



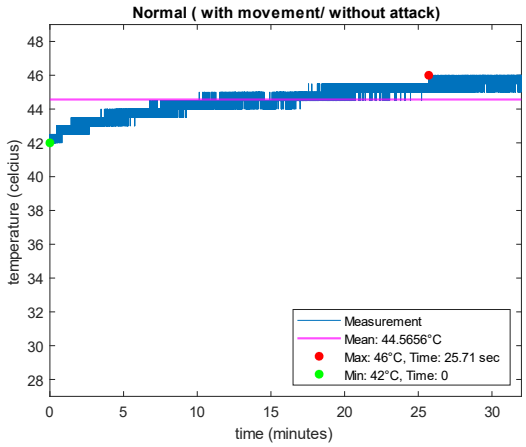
Εικόνα 19: Idle with movement, with attack



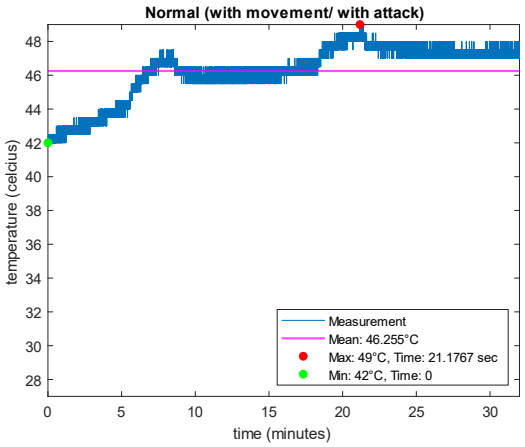
Εικόνα 20: Normal without movement, without attack



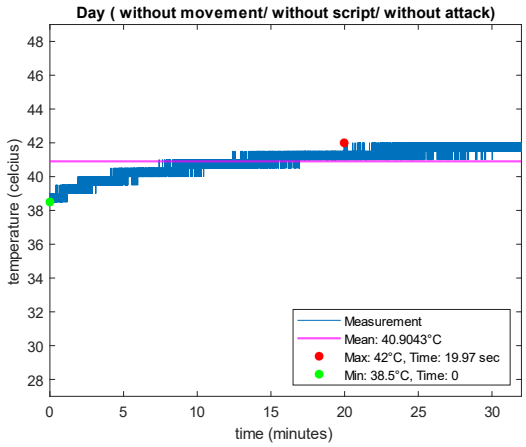
Εικόνα 21: Normal without movement, with attack



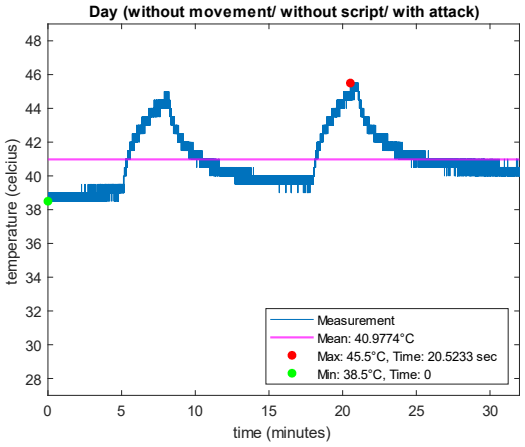
Εικόνα 22: Normal with movement, without attack



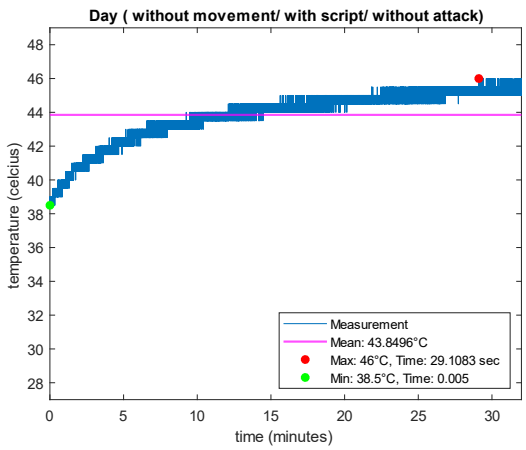
Εικόνα 23: Normal with movement, with attack



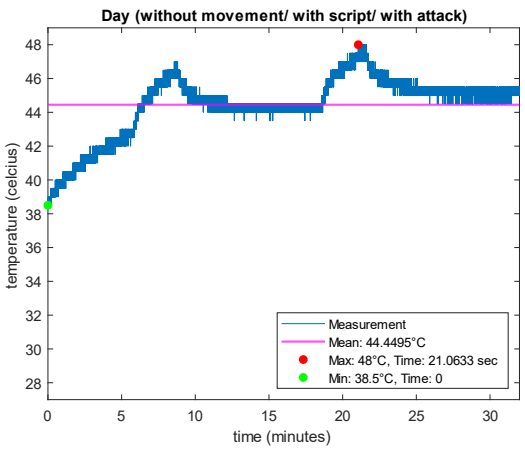
Εικόνα 24: Day without movement, without script, without attack



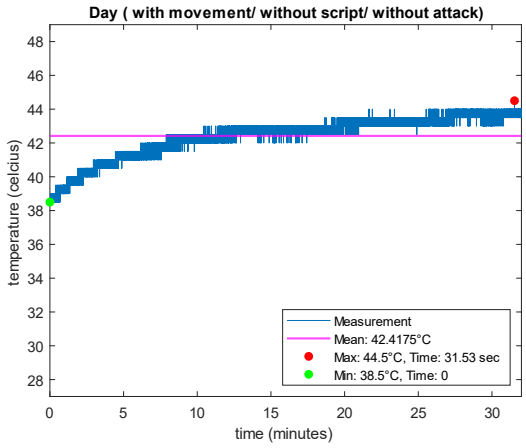
Εικόνα 25: Day without movement, without script, with attack



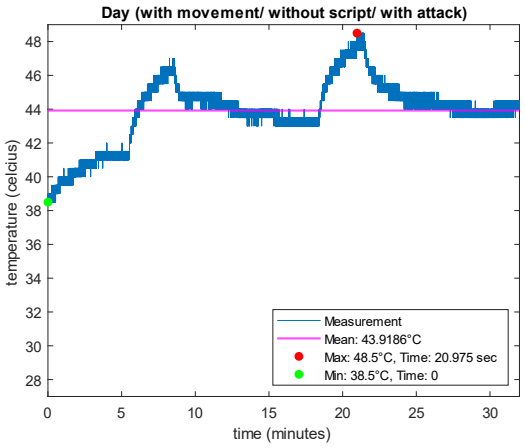
Εικόνα 26: Day without movement, with script, without attack



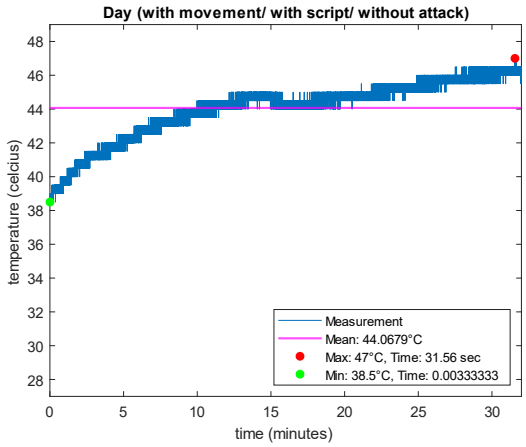
Εικόνα 27: Day without movement, with script, with attack



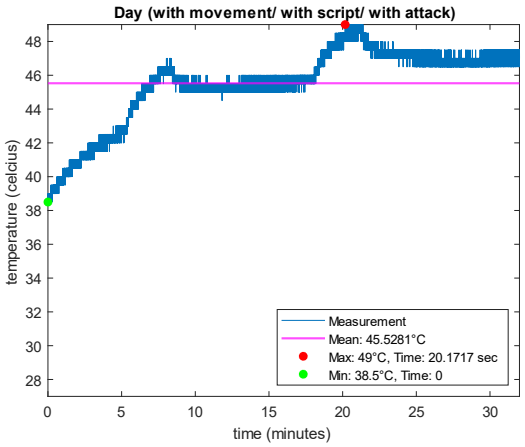
Εικόνα 28: Day with movement, without script, without attack



