
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

# «Μελέτη εφαρμογής της Μηχανικής Μάθησης για την ασφάλεια σε χαμηλά επίπεδα του IoT»

**Του φοιτητή**
**Ανδρέου Στυλιανού**
**Αρ. Μητρώου: 185314**

**Επιβλέπων**
**Αμανατιάδης Δημήτριος**

**Μάιος 2024**

Τίτλος Δ.Ε. «Μελέτη εφαρμογής της Μηχανικής Μάθησης για την ασφάλεια σε χαμηλά επίπεδα του IoT»

Κωδικός Δ.Ε. 22349

Ονοματεπώνυμο φοιτητή/τών: Ανδρέου Στυλιανός

Ονοματεπώνυμο εισηγητή Αμανατιάδης Δημήτριος

Ημερομηνία ανάληψης Δ.Ε. 30/11/2022

Ημερομηνία περάτωσης Δ.Ε. 25/05/2024

//

*Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.*



Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

# Πρόλογος

Το συγκεκριμένο θέμα για αυτή την διπλωματική, οφείλεται στο ενδιαφέρον για την σχέση μεταξύ της ασφάλειας και των ανερχόμενων τεχνολογιών, ιδίως στο Διαδίκτυο των Πραγμάτων. Τα συστήματα αυτά μπαίνουν στην καθημερινή μας ζωή όλο και πιο πολύ, γεγονός που παρουσιάζει ιδιαίτερες προκλήσεις ασφαλείας που απαιτούν δημιουργικές λύσεις. Τέτοιες δημιουργικές λύσεις μπορούν να προσφέρουν οι τεχνολογίες της μηχανικής και βαθιάς μάθησης. Η κατανόηση της κατάστασης της ασφάλειας του Διαδικτύου των Πραγμάτων, στις πιο πρόσφατες εξελίξεις στις τεχνολογίες μηχανικής και βαθιάς μάθησης και στον τρόπο χρήσης αυτών των τεχνολογιών ήταν το όφελος αυτής της διπλωματικής.

# Περίληψη

Η σύγχρονη κοινωνία εξαρτάται σε μεγάλο βαθμό από το IoT, το οποίο αποτελείται από τις πολυάριθμες συνδεδεμένες στο Διαδίκτυο συσκευές που αποτελούν μέρος της καθημερινής μας ζωής. Αυτές οι συσκευές γίνονται όλο και πιο διαδεδομένες, οπότε η προστασία τους από επιθέσεις στον κυβερνοχώρο είναι πολύ σημαντική. Η διπλωματική προσφέρει μια λεπτομερή ανάλυση του IoT, εστιάζοντας ιδιαίτερα στα χαμηλά επίπεδα της αρχιτεκτονικής του. Διερευνά τα κενά ασφαλείας που υπάρχουν σε αυτά τα θεμελιώδη επίπεδα, εξετάζοντας πως τα προβλήματα αυτά επηρεάζουν την αξιοπιστία και αποτελεσματικότητα των συστημάτων IoT. Επίσης διερευνάται ο τρόπος με τον οποίο αυτά τα προβλήματα ασφαλείας μπορούν να επιλυθούν με την εφαρμογή των τεχνολογιών μηχανικής μάθησης (Machine Learning, ML) και βαθιάς μάθησης (Deep Learning, DL). Εξετάζει και συγκρίνει διαφορετικούς αλγορίθμους, περιγράφοντας τα θεωρητικά τους θεμέλια, τα πλεονεκτήματα και τα μειονεκτήματα τους και παρουσιάζοντας πόσο καλά λειτουργούν για την ενίσχυση της ασφάλειας του IoT.

«Study on the application of Machine Learning for low-level IoT security»

«Stylianos Andreou»

## Abstract

Modern society is heavily dependent on the IoT, which consists of the numerous Internet-connected devices that are part of our daily lives. These devices are becoming more and more widespread, so protecting them from cyber attacks is very important. The thesis offers a detailed analysis of the IoT, focusing particularly on the low-levels of its architecture. It explores the security gaps that exist at these fundamental layers, examining how these problems affect the reliability and effectiveness of IoT systems. It also explores how these security problems can be solved by applying machine learning (ML) and deep learning (DL) technologies. It examines and compares different algorithms, describing their theoretical foundations, their advantages and disadvantages, and showing how well they work to enhance IoT security.

# Περιεχόμενα

# Κατάλογος Σχημάτων

# Κατάλογος Πινάκων

# Συντομογραφίες

| | |
|---|---|
| ANN | Artificial Neural Network |
| AE | Autoencoder |
| BL | Bluetooth |
| BLE | Bluetooth Low Energy |
| CNN | Convolutional Neural Network |
| DBN | Deep Belief Network |
| DL | Deep Learning |
| DODAG | Destination Oriented Directed Acyclic Graph |
| DT | Decision Tree |
| DNN | Deep Neural Network |
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| EL | Ensemble Learning |
| GBA | Gradient Boosting Algorithm |
| GPS | Global Positioning System |
| IoT | Internet of Things |
| IDS | Intrusion Detection System |
| KNN | k-Nearest Neighbor |
| LR | Linear Regression |
| LSTM | Long Short-Term Memory |
| ML | Machine Learning |
| NFC | Near Field Communication |
| NB | Naive Bayes |
| RF | Random Forest |
| RNN | Recurrent Neural Networks |
| RFID | Radio-frequency Identification |
| RPL | Routing Protocol for Low-Power and Lossy Networks |
| SVM | Support Vector Machine |