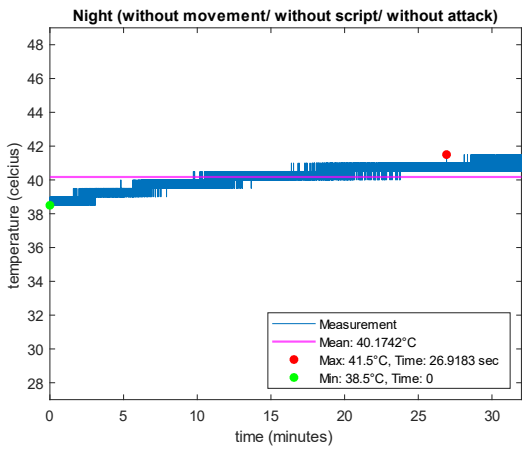
Εικόνα 29: Day with movement, without script, with attack



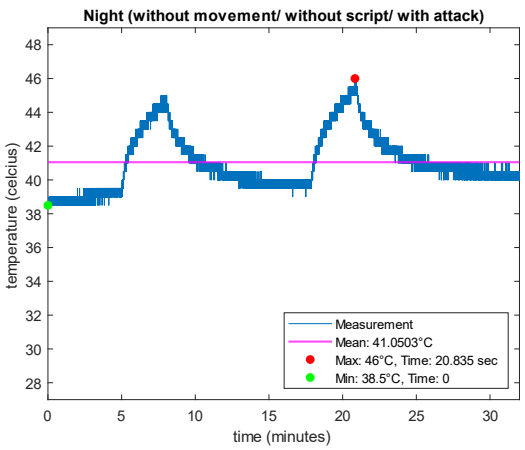
Εικόνα 30: Day with movement, with script, without attack



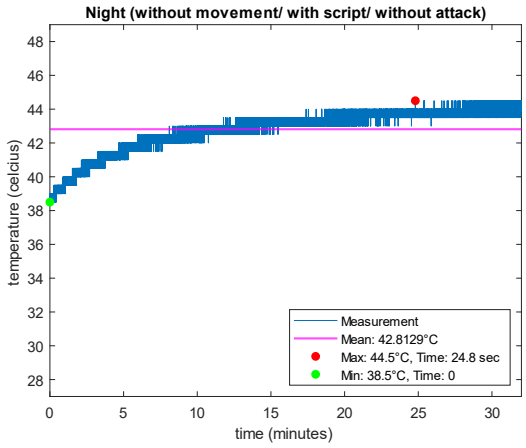
Εικόνα 31: Day with movement, with script, with attack



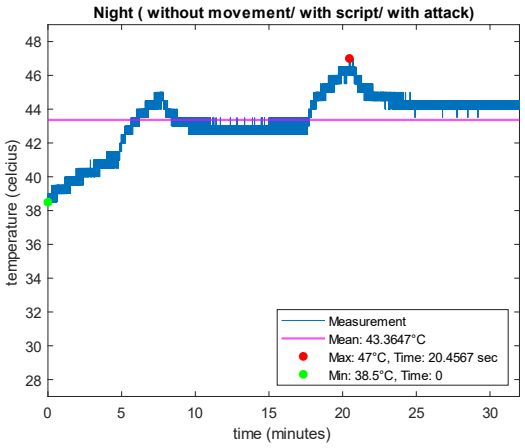
Εικόνα 32: Night without movement, without script, without attack



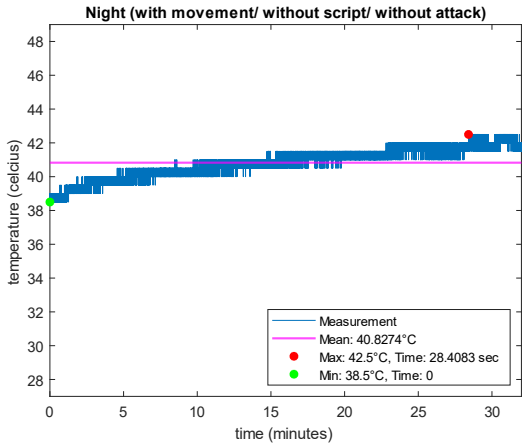
Εικόνα 33: Night without movement, without script, with attack



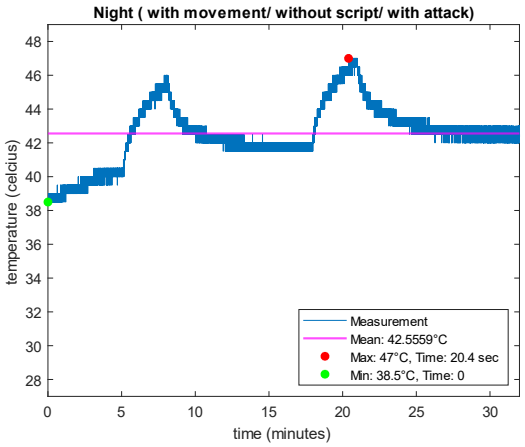
Εικόνα 34: Night without movement, with script, without attack



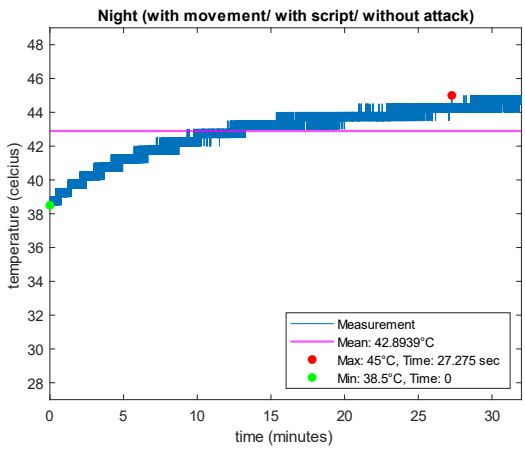
Εικόνα 35: Night without movement, with script, with attack



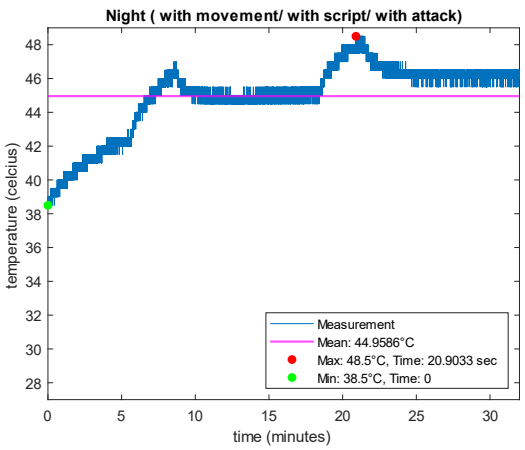
Εικόνα 36: Night with movement, without script, without attack



Εικόνα 37: Night with movement, without script, with attack



Εικόνα 38: Night with movement, with script, without attack



Εικόνα 39: Night with movement, with script, with attack

Για την μελέτη τον διαγραμμάτων θα υπολογίσουμε τον ρυθμό μεταβολής θερμοκρασίας (1) και την ποσοστιαία μεταβολή (2).

$$\frac{d\Theta(t)}{dt} = \frac{\Theta_{max} - \Theta_{min}}{t_{max} - t_{min}}, \quad (1)$$

$$\frac{\Theta_{max} - \Theta_{min}}{\Theta_{min}} * 100, \quad (2)$$

όπου, Θ_{max} η μέγιστη θερμοκρασία στο διάγραμμα, Θ_{min} η ελάχιστη θερμοκρασία, t_{max} ο χρόνος λήψης της μέγιστης θερμοκρασίας και t_{min} ο χρόνος λήψης της ελάχιστης θερμοκρασίας.

Πίνακας 5: Αποτελέσματα υπολογισμού ρυθμού μεταβολής και ποσοστιαίας μεταβολής για κάθε διάγραμμα.