# 1. Εισαγωγή στο Διαδίκτυο των Πραγμάτων

## 1.1 Εισαγωγή

Στο πρώτο κεφάλαιο γίνεται μια επισκόπηση της εξέλιξης του Διαδικτύου (Internet) στο Διαδίκτυο των πραγμάτων (Internet of Things, IoT). Επίσης, παρουσιάζει την σημαντική επιρροή του IoT στην παγκόσμια οικονομία και την ευρεία κοινωνική ενσωμάτωση του. Αναφέρεται για το πως οι τεχνολογίες του IoT αλλάζουν τους κλάδους, επιταχύνουν την οικονομική ανάπτυξη και μεταβάλλουν τον τρόπο με τον οποίο αλληλεπιδρούν οι εταιρείες και οι πελάτες. Διερευνώνται επίσης οι επιπτώσεις του IoT στην κοινωνία, δίνοντας έμφαση στις βελτιώσεις στην καθημερινή ζωή, συμπεριλαμβανομένων της αυξημένης ευκολίας, των καλύτερων πρωτοκόλλων υγείας και ασφάλειας και της αποτελεσματικότερης διαχείρισης των πόρων.

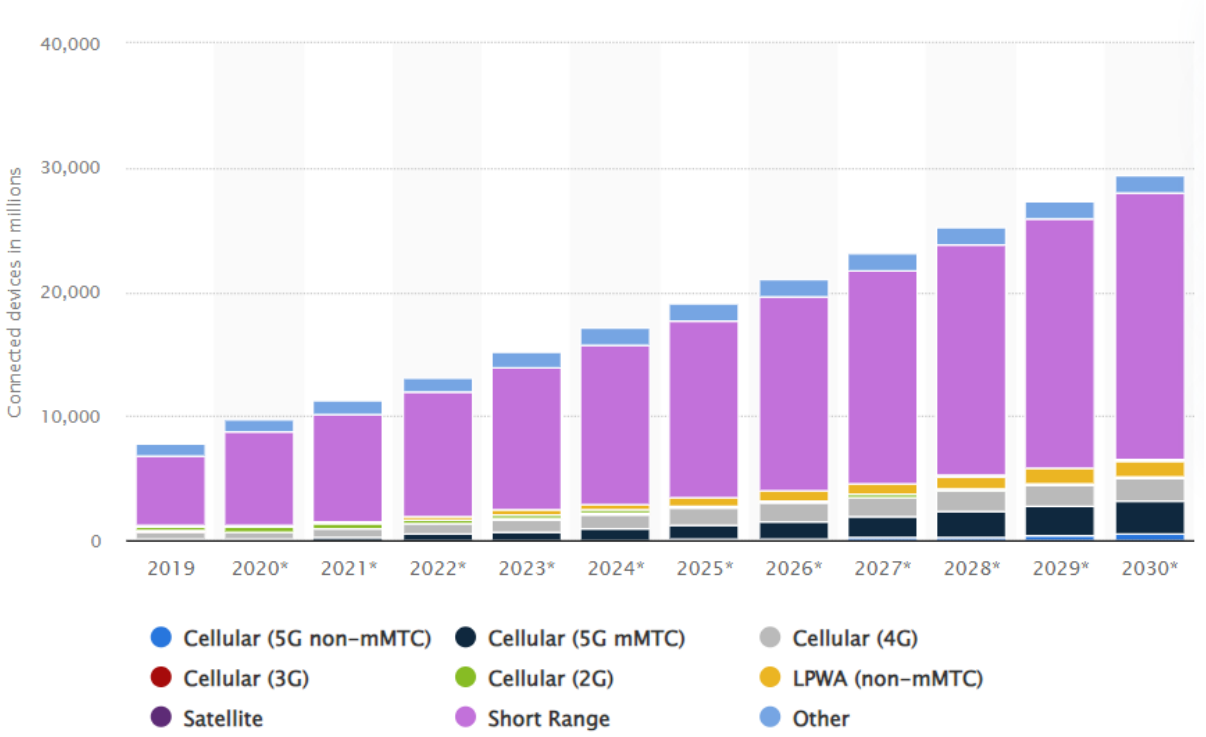
## 1.2 Το IoT ως επέκταση του Διαδικτύου

Από τα τέλη του 20ου αιώνα και ο 21ος αιώνας έχει αναδειχθεί σε μία περίοδο πρωτοφανούς τεχνολογικής προόδου, η οποία αλλάζει ραγδαία την ζωή μας. Κεντρικό ρόλο σε αυτή την μεταβολή παίζει το Διαδίκτυο, μία ιδέα ερευνητών και επιστημόνων που οραματίστηκαν ένα δίκτυο ικανό να υπερβεί τα γεωγραφικά σύνορα και να συνδέσει ανθρώπους σε όλο τον κόσμο. Στη δεκαετία του 1960, η δημιουργία του ARPANET αποτέλεσε το πρώτο βήμα προς την κατεύθυνση αυτού του οράματος [1]. Αυτό ήταν που έθεσε τα θεμέλια για αυτόν τον παγκόσμιο κολοσσό που αναγνωρίζουμε σήμερα.

Καθώς το Internet αναπτυσσόταν, προέκυψε η ιδέα της επέκτασης της συνδεσιμότητας στο Internet πέρα από τις συνηθισμένες υπολογιστικές συσκευές, και στον τομέα των φυσικών αντικειμένων. Το IoT προέκυψε ως η φυσική ενσάρκωση αυτής της ιδέας, αντικατοπτρίζοντας ένα παράδειγμα στο οποίο κοινά αντικείμενα, από οικιακές συσκευές έως βιομηχανικό εξοπλισμό, ενσωματώνονται με αισθητήρες, ενεργοποιητές και συνδεσιμότητα, επιτρέποντας τους να ανταλλάσσουν δεδομένα και να αλληλεπιδρούν αυτόνομα [2]. Ο αυτόματος πωλητής αναψυκτικών που εγκαταστάθηκε στο τμήμα επιστήμης υπολογιστών του Πανεπιστημίου Carnegie Mellon στις αρχές της δεκαετίας του 1980 δεν ήταν ένας απλός αυτόματος πωλητής, αλλά ένα πρωτοποριακό δείγμα τεχνολογίας που προανήγγειλε την έναρξη του IoT. Η ιστορία του αυτόματου πωλητή αναψυκτικών ξεκίνησε με τους John Zsarnay, David Nichols και Ivor Durham, τρεις φοιτητές του πανεπιστημίου Carnegie-Mellon, οι οποίοι ήταν δυσαρεστημένοι με την απρόβλεπτη διαθεσιμότητα αναψυκτικών στον αυτόματο πωλητή του κτιρίου. Το μηχάνημα μπορούσε να επικοινωνήσει και να καταχωρήσει στο σύστημα, τον αριθμό των αναψυκτικών που απέμεναν και αν ήταν αρκετά κρύα [3], [4], [5]. Στα τέλη της δεκαετίας του 1990, ο Kevin Ashton έλαβε ευρεία αναγνώριση για την επινόηση του όρου “Internet of Things”. Ο Ashton, πρωτοπόρος της τεχνολογίας και συνιδρυτής του Auto-ID Center στο Τεχνολογικό Ινστιτούτο της Μασαχουσέτης (Massachusetts Institute of Technology, MIT), διατύπωσε τον όρο αυτό καθώς εργαζόταν στην τεχνολογία αναγνώρισης ραδιοσυχνοτήτων (Radio-frequency Identification, RFID) [6]. Σε μια παρουσίαση το 1999, ο Ashton χρησιμοποίησε τον όρο "Internet of Things" για να περιγράψει τη σύνδεση φυσικών αντικειμένων στο διαδίκτυο. Στόχος ήταν τα αντικείμενα αυτά να μπορούν να συλλέγουν και να ανταλλάσσουν δεδομένα χωρίς την ανάγκη ανθρώπινης παρέμβασης, προωθώντας την αυτοματοποίηση, την αποδοτικότητα και νέες δυνατότητες για εφαρμογές σε διάφορους κλάδους [7].

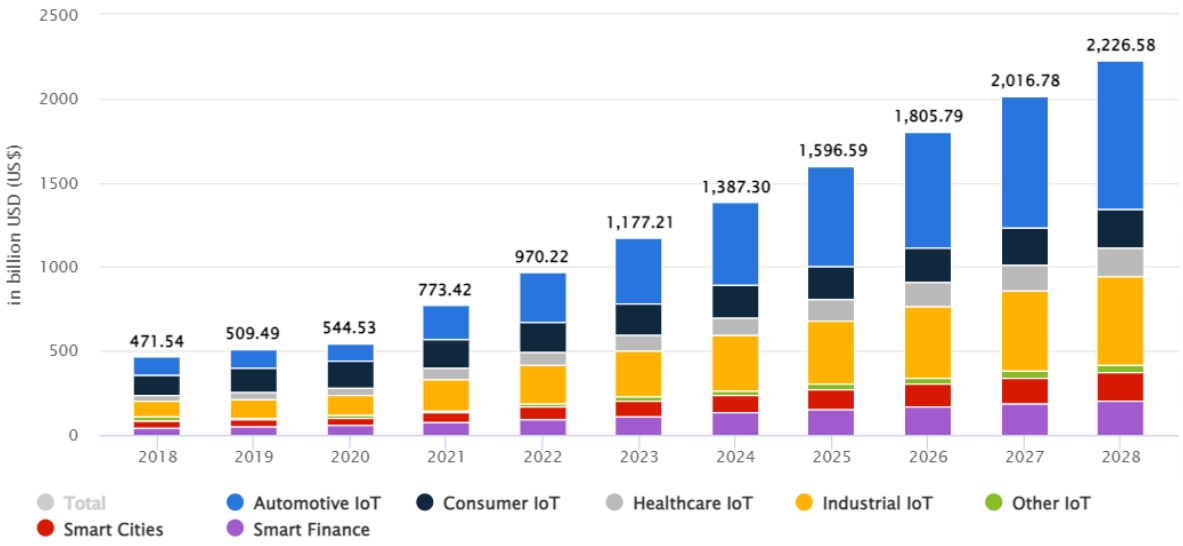
Η ραγδαία εξάπλωση του IoT έχει αποκτήσει καθοριστικό ρόλο σε μια εποχή όπου τα καθημερινά αντικείμενα έχουν μετατραπεί σε ευφυή υπολογιστικά συστήματα, μεταμορφώνοντας τον

τρόπο με τον οποίο ζούμε, εργαζόμαστε και αλληλεπιδρούμε με τον κόσμο γύρω μας. Πρόσφατα στατιστικά στοιχεία αναδεικνύουν τον εκπληκτικό ρυθμό υιοθέτησης του IoT, με δισεκατομμύρια συσκευές να έχουν πλέον ενσωματωθεί στην καθημερινή μας ζωή [8]. Σύμφωνα με το Σχήμα 1.1, ο αριθμός των συνδεδεμένων συσκευών το 2019 ήταν στα 7.7 δισεκατομμύρια, σήμερα - 2024 βρίσκεται στα 18.3 δισεκατομμύρια και μέχρι το τέλος της δεκαετίας οι προβλέψεις δείχνουν για περίπου 30 δισεκατομμύρια συσκευές. Αυτή η ψηφιακή επανάσταση, δεν έχει μόνο αναδιαμορφώσει τον τρόπο με τον οποίο ζούμε και εργαζόμαστε, αλλά έχει επίσης αναδιαμορφώσει και την παγκόσμια οικονομία [9].