ΕΙΚΟΝΑ	ΡΥΘΜΟΣ ΜΕΤΑΒΟΛΗΣ	ΠΟΣΟΣΤΙΑΙΑ ΜΕΤΑΒΟΛΗ
Εικόνα 14	≈ 0.314	29.629 %
Εικόνα 15	≈ 0.688	51.851 %

Εικόνα 16	≈ 0.127	7.792 %
Εικόνα 17	≈ 0.392	20.779 %
Εικόνα 18	≈ 0.287	11.688 %
Εικόνα 19	≈ 0.387	20.779 %
Εικόνα 20	≈ 0.114	8.333 %
Εικόνα 21	≈ 0.291	14.285 %
Εικόνα 22	≈ 0.155	9.523 %
Εικόνα 23	≈ 0.330	16.666 %
Εικόνα 24	≈ 0.175	9.090 %
Εικόνα 25	≈ 0.341	18.181 %
Εικόνα 26	≈ 0.257	19.480 %
Εικόνα 27	≈ 0.451	24.675 %
Εικόνα 28	≈ 0.190	15.584 %
Εικόνα 29	≈ 0.476	25.974 %
Εικόνα 30	≈ 0.269	22.077 %
Εικόνα 31	≈ 0.520	27.272 %
Εικόνα 32	≈ 0.111	7.792 %
Εικόνα 33	≈ 0.359	19.480 %
Εικόνα 34	≈ 0.241	15.584 %
Εικόνα 35	≈ 0.415	22.077 %
Εικόνα 36	≈ 0.140	10.389 %
Εικόνα 37	≈ 0.416	22.077 %

Εικόνα 38	≈ 0.238	16.883 %
Εικόνα 39	≈ 0.478	25.974 %

4.5.1. Αξιολόγηση μετρήσεων περίπτωσης εκκίνησης συστήματος

Κατά τη διάρκεια εκκίνησης, δίχως την εκτέλεση κάποιας επίθεσης (Εικόνα 14), μπορούμε να δούμε πως η ελάχιστη τιμή θερμοκρασίας βρέθηκε να είναι οι 27°C, η μέγιστη τιμή θερμοκρασίας βρέθηκε στους 35°C, ενώ η μέση τιμή θερμοκρασίας ορίστηκε στους 33.255°C. Η μέγιστη θερμοκρασία επετεύχθη μετά από 25.43 λεπτά λειτουργίας, ορίζοντας έτσι τον ρυθμό μεταβολής της θερμοκρασίας στην τιμή 0.314°C ανά λεπτό. Η μέγιστη ποσοστιαία μεταβολή θερμοκρασίας από όλο το διάγραμμα υπολογίστηκε στο 29.63%. Στην ίδια κατάσταση, όταν εκτελείται επίθεση (Εικόνα 15), έχουμε ελάχιστη τιμή θερμοκρασίας στους 27°C, ίδια με την ελάχιστη τιμή στην περίπτωση χωρίς επίθεση. Η πρώτη επίθεση εκτελείται μετά από 5 λεπτά λειτουργίας του συστήματος και διαρκεί τρία λεπτά. Η μεγαλύτερη τιμή θερμοκρασίας που επιτυγχάνεται κατά τη διάρκεια της πρώτης επίθεσης είναι 40°C. Η μέγιστη τιμή θερμοκρασίας επιτυγχάνεται στη δεύτερη επίθεση, η οποία αρχίζει 10 λεπτά μετά την ολοκλήρωση της πρώτης, και έχει τιμή 41°C. Μετρώντας από την αρχή του διαγράμματος, η μέγιστη θερμοκρασία επετεύχθη μετά από 20.3483 λεπτά. Ο ρυθμός μεταβολής, λαμβάνοντας υπόψη την ελάχιστη και μέγιστη θερμοκρασία, βρέθηκε 0.688°C ανά λεπτό. Ο ρυθμός μεταβολής με επίθεση είναι σαφώς μεγαλύτερος από τον ρυθμό μεταβολής χωρίς επίθεση. Η μέση τιμή θερμοκρασίας του διαγράμματος υπολογίστηκε στους 35.8632°C, ενώ κατά την ολοκλήρωση των επιθέσεων, η θερμοκρασία της συσκευής σταθεροποιείται λίγο πιο κάτω από την μέση τιμή, μεταξύ των θερμοκρασιών 35°C και 35.5°C. Η μέγιστη ποσοστιαία μεταβολή από όλο το διάγραμμα ορίστηκε στο 51.85%, γεγονός που οφείλεται στη συνεχή αύξηση της θερμοκρασία κατά τη διάρκεια εκκίνησης της συσκευής μέχρι να σταθεροποιηθεί, και παράλληλα η εκτέλεση της επίθεσης ανεβάζει τη μέση θερμοκρασία.

4.5.2. Αξιολόγηση μετρήσεων περίπτωσης αδράνειας συστήματος

Στην κατάσταση αδράνειας (idle) έχουμε τέσσερεις διαφορετικές περιπτώσεις.

1. Αδρανής χωρίς κίνηση και χωρίς επίθεση
2. Αδρανής χωρίς κίνηση με επίθεση
3. Αδρανής με κίνηση χωρίς επίθεση
4. Αδρανής με κίνηση και επίθεση

Στην πρώτη υποπερίπτωση (Εικόνα 16), η ελάχιστη τιμή θερμοκρασίας υπολογίζεται στους 38.5°C, ενώ η μέγιστη θερμοκρασία υπολογίζεται στους 41.5°C μετά από 23.5 λεπτά λειτουργίας. Η μέση τιμή θερμοκρασίας ορίστηκε στους 40.3774°C. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.127°C ανά λεπτό. Η μέγιστη ποσοστιαία μεταβολή βρέθηκε στο 7.79%, καθώς κατά την υποπερίπτωση αυτή, δεν υπάρχει καμία αύξηση θερμοκρασίας λόγω κίνησης ή επίθεσης, εφόσον η κάμερα καταγράφει στατικές εικόνες. Στην δεύτερη υποπερίπτωση (Εικόνα 17) έχουμε επίθεση αλλά δεν έχουμε κίνηση, επομένως η κάμερα συνεχίζει να καταγράφει στατικές εικόνες. Η ελάχιστη τιμή θερμοκρασίας βρέθηκε στους 38.5°C, ενώ η μέγιστη βρέθηκε μετά από 20.39 λεπτά στους 46.5°C. Η μέση τιμή θερμοκρασίας ορίστηκε στους 41.8393°C, ενώ ο ρυθμός μεταβολής υπολογίστηκε στους 0.392°C ανά λεπτό. Εύλογο είναι πως ο ρυθμός μεταβολής βρέθηκε μεγαλύτερος του ρυθμού μεταβολής της πρώτης υποπερίπτωσης, καθώς η ύπαρξη επίθεσης ανεβάζει την θερμοκρασία. Η μέγιστη ποσοστιαία μεταβολή υπολογίστηκε στο 20.78%. Μετά την ολοκλήρωση της επίθεσης η θερμοκρασία σταθεροποιείται κοντά στη μέση τιμή και συγκεκριμένα μεταξύ των θερμοκρασιών 40.5°C και 41°C. Η μέγιστη τιμή θερμοκρασίας βρέθηκε κατά τη διάρκεια της δεύτερης επίθεσης, η οποία ξεκίνησε 10 λεπτά μετά την ολοκλήρωση της πρώτης επίθεσης.

Στην τρίτη υποπερίπτωση (Εικόνα 18), η ελάχιστη τιμή θερμοκρασίας βρέθηκε στους 38.5°C και η μέγιστη στους 43°C. Η μέση τιμή θερμοκρασίας υπολογίστηκε στους 41.74°C, ενώ ο ρυθμός μεταβολής στους 0.287°C ανά λεπτό. Η αύξηση της θερμοκρασίας σε σχέση με την πρώτη υποπερίπτωση οφείλεται στην ύπαρξη κίνησης στη συνεχή ροή εικόνων, ενώ δεν ξεπερνά την αύξηση που οφείλεται στην ύπαρξη επίθεσης. Η μέγιστη ποσοστιαία μεταβολή στο διάγραμμα υπολογίζεται στο 11.69%, μικρότερη από την μέγιστη ποσοστιαία μεταβολή στην δεύτερη υποπερίπτωση. Από

αυτό μπορούμε να συμπεράνουμε πως η ύπαρξη κίνησης δεν οδηγεί σε τόσο μεγάλη αύξηση θερμοκρασίας, όσο με την ύπαρξη επίθεσης. Συνεπώς, είναι αναμενόμενο πως στην τέταρτη υποπερίπτωση (Εικόνα 19) οι τιμές θερμοκρασίας θα ακολουθούν περισσότερο τις αλλαγές που οφείλονται σε επίθεση, παρά σε κίνηση. Η ελάχιστη τιμή θερμοκρασίας στο διάγραμμα βρέθηκε στους 38.5°C, ίδια με κάθε προηγούμενη υποπερίπτωση, ενώ η μέγιστη τιμή θερμοκρασίας εκδηλώθηκε μετά από 20.6 λεπτά, με τιμή 46.5°C, ίδια με την μέγιστη τιμή της δεύτερης υποπερίπτωσης. Η μέση τιμή θερμοκρασίας είναι ίση με 42°C, ενώ ο ρυθμός μεταβολής είναι 0.387°C ανά λεπτό, σχεδόν ίσος με τον ρυθμό της δεύτερης υποπερίπτωσης. Ενδιαφέρον παρουσιάζει η μέγιστη ποσοστιαία μεταβολή, η οποία είναι ίση με την μέγιστη ποσοστιαία μεταβολή της δεύτερης υποπερίπτωσης, επαληθεύοντας την υπόθεση μας πως η τέταρτη υποπερίπτωση ακολουθεί περισσότερο τις αλλαγές θερμοκρασίας που οφείλονται σε επίθεση παρά σε κίνηση.

4.5.3. Αξιολόγηση μετρήσεων περίπτωσης κανονικής λειτουργίας συστήματος

Στην κατάσταση κανονικής λειτουργίας έχουμε τέσσερεις συνδυασμούς.

1. Κανονική λειτουργία χωρίς κίνηση και χωρίς επίθεση
2. Κανονική λειτουργία χωρίς κίνηση με επίθεση
3. Κανονική λειτουργία με κίνηση χωρίς επίθεση
4. Κανονική λειτουργία με κίνηση και επίθεση

Σε κάθε υποπερίπτωση εκτελείται ταυτόχρονα ένα σενάριο κελύφους (βλ. Παράρτημα Β: Σενάρια κελύφους Raspberry Pi, I, σελ. 58). Η εκτέλεση του σεναρίου προσδίδει αύξηση στην θερμοκρασία της CPU. Για την πρώτη υποπερίπτωση, όπου έχουμε κανονική λειτουργία χωρίς κίνηση και χωρίς επίθεση (Εικόνα 20), έχουμε ελάχιστη τιμή θερμοκρασίας τους 42°C, μέγιστη τους 45.5°C μετά από 30.69 λεπτά λειτουργίας, και μέση τιμή θερμοκρασίας τους 44.31°C. Ο ρυθμός μεταβολής της θερμοκρασίας υπολογίστηκε στους 0.114°C ανά λεπτό, ενώ η μέγιστη ποσοστιαία μεταβολή θερμοκρασίας βρέθηκε ως 8.333%. Παρατηρούμε ότι η υποπερίπτωση αυτή μοιάζει με την πρώτη υποπερίπτωση στην κατάσταση αδράνειας, όπου ο ρυθμός μεταβολής είναι ιδιαίτερα χαμηλός, και η μέγιστη ποσοστιαία μεταβολή είναι στο

7.79%. Η αύξηση στην μέγιστη ποσοστιαία μεταβολή μεταξύ των δύο υποπεριπτώσεων οφείλεται στην εκτέλεση σεναρίου κελύφους στο παρασκήνιο, το οποίο συμμετέχει αυξητικά στην θερμοκρασία. Για την δεύτερη υποπερίπτωση (Εικόνα 21), όπου έχουμε επίθεση χωρίς κίνηση, η ελάχιστη θερμοκρασία έφτασε τους 42°C, ενώ η μέγιστη έφτασε στους 48°C. Η μέση τιμή θερμοκρασίας ορίστηκε στους 44.77°C, ενώ ο ρυθμός μεταβολής υπολογίστηκε στους 0.291°C ανά λεπτό. Παρατηρούμε αύξηση τόσο στη μέση θερμοκρασία, όσο και στο ρυθμό μεταβολής, το οποίο είναι λογικό λόγω της επίθεσης. Ειδικά, η μέγιστη ποσοστιαία μεταβολή υπολογίστηκε στο 14.285%, αρκετά μεγαλύτερη από την αντίστοιχη στην πρώτη υποπερίπτωση. Με την ολοκλήρωση της επίθεσης, η θερμοκρασία σταθεροποιείται γύρω από την μέση τιμή, στο εύρος θερμοκρασιών από 44.5°C μέχρι 45°C.

Στην τρίτη υποπερίπτωση (Εικόνα 22) έχουμε ύπαρξη κίνησης χωρίς όμως εκτέλεση επίθεσης στη συσκευή. Παρατηρούμε πως το διάγραμμα μοιάζει σχηματικά με την πρώτη υποπερίπτωση, απλά με αυξημένες τιμές θερμοκρασίας. Συγκεκριμένα έχουμε ελάχιστη τιμή θερμοκρασίας 42°C, μέγιστη 46°C μετά από 25.7 λεπτά λειτουργίας και μέση τιμή θερμοκρασίας στους 44.56°C. Ιδιαίτερο ενδιαφέρον παρουσιάζει η τιμή της μέσης θερμοκρασίας, η οποία είναι ελάχιστα μεγαλύτερη από την πρώτη υποπερίπτωση, 44.31°C, και μικρότερη από την δεύτερη υποπερίπτωση, 44.77°C. Η μέγιστη ποσοστιαία μεταβολή στην τρίτη υποπερίπτωση υπολογίστηκε στο 9.523%, αρκετά μικρότερη από την δεύτερη υποπερίπτωση, αλλά πολύ κοντά στην πρώτη υποπερίπτωση. Το ίδιο συμπέρασμα εξάγεται και για τον ρυθμό μεταβολής, ο οποίος υπολογίστηκε στους 0.155°C ανά λεπτό. Στην τέταρτη υποπερίπτωση (Εικόνα 23) έχουμε συνδυασμό και επίθεσης και κίνησης, όπου αναμένεται να εμφανίσει τις μεγαλύτερες τιμές. Όντως, η ελάχιστη και η μέγιστη τιμή θερμοκρασίας βρέθηκαν 42°C και 49°C αντίστοιχα, ενώ η μέση τιμή θερμοκρασίας έχει αυξηθεί σημαντικά στους 46.255°C. Ο ρυθμός μεταβολής της θερμοκρασίας υπολογίστηκε στους 0.330°C ανά λεπτό, ενώ η μέγιστη ποσοστιαία μεταβολή υπολογίστηκε στο 16.67%. Συνεπώς, επαληθεύεται ο υπαινιγμός μας, πως η υποπερίπτωση αυτή θα σημειώσει τις μεγαλύτερες τιμές θερμοκρασίας σε σχέση με τις υπόλοιπες. Κύριο ρόλο στην αύξηση της θερμοκρασίας παρατηρούμε πως κατέχει η ύπαρξη ή όχι επίθεσης, σε αντίθεση με τις μικρές αυξήσεις που προκαλούνται από την ύπαρξη κίνησης.

4.5.4. Αξιολόγηση μετρήσεων κατά τη διάρκεια της ημέρας

Για την αξιολόγηση των μετρήσεων που πάρθηκαν κατά τη διάρκεια της ημέρες διακρίνονται 8 διαφορετικές υποπεριπτώσεις.