Σχήμα 1.1: *Αριθμός συνδεδεμένων συσκευών στο IoT παγκοσμίως από το 2019 έως το 2030, ανά τεχνολογία επικοινωνιών. (σε εκατομμύρια)* [8]

Η αγορά των συσκευών IoT συνεχίζει να αναπτύσσεται με εντυπωσιακούς ρυθμούς, και ο εκτιμώμενος αριθμός εσόδων ανά κατηγορία εφαρμογής αποτελεί ενδιαφέρον παράγοντα για τον κλάδο. Στην κατηγορία της έξυπνης κατοικίας, οι προβλέψεις υποδεικνύουν σημαντική αύξηση των εσόδων, καθώς οι καταναλωτές επενδύουν σε συστήματα αυτοματισμού και ασφαλείας. Οι εφαρμογές υγείας και φροντίδας, με τη χρήση συσκευών παρακολούθησης και ιατρικών αισθητήρων, προβλέπεται να συνεχίσουν την άνοδό τους. Επιπλέον, οι εφαρμογές στον τομέα της βιομηχανίας και της γεωργίας επίσης αναμένεται να συνεισφέρουν σημαντικά στα έσοδα, καθώς οι επιχειρήσεις ενσωματώνουν όλο και περισσότερες συσκευές IoT για τη βελτίωση της απόδοσης και της αποτελεσματικότητάς τους. Συνολικά, ο εκτιμώμενος αριθμός εσόδων από τις συσκευές IoT καταδεικνύει ένα δυναμικό τοπίο, όπου η τεχνολογία συνεχίζει να επιφέρει καινοτομίες και ανατροπές σε διάφορους τομείς. Το Σχήμα 1.2 παρουσιάζει τον εκτιμώμενο αριθμό εσόδων από την πώληση συσκευών IoT ανά κατηγορία εφαρμογής. Τα αποτελέσματα δείχνουν ότι η αυτοκινητοβιομηχανία και ο τομέας της υγείας θα είναι οι εφαρμογές που θα φέρουν τα μεγαλύτερα έσοδα στην παγκόσμια οικονομία.




Σχήμα 1.2: *Έσοδα από πώληση συσκευών του IoT παγκοσμίως από το 2018 έως το 2028, ανά εφαρμογή. (σε δισεκατομμύρια)* [9]

Η αυξανόμενη δημοτικότητα των συσκευών IoT έχει προέλθει από τις εξελίξεις στις τεχνολογίες δικτύων και αισθητήρων. Τα σύγχρονα δίκτυα προσφέρουν τις υποδομές για την ομαλή επικοινωνία και ένα σύνολο από αισθητήρες διευκολύνει την συλλογή των δεδομένων. Μαζί, αυτά τα δύο κύρια στοιχεία των συστημάτων IoT, έχουν δημιουργήσει ένα παράδειγμα στο οποίο τα αντικείμενα είναι ικανά να αλληλεπιδρούν έξυπνα με το περιβάλλον τους, να ανταλλάσσουν πληροφορίες και να επικοινωνούν. Η ανάγκη για αυτοματοποίηση είναι ένας ακόμη παράγοντας της εξάπλωσης. Οι επιχειρήσεις έλκονται από την υπόσχεση της βελτιωμένης επιχειρησιακής απόδοσης που μπορεί να προσφέρει το IoT. Οι επιχειρήσεις μπορούν να φτάσουν σε νέα επίπεδα αποδοτικότητας χάρη στην απλότητα με την οποία μπορεί να συνδεθεί και να παρακολουθήσει τις συσκευές. Ο έλεγχος των συσκευών IoT προσφέρει μια ολοκληρωμένη εικόνα των λειτουργιών, επιτρέποντας την άμεση λήψη αποφάσεων και την ανίχνευση προβλημάτων. Οι συσκευές IoT για ιδιωτική χρήση έχουν μετασχηματίσει ριζικά τη φύση της καθημερινότητάς μας, ενσωματώνοντας έξυπνες λύσεις σε κάθε πτυχή της ζωής μας. Από τα έξυπνα σπίτια που προσφέρουν αυτοματοποιημένο έλεγχο των συσκευών και των φωτιστικών, μέχρι τις φορητές συσκευές υγείας που παρακολουθούν συνεχώς την κατάσταση του σώματός μας, η τεχνολογία IoT δημιουργεί έναν ενιαίο και έξυπνο χώρο ζωής. Οι έξυπνες κάμερες και οι αισθητήρες ασφαλείας προσφέρουν αίσθηση ασφάλειας, ενώ οι φορητές συσκευές επιτρέπουν την σύνδεση και τον έλεγχο από οπουδήποτε. Η δυνατότητα αλληλεπίδρασης με το περιβάλλον μας μέσω smartphone ή φωνητικών εντολών επιτρέπει στους ανθρώπους να διαχειρίζονται και να προσαρμόζουν το περιβάλλον τους με άνεση και αποτελεσματικότητα. Οι συσκευές IoT για ιδιωτική χρήση δημιουργούν μία νέα πραγματικότητα, συνδυάζοντας την έξυπνη τεχνολογία με την καθημερινή ζωή για να την κάνουν πιο άνετη [5].