1. Χωρίς κίνηση, χωρίς σενάριο κελύφους και χωρίς επίθεση
2. Χωρίς κίνηση, χωρίς σενάριο κελύφους και με επίθεση
3. Χωρίς κίνηση, με σενάριο κελύφους και χωρίς επίθεση
4. Χωρίς κίνηση, με σενάριο κελύφους και με επίθεση
5. Με κίνηση, χωρίς σενάριο κελύφους και χωρίς επίθεση
6. Με κίνηση, χωρίς σενάριο κελύφους και με επίθεση
7. Με κίνηση, με σενάριο κελύφους και χωρίς επίθεση
8. Με κίνηση, με σενάριο κελύφους και με επίθεση

Σε κάθε διάγραμμα από τις 8 υποπεριπτώσεις, η ελάχιστη θερμοκρασία ήταν πάντα 38.5℃. Στην πρώτη υποπερίπτωση (Εικόνα 24) η μέγιστη θερμοκρασία βρέθηκε στους 42℃, η μέση τιμή θερμοκρασίας στους 40.9℃ ενώ ο ρυθμός μεταβολής της θερμοκρασίας στους 0.175℃ ανά λεπτό. Η μέγιστη ποσοστιαία μεταβολή στο διάγραμμα υπολογίστηκε στο 9.09%. Η δεύτερη υποπερίπτωση (Εικόνα 25) η μέγιστη τιμή θερμοκρασίας βρέθηκε στους 45.5℃ μετά από 20.53 λεπτά λειτουργίας. Η μέση τιμή θερμοκρασίας ορίστηκε στους 40.98℃, ενώ ο ρυθμός μεταβολής υπολογίστηκε στους 0.341℃ ανά λεπτό. Παρατηρούμε πως η ύπαρξη επίθεσης σχεδόν διπλασίασε τον ρυθμό μεταβολής θερμοκρασίας, ενώ το ίδιο συνέβη στη μέγιστη ποσοστιαία μεταβολή, η οποία υπολογίστηκε στο 18.181%.

Η τρίτη υποπερίπτωση (Εικόνα 26) εμφάνισε μέγιστη τιμή θερμοκρασίας στους 46℃ μετά από 29.10 λεπτά και μέση τιμή θερμοκρασίας στους 43.85℃. Ο ρυθμός μεταβολής της θερμοκρασίας ορίστηκε στους 0.257℃ ανά λεπτό, ενώ η μέγιστη ποσοστιαία μεταβολή ορίστηκε στο 19.48%. Ενδιαφέρον εμφανίζει, πως αν και η μέγιστη θερμοκρασία είναι μεγαλύτερη από την ακριβώς προηγούμενη υποπερίπτωση, ο ρυθμός μεταβολής είναι μικρότερος, γεγονός που δηλώνει πως η ύπαρξη επίθεσης ανιχνεύεται καλύτερα μελετώντας τον ρυθμό μεταβολής, παρά την μέγιστη ποσοστιαία μεταβολή. Συνεχίζει επομένως να ισχύει πως η ύπαρξη επίθεσης επιδρά περισσότερο στην θερμοκρασία σε σχέση με την εκτέλεση σεναρίου ή την ύπαρξη κίνησης.Η τέταρτη υποπερίπτωση (Εικόνα 27) αποτελεί συνδυασμό και επίθεσης και εκτέλεσης σεναρίου με μέγιστη τιμή θερμοκρασίας τους 48℃ μετά από

21 λεπτά, και μέση τιμή τους 44.45°C. Ο ρυθμός μεταβολής είναι αναμενόμενα υψηλός, με τιμή 0.451°C ανά λεπτό, ενώ η μέγιστη ποσοστιαία μεταβολή είναι 24.68%.

Στην πέμπτη υποπερίπτωση (Εικόνα 28) έχουμε την ύπαρξη μόνο κίνησης, το οποίο οδηγεί σε μέγιστη θερμοκρασία στους 44.5°C, μέση τιμή 42.175°C και ρυθμό μεταβολής 0.19°C ανά λεπτό. Η μέγιστη ποσοστιαία μεταβολή υπολογίστηκε στο 15.584%. Συγκρίνοντας τις υποπεριπτώσεις που λαμβάνει χώρα μόνο ένα από τα τρία ενδεχόμενα, ο ρυθμός μεταβολής αποδεικνύει για άλλη μια φορά την ταξινόμηση του αντίκτυπου που προκαλεί το κάθε ενδεχόμενο. Συγκεκριμένα, ο ρυθμός μεταβολής μόνο με ύπαρξη κίνησης είναι 0.19°C/λεπτό, μόνο με εκτέλεση σεναρίου είναι 0.257°C/λεπτό και μόνο με εκτέλεση επίθεσης είναι 0.341°C/λεπτό. Στην έκτη υποπερίπτωση (Εικόνα 29) έχουμε μέγιστη τιμή θερμοκρασίας τους 48.5°C μετά από 20.9 λεπτά και μέση τιμή θερμοκρασίας στους 43.92°C. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.476°C ανά λεπτό, και η μέγιστη ποσοστιαία μεταβολή στο 25.974%.

Στην έβδομη υποπερίπτωση (Εικόνα 30) έχουμε τον συνδυασμό των μικρότερων σε μεταβολή θερμοκρασίας ενδεχομένων. Η μέγιστη θερμοκρασία που σημειώνεται είναι οι 47°C, ενώ η μέση τιμή είναι στους 44.1°C. Ο ρυθμός μεταβολής είναι 0.269°C ανά λεπτό και η μέγιστη ποσοστιαία μεταβολή είναι 22.1%. Παρατηρούμε πως για άλλη μια φορά η ύπαρξη κίνησης δεν προκαλεί μεγάλη διαφορά στον ρυθμό μεταβολής της θερμοκρασίας, με την τρίτη υποπερίπτωση να εμφανίζει ρυθμό μεταβολής ίσο με 0.257°C/λεπτό και την παρούσα να έχει 0.269°C/λεπτό. Τέλος, η όγδοη υποπερίπτωση (Εικόνα 31) αποτελεί την μεγαλύτερη περίπτωση μεταβολής θερμοκρασίας καθώς λαμβάνουν χώρα όλα τα ενδεχόμενα. Η μέγιστη τιμή θερμοκρασίας είναι στους 49°C και μέση τιμή θερμοκρασίας 45.53°C. Ο ρυθμός μεταβολής είναι ο μεγαλύτερος με τιμή 0.52°C ανά λεπτό, και η μέγιστη ποσοστιαία μεταβολή 27.272%.

4.5.5. Αξιολόγηση μετρήσεων κατά τη διάρκεια της νύχτας

Για την αξιολόγηση των μετρήσεων που πάρθηκαν κατά τη διάρκεια της νύχτας διακρίνονται 8 διαφορετικές υποπεριπτώσεις.

1. Χωρίς κίνηση, χωρίς σενάριο κελύφους και χωρίς επίθεση
2. Χωρίς κίνηση, χωρίς σενάριο κελύφους και με επίθεση
3. Χωρίς κίνηση, με σενάριο κελύφους και χωρίς επίθεση
4. Χωρίς κίνηση, με σενάριο κελύφους και με επίθεση
5. Με κίνηση, χωρίς σενάριο κελύφους και χωρίς επίθεση
6. Με κίνηση, χωρίς σενάριο κελύφους και με επίθεση
7. Με κίνηση, με σενάριο κελύφους και χωρίς επίθεση
8. Με κίνηση, με σενάριο κελύφους και με επίθεση

Σε όλες τις υποπεριπτώσεις η ελάχιστη τιμή θερμοκρασίας βρέθηκε στους 38.5°C.

Παρατηρώντας όλες τις υποπεριπτώσεις κατά τη διάρκεια της νύχτας σε σχέση με τις αντίστοιχες υποπεριπτώσεις κατά τη διάρκεια της ημέρας, διαπιστώθηκε ότι η έλλειψη φωτός κατά την καταγραφή συνεχούς ροής εικόνας επιδρά αρνητικά στις τιμές θερμοκρασίας.

Η πρώτη υποπερίπτωση (Εικόνα 32) παρουσιάζει μέγιστη τιμή θερμοκρασίας τους 41.5°C και μέση τιμή τους 40.1742°C. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.111°C ανά λεπτό ενώ η μέγιστε ποσοστιαία μεταβολή βρέθηκε 7.79%. Στη δεύτερη υποπερίπτωση (Εικόνα 33) η εκτέλεση επίθεσης προκάλεσε την αύξηση των τιμών θερμοκρασίας. Η μέγιστη θερμοκρασία βρέθηκε στους 46°C και η μέση τιμή στους 41°C. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.359°C ανά λεπτό και η μέγιστη ποσοστιαία μεταβολή βρέθηκε 19.48%. Η εκτέλεση επίθεσης σχεδόν τριπλασίασε τα αποτελέσματα του ρυθμού μεταβολής και της μέγιστης ποσοστιαίας μεταβολής.

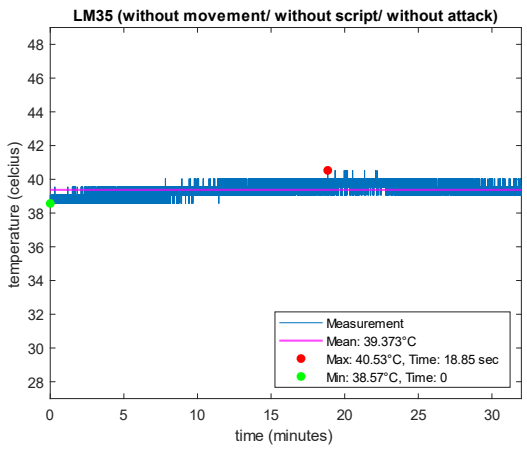
Η τρίτη υποπερίπτωση (Εικόνα 34) παρουσιάζει μέγιστη τιμή θερμοκρασίας τους 44.5°C και μέση τιμή τους 42.81°C. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.241°C ανά λεπτό και η μέγιστη ποσοστιαία μεταβολή βρέθηκε 15.58%. Παρατηρούμε ότι η υποπερίπτωση αυτή παρουσιάζει αύξηση στον ρυθμό μεταβολής και στη μέγιστη ποσοστιαία μεταβολή έναντι της πρώτης υποπερίπτωσης. Αυτό οφείλεται στην εκτέλεση του σεναρίου κελύφους. Στην τέταρτη υποπερίπτωση (Εικόνα 35) η μέγιστη θερμοκρασία βρέθηκε στους 47°C και η μέση τιμή στους 43.365°C. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.415°C ανά λεπτό και η μέγιστη ποσοστιαία μεταβολή βρέθηκε 22.077%.

Η πέμπτη υποπερίπτωση (Εικόνα 36) παρουσιάζει μέγιστη τιμή θερμοκρασίας τους 42.5°C και μέση τιμή τους 40.83°C. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.140°C ανά λεπτό ενώ η μέγιστη ποσοστιαία μεταβολή βρέθηκε 10.39%. Συγκρίνοντας την τρίτη υποπερίπτωση με την πέμπτη παρατηρούμε ότι, η εκτέλεση του σεναρίου κελύφους επιδρά περισσότερο στην μεταβολή της θερμοκρασίας από την κίνηση κατά την καταγραφή της συνεχούς ροής εικόνας. Στην έκτη υποπερίπτωση (Εικόνα 37) η μέγιστη τιμή θερμοκρασίας και η μέση τιμή βρέθηκαν στους 47°C και 42.556°C αντίστοιχα. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.416°C ανά λεπτό και η μέγιστη ποσοστιαία μεταβολή βρέθηκε 22.077%. Μεταξύ των υποπεριπτώσεων τέσσερα και έξη, παρουσιάζεται ταύτιση αποτελεσμάτων του ρυθμού μεταβολής και της μέγιστης ποσοστιαίας μεταβολής που οφείλεται στην εκτέλεση επίθεσης.

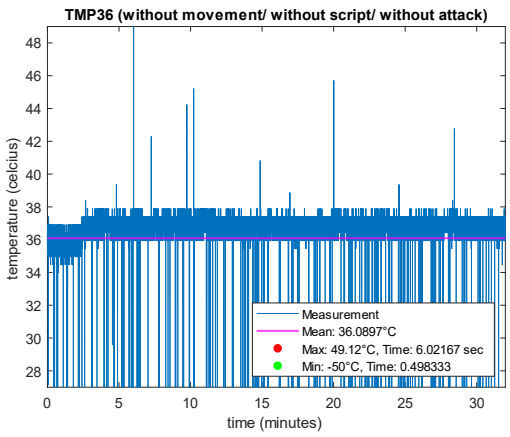
Η έβδομη υποπερίπτωση (Εικόνα 38) παρουσιάζει μέγιστη τιμή θερμοκρασίας τους 45°C και μέση τιμή τους 42.894°C. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.238°C ανά λεπτό και η μέγιστη ποσοστιαία μεταβολή βρέθηκε 16.88%. Στην αντίστοιχη υποπερίπτωση με επίθεση (Εικόνα 39) η μέγιστη τιμή θερμοκρασίας βρέθηκε στους 48.5°C και η μέση τιμή στους 44.96°C. Ο ρυθμός μεταβολής υπολογίστηκε στους 0.478°C ανά λεπτό και η μέγιστη ποσοστιαία μεταβολή βρέθηκε 25.974%. Όπως αναμένεται, η τελευταία υποπερίπτωση εμφανίζει τις μεγαλύτερες τιμές, τόσο στον ρυθμό μεταβολής όσο και στην μέγιστη ποσοστιαία μεταβολή, καθώς λαμβάνουν χώρα όλα τα ενδεχόμενα.

4.5.6. Εναλλακτικοί αισθητήρες θερμοκρασίας

Η απόφαση να χρησιμοποιηθεί ο αισθητήρας θερμοκρασίας MCP9808 στην παρούσα υλοποίηση έναντι των εναλλακτικών αισθητήρων LM35 και TMP36, πάρθηκε σύμφωνα με τα αποτελέσματα των παρακάτω μετρήσεων σε κατάσταση αδράνειας χωρίς κίνηση, χωρίς την εκτέλεση σεναρίου κελύφους και χωρίς την εκτέλεση επίθεσης κατά τη συνεχή ροή εικόνας (Εικόνα 16).



Εικόνα 40: Idle without movement, without script, without attack, with temperature sensor LM35



Εικόνα 41: Idle without movement, without script, without attack, with temperature sensor TMP36

Παρατηρώντας το διάγραμμα για την περίπτωση χρήσης του αισθητήρα LM35 (Εικόνα 40) μπορούμε να αποφανθούμε πως ο αισθητήρας αδυνατεί να παρουσιάσει ακριβείς μετρήσεις θερμοκρασίας. Συγκεκριμένα βλέπουμε πως η μεταβολές της θερμοκρασίας κατά την διάρκεια λειτουργίας των 32 λεπτών είναι αρκετά μικρές. Χειρότερα είναι τα αποτελέσματα καταγραφής για τον αισθητήρα TMP36 (Εικόνα 41), όπου φαίνονται ακόμα και αρνητικές τιμές, κάτι που δεν αντιστοιχεί στην πραγματικότητα. Σε όλη την διάρκεια μέτρησης μπορούμε να δούμε πως στην καταγραφή εμφανίζεται περιβαλλοντικός θόρυβος. Ο λόγος που και οι δύο αισθητήρες δεν είναι ικανοί να ανιχνεύσουν τις αλλαγές θερμοκρασίας της CPU του Raspberry, καθώς μετρούν την θερμοκρασία δωματίου (ambient temperature). Σε αντίθεση με αυτούς, ο αισθητήρας MCP9808 δύναται να μετρήσει την θερμοκρασίας της CPU εξ επαφής, επιτρέποντας την καταγραφή αλλαγών στην θερμοκρασία με μεγαλύτερη ακρίβεια.