Η έκταση της χρήσης συσκευών IoT έχει ανοίξει νέα παράθυρο για ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής και την ακεραιότητα των δεδομένων. Καθώς οι συσκευές IoT συλλέγουν διαρκώς προσωπικά δεδομένα για τις συνήθειες και τις προτιμήσεις μας, αυξάνεται ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης σε αυτές τις πληροφορίες. Η ανησυχία αυτή επεκτείνεται σε ζητήματα ασφάλειας, καθώς πιθανές απειλές όπως η απόκτηση μη εξουσιοδοτημένης πρόσβασης και οι κακόβουλες επιθέσεις μπορούν να θέσουν σε κίνδυνο την ιδιωτικότητα και την ακεραιότητα των δεδομένων. Ωστόσο, αυτή η αύξηση της συνδεσιμότητας φέρνει μαζί της μια σειρά από νέες

προκλήσεις, υπογραμμίζοντας την κρίσιμη σημασία της ασφάλειας στο περιβάλλον του IoT. Όσο αυξάνεται ο αριθμός των συνδεδεμένων συσκευών, τόσο αυξάνεται και το κίνητρο για επίθεση στις ευπάθειες (vulnerabilities) από τους κακόβουλους χρήστες. Ένα σενάριο όπου ένας κακόβουλος χρήστης αποκτά μη εξουσιοδοτημένη πρόσβαση σε συσκευή IoT σίγουρα θα έχει καταστροφικά αποτελέσματα. Για παράδειγμα αν αποκτήσει πρόσβαση στο σύστημα ενός έξυπνου σπιτιού, θα μπορεί να απενεργοποιήσει το σύστημα συναγερμού, να παρακολουθήσει τους ιδιοκτήτες από τις κάμερες ασφαλείας αλλά ακόμη και να διαχειριστεί το σύστημα θέρμανσης του σπιτιού. Οι ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής, την ακεραιότητα των δεδομένων και την πιθανότητα μη εξουσιοδοτημένης πρόσβασης αποτελούν σημαντικές απειλές που πρέπει να αντιμετωπιστούν με προσοχή [10].

Τα υπόλοιπα κεφάλαια της διπλωματικής οργανώνονται ως εξής: Στο Κεφάλαιο 2 καλύπτονται λεπτομερώς τα βασικά στοιχεία του IoT, μαζί με τις τοπολογίες και τις τεχνολογίες ενσύρματων και ασύρματων δικτύων. Στο Κεφάλαιο 3 εξετάζονται τα στοιχεία, οι αρχιτεκτονικές, οι τεχνολογίες και οι εφαρμογές του IoT. Το Κεφάλαιο 4 επικεντρώνεται στις λειτουργίες της μηχανικής μάθησης (Machine Learning, ML) και της βαθιάς μάθησης (Deep Learning, DL). Οι αρχές της κυβερνοασφάλειας καλύπτονται στο Κεφάλαιο 5 και επεκτείνεται στο Κεφάλαιο 6 με την ανάλυση συγκεκριμένων ζητημάτων κυβερνοασφάλειας του IoT. Στο Κεφάλαιο 7, παρουσιάζονται λύσεις βασισμένες στο ML και DL.

## 1.3 Επίλογος

Σε αυτό το πρώτο εισαγωγικό κεφάλαιο παρουσιάζεται μία ολοκληρωμένη ιστορία του IoT, από την δημιουργία του έως την σημερινή του θέση ως μετασχηματιστικό στοιχείο στον σημερινό διασυνδεδεμένο κόσμο. Καταγράφεται η εξέλιξη του διαδικτύου από την γέννηση του έως την ευρεία εξάπλωση των συσκευών IoT, δίνοντας έμφαση στην βαθιά επιρροή του σε μια σειρά από κλάδους, όπως τα έξυπνα σπίτια, η υγειονομική περίθαλψη και οι βιομηχανικές λειτουργίες. Παρά τα πλεονεκτήματα της αύξησης της παραγωγικότητας και της δημιουργικότητας, το κεφάλαιο αναφέρεται στα σοβαρά ζητήματα ασφάλειας, στην προστασία της ιδιωτικής ζωής και στην ακεραιότητα των δεδομένων που προκύπτουν με την ανάπτυξη του IoT. Επισημαίνει την αναγκαιότητα ισχυρών μέτρων ασφαλείας προβάλλοντας τους πραγματικούς κινδύνους που δημιουργούν οι επιθέσεις μέσω παραδειγμάτων.

# 2. Θεμέλια δικτύων για το IoT

## 2.1 Εισαγωγή

Αυτό το κεφάλαιο διερευνά τις βασικές τεχνολογίες δικτύων που υποστηρίζουν το IoT, επιτρέποντας την επικοινωνία και την συνδεσιμότητα μεταξύ ενός ευρέος φάσματος συστημάτων και συσκευών. Αρχικά δίνεται μια επισκόπηση των ενσύρματων δικτυακών υποδομών, δεδομένου ότι τα συστήματα αυτά είναι απαραίτητα για την παροχή της ταχύτητας και της ανθεκτικότητας που απαιτούν τα αξιόπιστα δίκτυα IoT. Στην συνέχεια, η έρευνα μετατοπίζεται στις τεχνολογίες ασύρματων δικτύων, δίνοντας έμφαση στην παροχή της επεκτασιμότητας και της ευελιξίας που απαιτούνται για την ικανοποίηση των αυξανόμενων απαιτήσεων των εφαρμογών του IoT.

Επίσης εξετάζει τις διαφορετικές τοπολογίες δικτύου που ελέγχουν τον τρόπο με τον οποίο οι συνδεδεμένες συσκευές αλληλεπιδρούν μεταξύ τους. Η βελτίωση της ανθεκτικότητας του δικτύου και της αποδοτικότητας της επικοινωνίας απαιτεί την εις βάθος κατανόηση αυτών των τοπολογιών. Κάθε τοπολογία έχει μοναδικά πλεονεκτήματα και μειονεκτήματα που επηρεάζουν τον τρόπο σχεδιασμού και λειτουργίας των περιβάλλοντων IoT, ο οποίος είναι απαραίτητος για την διασφάλιση της ασφαλούς και απρόσκοπτης μεταφοράς των δεδομένων.

## 2.2 Ενσύρματα Δίκτυα

Τα ενσύρματα δίκτυα αποτελούν την βάση πολλών εφαρμογών του IoT, παρέχοντας ένα σταθερό και αξιόπιστο περιβάλλον για την ομαλή μεταφορά των δεδομένων. Παρακάτω παρουσιάζονται τα διάφορα πρότυπα και μέσα που χρησιμοποιούνται για να δημιουργήσουν αυτό το αξιόπιστο περιβάλλον.

- **Ethernet:** Το Ethernet, ένα διαχρονικό πρότυπο στην τεχνολογία δικτύωσης, περιγράφεται από το IEEE 802.3 [11]. Παρέχει μια ισχυρή βάση για τοπικά δίκτυα σε διάφορα περιβάλλοντα, όπως σπίτια και γραφεία, εφόσον είναι γνωστό για τις γρήγορες ταχύτητες και την ελάχιστη καθυστέρηση. Η ανάπτυξη του Real-Time Ethernet είναι ιδιαίτερα χρήσιμη στο IoT, όπου η ταχύτητα απόκρισης είναι κρίσιμη [12]. Αυτές οι προσαρμοσμένες τροποποιήσεις εγγυώνται αξιόπιστη και έγκαιρη μεταφορά των δεδομένων, γεγονός που τις καθιστά απαραίτητες για εφαρμογές που χρειάζονται άμεση επικοινωνία, όπως ο βιομηχανικός αυτοματισμός.
- **Οπτική Ίνα:** Η μετάδοση των δεδομένων απέκτησε μια νέα και επαναστατική διάσταση με την έλευση των δικτύων οπτικών ινών. Τα δίκτυα αυτά, χρησιμοποιούν σήματα φωτός για την δημιουργία συνδέσεων με υψηλό εύρος ζώνης και ταχύτητα. Στο πεδίο του IoT, οι οπτικές ίνες γίνονται απαραίτητοι επικοινωνιακοί αγωγοί μεγάλων αποστάσεων, μειώνοντας τις απώλειες σήματος και προσφέροντας την βάση για την μεταφορά τεράστιου όγκου δεδομένων. Υπάρχουν δύο βασικές κατηγορίες οπτικών ινών: Η μονότροπη ίνα (Single-Mode Fiber, SMF), η οποία προβλέπεται για μεταδόσεις σε μεγαλύτερες αποστάσεις, και η πολύτροπη ίνα (Multi-Mode Fiber, MMF), η οποία είναι καλύτερη για μικρότερες αποστάσεις. Οι ιδιαίτερες ανάγκες της εκάστοτε εφαρμογής IoT καθορίζουν ποια από τις MMF και SMF θα χρησιμοποιηθεί [2], [13].
- **Ψηφιακή συνδρομητική γραμμή (Digital Subscriber Line, DSL):** Βασικό στοιχείο για την παροχή πρόσβασης στο διαδίκτυο είναι το DSL, μία ευρηματική τροποποίηση των σημερινών τηλεφωνικών γραμμών που χρησιμοποιούν καλώδια χαλκού. Αυτή η τεχνολογία δεν παρέχει μόνο ευρυζωνική πρόσβαση αλλά καθιστά επίσης δυνατή την ταυτόχρονη μετάδοση δεδομένων και φωνής [2]. Το DSL τονίζει την προσαρμοστικότητα του στο IoT, καλύπτοντας διαφορετικές

ανάγκες σε εύρος ζώνης. Αυτό επιτυγχάνεται με την χρήση των Asymmetric DSL (ADSL) και Very-high-bitrate DSL (VDSL), όπου είναι οι εξελίξεις της τεχνολογίας DSL [14].

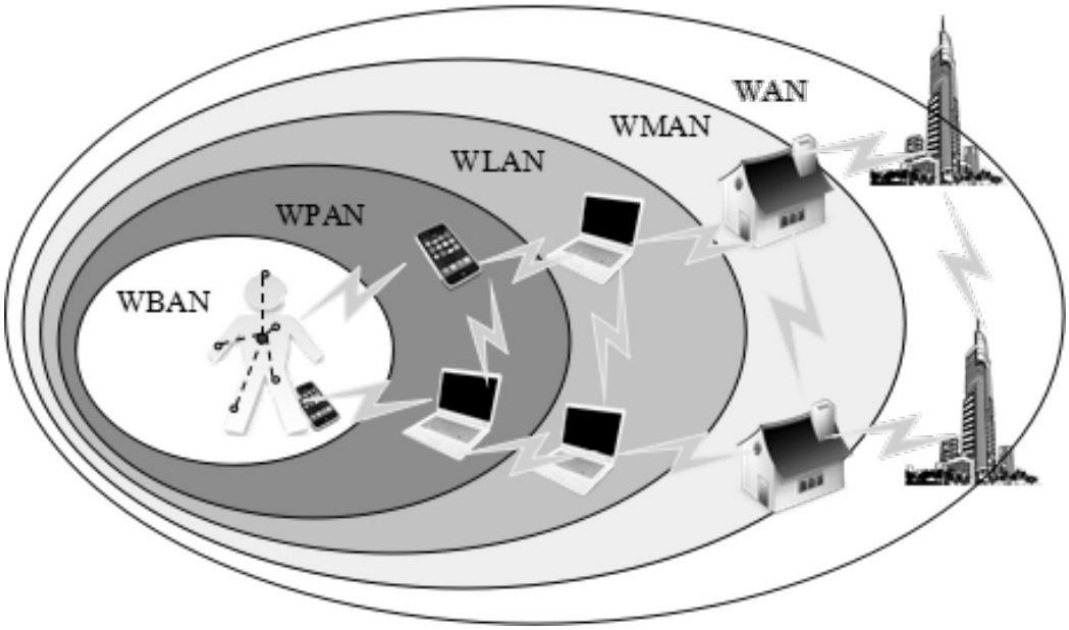
- **Επικοινωνία με καλώδια ρεύματος (Powerline Communication, PLC):** Αξιοποιώντας τις ήδη υπάρχουσες γραμμές ηλεκτρικής ενέργειας, η τεχνολογία PLC παρέχει μία λειτουργική λύση για την μετάδοση των δεδομένων. Το PLC χρησιμοποιείται ευρέως στην οικιακή δικτύωση και στα έξυπνα δίκτυα (smart grid) [15]. Χρησιμοποιεί έξυπνα την υπάρχουσα ηλεκτρική καλωδίωση, προσφέροντας ένα πιο απλό και αποτελεσματικό μοντέλο ανάπτυξης. Παίζει καθοριστικό ρόλο στο IoT, προσφέροντας μια διαφορετική και ευέλικτη επιλογή συνδεσιμότητας για ένα ευρύ φάσμα εφαρμογών. Οι τεχνολογίες PLC μπορούν να προσαρμοστούν σε διαφορετικά σενάρια, όπως Narrowband PLC και Broadband over Powerline, γεγονός που αυξάνει την εμβέλεια της συνδεσιμότητας [16].