4.5.7 Εναλλακτικές επιθέσεις

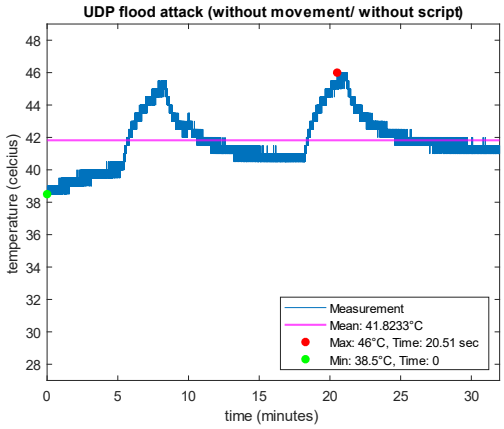
Κατά την πειραματική αξιολόγηση του συστήματος εκτός από την TCP SYN flood επίθεση, δοκιμάστηκαν και οι επιθέσεις UDP flood και SMURF. Τα αποτελέσματα της καταγραφής φαίνονται στα παρακάτω διαγράμματα, τα οποία πάρθηκαν σε κατάσταση αδράνειας χωρίς κίνηση κατά τη συνεχή ροή εικόνας. Για την επίθεση UDP flood η εντολή είναι η εξής

```
hping3 -2 -c 10000 -p 8160 --flood --rand-source [Target IP Address]
```

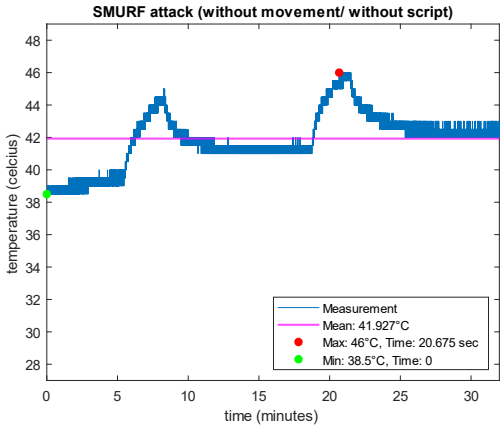
Η παράμετρος "-2" καθορίζει ότι η επίθεση θα πραγματοποιηθεί σε θύρα του πρωτοκόλλου UDP. Ενώ η εντολή για την επίθεση SMURF συντάσσεται ως

```
hping3 --icmp --flood [Target IP Address] -a [Source IP Address]
```

Η παράμετρος "--icmp" καθορίζει ότι τα πακέτα που θα στέλνονται θα είναι πακέτα ICMP Echo και η παράμετρος "-a" παραποιεί την διεύθυνση IP του αποστολέα σε αυτή που θα ορίσει ο επιτιθέμενος.



Εικόνα 42: Idle without movement, with UDP flood attack



Εικόνα 43: Idle without movement, with SMURF attack

Από παρατήρηση των διαγραμμάτων θερμοκρασίας των εναλλακτικών επιθέσεων, μπορούμε να δούμε πως υπάρχει διαφορά κατά 0.5°C συγκριτικά με την επίθεση TCP SYN flood (Εικόνα 17). Η διαφορά αυτή οφείλεται στο γεγονός πως η μεταφορά των δεδομένων συνεχούς ροής εικόνας από την κάμερα χρησιμοποιεί το πρωτόκολλο HTTP, το οποίο βασίζεται στο πρωτόκολλο TCP. Ως εκ τούτου, οι επιθέσεις που στοχεύουν σε θύρες πρωτοκόλλου TCP, είναι αναμενόμενο να προκαλέσουν μεγαλύτερες επιπτώσεις, από επιθέσεις που στοχεύουν σε άλλα πρωτόκολλα.

Κεφάλαιο 5. Συμπεράσματα

Ο αυξανόμενος αριθμός των συσκευών IoT οδηγεί στην ανάγκη προστασίας τους από κάθε είδους κυβερνητικών επιθέσεων, που έχουν ως στόχο την διατάραξη της ομαλής λειτουργίας τους. Καθήκον των συστημάτων παρακολούθησης φυσικών χαρακτηριστικών είναι η έγκαιρη ανίχνευση επιθέσεων σε συσκευές IoT, για την ελαχιστοποίηση των επιπτώσεων στην ποιότητα της παρεχόμενης υπηρεσίας και στην ιδιωτικότητα των χρηστών. Το προτεινόμενο σύστημα παρακολούθησης φυσικών χαρακτηριστικών διερευνά την δυνατότητα ανίχνευσης επιθέσεων με βάση την μετρούμενη θερμοκρασία της CPU της συσκευής IoT. Ως συσκευή IoT κατασκευάζεται μια IP Camera, ενώ η λήψη των μετρήσεων γίνεται με τη χρήση αισθητήρα θερμοκρασίας υψηλής ακρίβειας και τον μικροελεγκτή Arduino UNO. Το προτεινόμενο σύστημα αξιολογήθηκε με βάση πολλαπλά σενάρια λειτουργίας, χρήση εναλλακτικών αισθητήρων θερμοκρασίας και απόκριση σε διαφορετικά είδη επιθέσεων.

Από την πειραματική αξιολόγηση συμπεράθηκε ότι, η θερμοκρασία αποτελεί ικανό μέτρο για την ανίχνευση επιθέσεων σε συσκευές IoT, με τον ρυθμό μεταβολής θερμοκρασίας να παρέχει επαρκή πληροφορία για την ύπαρξη ή όχι επίθεσης. Στα πλαίσια της αρχής λειτουργίας της κάμερας IP, παρατηρήθηκε πως ο φωτισμός του περιβάλλοντος επιδρά ελάχιστα στη θερμοκρασία, με υψηλότερες τιμές φωτεινότητας να οδηγούν σε ελαφρώς αυξημένα επίπεδα θερμοκρασίας, συγκριτικά με τα αντίστοιχα επίπεδα σε περίπτωση συσκότισης. Η ύπαρξη ή όχι κίνησης στη ροή εικόνων της κάμερας δεν οδηγεί σε σημαντικές μεταβολές θερμοκρασίας, γεγονός που επαληθεύεται από τις αντίστοιχες τιμές του ρυθμού μεταβολής. Αντίστοιχα συμπεράσματα λαμβάνονται και για την μεταβολή της θερμοκρασίας που οφείλεται σε εκτέλεση σεναρίων κελύφους στο παρασκήνιο της συσκευής. Συλλογικά, παρατηρούμε πως η ύπαρξη επίθεσης οδηγεί και σε μεγαλύτερες τιμές του ρυθμού μεταβολής θερμοκρασίας.

Με την ολοκλήρωση της παρούσας πτυχιακής εργασίας, μελετήσαμε τον χώρο του IoT, την αρχιτεκτονική του και τις τεχνολογίες που επιτρέπουν την ανάπτυξή του. Μελετήσαμε τον χώρο των συστημάτων ανίχνευσης εισβολών, αλλά και τα διάφορα ζητήματα ασφαλείας που διέπουν το Διαδίκτυο των Πραγμάτων. Προτείναμε ένα σύστημα ανίχνευσης επιθέσεων με βάση την θερμοκρασίας της CPU, το υλοποιήσαμε

και αξιολογήσαμε την λειτουργία του. Από την αξιολόγηση αντλήσαμε συμπεράσματα για την ιδανικότητα της θερμοκρασίας ως μέτρο ανίχνευσης επιθέσεων.

Βιβλιογραφία

[1] M. R. Kadri, A. Abdelli και J. B. Othman, «Survey and classification of Dos and DDos attack detection and validation approaches for IoT environments,» *Internet of Things,* τόμ. 25, 2024.

[2] A. Berguiga και A. Harchay, «An IoT-Based Intrusion Detection System Approach for TCP SYN Attacks,» *Computers, Materials & Continua,* τόμ. 71, αρ. 2, pp. 3839-3851, 2022.

[3] M. Roopak, G. Y. Tian και J. Chambers, «An Intrusion Detection System Against DDoS Attacks in IoT Networks,» σε *2020 10th Annual Computing and Communication Workshop and Conference (CCWC),* Las Vegas, NV, USA, 2020.

[4] M. Shurman, R. Khrais και A. Yateem, «DoS and DDoS Attack Detection Using Deep Learning and IDS,» *The International Arab Journal of Information Technology,* τόμ. 17, αρ. 4A, 2020.

[5] N. F. Syed, Z. Baig, A. Ibrahim και C. Valli, «Denial of service attack detection through machine learning for the IoT,» *Journal Information and Telecommunication,* τόμ. 4, αρ. 4, pp. 482-503, 2020.

[6] G. De La Torre Parra, P. Rad, K.-K. R. Choo και N. Beebe, «Detecting Internet of Things attacks using distributed deep learning,» *Journal of Network and Computer Applications,* αρ. 163, 2020.