## 2.3 Ασύρματα Δίκτυα

Με την εισαγωγή των ασύρματων δικτύων, το περιβάλλον της συνδεσιμότητας άλλαξε, φέρνοντας μαζί του μια νέα εποχή ευελιξίας στον τομέα του IoT. Αυτό το υποκεφάλαιο εξετάζει μια ποικιλία ασύρματων δικτύων που αποτελούν στοιχείο του συνεχώς εξελισσόμενου IoT. Κάθε ασύρματη τεχνολογία έχει ξεχωριστό αντίκτυπο στον τρόπο σύνδεσης, από τις δυνατότητες μικρής εμβέλειας των Ασύρματων Δικτύων Προσωπικής Περιοχής (Wireless Personal Area Networks, WPAN), εως την ευρεία κάλυψη που προσφέρουν τα Ασύρματα Δίκτυα Ευρείας Περιοχής (Wireless Wide Area Networks, WWAN).

- **Ασύρματα Δίκτυα Περιοχής Σώματος (Wireless Body Area Network, WBAN):** Τα WBANs, είναι δίκτυα που προορίζονται να καλύψουν ολόκληρο το σώμα και να παρέχουν στις έξυπνες συσκευές υγείας ένα ολοκληρωμένο περιβάλλον επικοινωνίας. Η μετάδοση συνεχών μετρήσεων σε πραγματικό χρόνο καθίσταται δυνατή χάρη σε αυτή την εξέλιξη των ασύρματων επικοινωνιών, παρέχοντας πληθώρα δεδομένων σχετικά με την κατάσταση της υγείας. Επειδή οι χρήστες μπορούν να λαμβάνουν ενημερώσεις σε πραγματικό χρόνο σχετικά με τις λειτουργίες του σώματός τους, αυτό διευκολύνει την προληπτική διαχείριση της υγείας [17].
- **Ασύρματα Δίκτυα Προσωπικής Περιοχής (Wireless Personal Area Network, WPAN):** Στον χώρο του IoT, τα δίκτυα WPAN αποτελούν μια σημαντική κατηγορία δικτύων. Οι τεχνολογίες WPAN χρησιμοποιούνται συνήθως από συσκευές που λειτουργούν σε ακτίνα 10 μέτρων για τη διευκόλυνση της αποτελεσματικής ασύρματης επικοινωνίας. Για παράδειγμα, το Bluetooth παρέχει αξιόπιστη συνδεσιμότητα μεταξύ των IoT συσκευών. Αντίθετα, η χαμηλή κατανάλωση ενέργειας και η αξιόπιστη επικοινωνία σε κοντινές αποστάσεις είναι απαιτήσεις που μπορεί να ικανοποιήσει η τεχνολογία Zigbee [18]. Με βάση το WPAN, το βλέμμα στρέφεται στα Ασύρματα Προσωπικά Δίκτυα Χαμηλού Ρυθμού (Low-Rate Wireless Personal Area Network, LR-WPAN), με ιδιαίτερη έμφαση στην υποστήριξη εφαρμογών που απαιτούν χαμηλότερους ρυθμούς δεδομένων. Επεκτείνοντας την λειτουργικότητα των WPANs, τα LR-WPANs μπορούν να χρησιμοποιηθούν σε καταστάσεις όπου ο υψηλός ρυθμός μετάδοσης και η χαμηλή κατανάλωση ενέργειας είναι κρίσιμα [19]. Στα επόμενα κεφάλαια θα εξεταστούν λεπτομερώς τα χαρακτηριστικά, οι χρήσεις και οι μελλοντικές εξελίξεις που αφορούν τα WPAN και τα LR-WPAN στο πλαίσιο του IoT.
- **Ασύρματα Τοπικά Δίκτυα (Wireless Local Area Network, WLAN):** Η τεχνολογία που είναι γνωστή ως WLAN, παρέχει ασύρματη συνδεσιμότητα σε περιοχές έως και 100 μέτρα. Η ευρεία υιοθέτηση της τεχνολογίας Wi-Fi, είναι θεμελιώδης για τα δίκτυα αυτά [20].