[7] F. A. Fernandes Silveira, F. Lima-Filho, F. S. Dantas Silva, A. de Medeiros Brito Junior και L. F. Silveira, «Smart Detection-IoT: A DDoS Sensor System for Internet of Things,» *2020 International Conference on Systems, Signals and Image Processing (IWSSIP),* pp. 343-348, 2020.

[8] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad και G. A. Shah, «IoT DoS and DDoS Attack Detection using ResNet,» *2020 IEEE 23rd International Multitopic Conference (INMIC),* pp. 1-6, 2020.

[9] D. Myridakis, G. Spathoulas, A. Kakarountas, D. Schoinianakis και J. Lueken, «Mimicking Biometrics on Smart Devices and Its Application in IoT Security for Health Systems,» σε *IoT and ICT for Healthcare Applications,* N. Gupta και S. Paiva, Επιμ., Springer, Cham, 2020, pp. 175-189.

[10] D. Myridakis, G. Spathoulas, A. Kakarountas, D. Schinianakis και J. Lueken, «Monitoring Supply Current Thresholds for Smart Device's Security Enhancement,» *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS),* pp. 224-227, 2019.

[11] «Internet of Things (IoT),» ENISA, [Ηλεκτρονικό]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot.

[12] International Telecommunication Union, *Overview of the Internet of things,* ITU, 2012.

[13] International Telecommunication Union, ITU Internet Reports The Internet of Things, ITU, 2005.

[14] T. Savolainen, J. Soininen και B. Silverajan, «IPv6 Addressing Strategies for IoT,» *Sensors,* τόμ. 13, αρ. 10, pp. 3511-3519, 2013.

[15] O. Mazur, «10+ stats about the Internet of Things for eCommerce managers,»

Cloudflight, 2019. [Ηλεκτρονικό]. Available: https://ecommerce.cloudflight.io/blog/10-stats-about-the-internet-of-things-for-ecommerce-managers.

[16] J. Ding, M. Nemati, C. Ranaweera και J. Choi, «IoT Connectivity Technologies and Applications: A Survey,» *IEEE Access,* τόμ. 8, pp. 67646-67673, 2020.

[17] J. F. Kurose και K. W. Ross, Computer Networking: A Top-Down Approach, 7th Edition επιμ., Pearson Education Inc., 2017.

[18] «What is Wi-Fi 6?,» In-Synch Systems, 2024. [Ηλεκτρονικό]. Available: https://www.in-synchrms.com/single-post/what-is-wi-fi-6.

[19] «Internet of Things,» Wi-FI Alliance, 2024. [Ηλεκτρονικό]. Available: https://www.wi-fi.org/discover-wi-fi/internet-things.

[20] «Wi-Fi delivers strong IoT Advantage,» Wi-Fi Alliance, 2024. [Ηλεκτρονικό]. Available: https://www.wi-fi.org/news-events/newsroom/wi-fi-delivers-strong-iot-advantage.

[21] D. Ngo, «Wi-Fi Range Explained: Great Expectations vs. Harsh Reality of the Invisible Magic,» Dong Knows Tech, 25 5 2024. [Ηλεκτρονικό]. Available: https://dongknows.com/wi-fi-range-expectations-vs-reality/.

[22] E. R. Permana, F. N. Wahyu, H. Taufik και T. Thoyyibah, «The OSI and TCP/ IP Reference Models in the Era of Industry 4.0,» *Indonesian Journal of Machine Learning and Computer Science,* τόμ. 4, αρ. 3, pp. 936-942, 2024.

[23] A. Fraihat, «Computer Networking Layers Based on the OSI Model,» *TEST ENGINEERING AND MANAGEMENT,* τόμ. 83, pp. 6485-6495, 2021.

[24] A. A. Mughal, «Cyber Attacks on OSI Layers: Understanding the Threat Landscape,» *Journal of Humanities and Applied Science Research,* τόμ. 3, αρ. 1, pp. 1-18, 2020.

[25] M. Hossain, G. Kayas, R. Hasan, A. Skjellum, S. Noor και S. M. Riazul Islam, «A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives,» *Future Internet,* τόμ. 16, αρ. 2, 2024.

[26] N. Abughazaleh, R. b. Jabal και M. Btish, «DoS Attacks in IoT Systems and Proposed Solutions,» *International Journal of Computer Applications,* τόμ. 176, αρ. 33, 2020.

[27] H. S. Obaid και E. H. Abeed, «DoS and DDoS Attacks at OSI Layers,» *International Journal of Multidisciplinary Research and Publications,* τόμ. 2, αρ. 8, pp. 1-9, 2020.

[28] «HTTP flood attack,» Cloudflare, [Ηλεκτρονικό]. Available: https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/.

[29] S. Pal, M. Hitchens, T. Rabehaja και S. Mukhopadhyay, «Security Requirements for the Internet of Things: A Systematic Approach,» *Sensors,* τόμ. 20, αρ. 20, 2020.

[30] A. Nisar, «Intrusion Detection Systems: Categories, Attack Detection and Response,» *SSRN,* p. 5, 2023.

[31] I. Martins, J. S. Resende, P. R. Sousa, S. Silva, L. Antunes και J. Gama, «Host-based IDS: A review and open issues of an anomaly detection system in IoT,» *Future Generation Computer Systems,* τόμ. 133, pp. 95-113, 2022.

[32] P. Panagiotou, N. Mengidis, T. Tsikrika, S. Vrochidis και I. Kompatsiaris, «Host-based intrusion detection using signature-based and AI-driven anomaly detection

methods,» *Information and Security,* τόμ. 50, 2021.

[33] E. M. Maseno, Z. Wang και H. Xing, «A Systematic Review on Hybrid Intrusion Detection System,» *Security and Communication Networks,* τόμ. 2022, p. 23, 2022.

[34] E. Gamess και S. Hernandez, «Performance Evaluation of Different Raspberry Pi Models for a Broad Spectrum of Interests,» *International Journal of Advanced Computer Science and Applications,* τόμ. 13, αρ. 2, 2022.

[35] S. F. Barrett, Arduino Microcontroller Processing for Everyone, Springer, 2022.

[36] Microchip Technology Inc., *MCP9808,* 2018.

[37] TEXAS INSTRUMENTS, *LM35 Precision Centigrade Temperature Sensors,* 2017.

[38] ANALOG DEVICES, *Low Voltage Temperature Sensors TMP35/TMP36/TMP37,* 2002.

[39] «HOW DO THERMAL PADS WORK?,» SUR-SEAL ADVANCED MATERIAL SOLUTIONS, [Ηλεκτρονικό]. Available: https://www.sur-seal.com/blog/how-do-thermal-pads-work/.

[40] A. Munshi, N. A. Alqarni και N. A. Almalki, «DDOS Attack on IOT Devices,» σε *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS),* Riyadh, Saudi Arabia, 2020.

[41] R. Dilki, «An overview of the OSI model and its security threats,» FORTRA, 5 5 2023. [Ηλεκτρονικό]. Available: https://www.tripwire.com/state-of-security/overview-osi-model-and-its-security-threats.

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);

}
```

II. Κώδικας αισθητήρα θερμοκρασίας TMP36

```
#define sensorPin A0

void setup() {
 Serial.begin(9600);
 }

 void loop() {
 int reading = analogRead(sensorPin);

 float voltage = reading * (5.0 / 1024.0);

 float temperature = (voltage - 0.5) * 100;

 Serial.println(temperature);
 delay(100);
 }
```

III. Κώδικας αισθητήρα θερμοκρασίας LM35

```
#define sensorPin A0

void setup() {
  Serial.begin(9600);
}

void loop() {
  int adcData = analogRead(sensorPin);
  float voltage = adcData * (5.0 / 1024.0);
  float temperature = voltage * 100;
  Serial.println(temperature);
  delay(100); // wait a second between readings
}
```

Παράρτημα Β: 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

I. Κώδικας γραφημάτων τιμών θερμοκρασίας

```
clear all;
clc;

file1 = load(['filePath'])';
Ts = 0.1;

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

figure;
plot(t1,file1);
title('Title');
[min_val,idx_min] = min(file1);
[max_val,idx_max] = max(file1);
hold on;
mean(file1)
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 32]);
ylim([27 49]);
xlabel('time (minutes)');
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');
```