- **Ασύρματα Μητροπολιτικά Δίκτυα (Wireless Metropolitan Area Network, WMAN):** Τα WMANs είναι ένας τύπος προηγμένου ασύρματου δικτύου που συνδέει WLANs, εξασφαλίζοντας ευρυζωνική και υψηλής απόδοσης επικοινωνία. Η τεχνολογία WiMAX ξεχωρίζει για την ικανότητά της να παρέχει ασύρματη πρόσβαση υψηλής ταχύτητας σε αυτούς τους τύπους δικτύων [21].
- **Ασύρματα Δίκτυα Ευρείας Περιοχής (Wireless Wide Area Network, WWAN):** Τα WWANs γίνονται απαραίτητα μέσα για την διασφάλιση των επικοινωνιών σε γεωγραφικά απομονωμένες περιοχές, προωθώντας τη συνδεσιμότητα σε απομακρυσμένες τοποθεσίες που προηγουμένως δεν ήταν προσβάσιμες. Τα κυψελοειδή δίκτυα και τα δορυφορικά δίκτυα αποτελούν παραδείγματα αυτών των τεχνολογιών ασύρματης επικοινωνίας, οι οποίες είναι απαραίτητες για τη σύνδεση των IoT συσκευών σε μέρη με ελλιπή υποδομή επικοινωνιών [18]. Με την έλευση των Δικτύων Χαμηλής Ισχύος Ευρείας Περιοχής (Low-Power Wide-Area Networks, LPWANs), τα WWANs έχουν παρουσιάσει μια σημαντική αλλαγή. Η αλλαγή αυτή σηματοδοτεί μία νέα εποχή στην συνδεσιμότητα, με τις τεχνολογίες LPWAN να παρέχουν αξιόπιστες συνδέσεις μεγάλης εμβέλειας με αξιοσημείωτα χαμηλή κατανάλωση ενέργειας. Αυτό τις καθιστά την ιδανική επιλογή για εφαρμογές που πρέπει να καλύπτουν μεγαλύτερες αποστάσεις και να έχουν μεγαλύτερη διάρκεια ζωής της μπαταρίας [22].



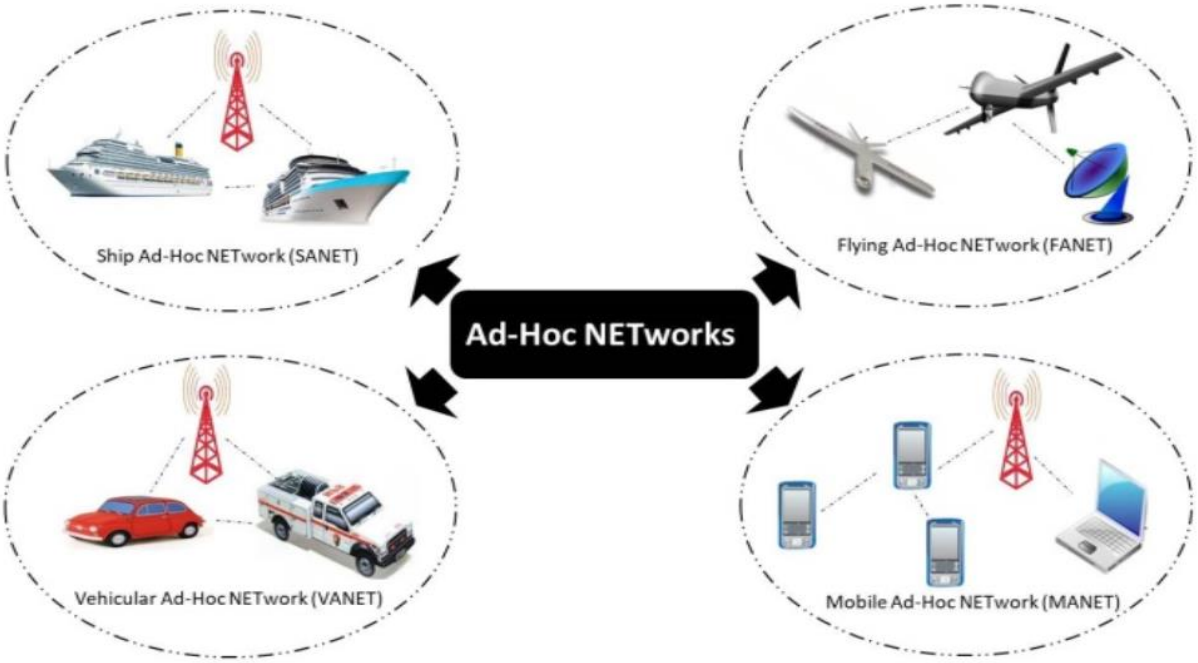

Σχήμα 2.1: *Η σχέση του WBAN και άλλων τεχνολογιών ασύρματων δικτύων* [23]

Επεκτείνοντας την έρευνα μας πέρα από τις προαναφερθείσες ασύρματες τεχνολογίες, εξετάζουμε μία σειρά πρόσθετων ασύρματων τεχνολογιών, όπως τα δίκτυα ad hoc, τα δορυφορικά δίκτυα, τα κυψελοειδή δίκτυα και τα ασύρματα δίκτυα αισθητήρων. Κάθε μία από αυτές τις τεχνολογίες έχει μοναδικά χαρακτηριστικά και εφαρμογές που παρουσιάζονται παρακάτω:

- **Δίκτυα Ad-hoc:** Τα ad-hoc δίκτυα είναι δυναμικά και αυτοδιαμορφούμενα ασύρματα συστήματα στα οποία οι συσκευές συνεργάζονται για να δημιουργήσουν ένα προσωρινό δίκτυο. Τα δίκτυα αυτά, παρέχουν την καλύτερη επιλογή για αξιόπιστες και άμεσες επικοινωνίες, ιδίως στο πλαίσιο του IoT, όπου οι συσκευές μπορεί να είναι κινητές ή να βρίσκονται σε μεταβαλλόμενα περιβάλλοντα. Η ικανότητα των δικτύων αυτών για αυτόματη διαμόρφωση και αναδιαμόρφωση, τους επιτρέπει να προσαρμόζονται δυναμικά στις

μεταβαλλόμενες συνθήκες και να εγγυώνται αξιόπιστη επικοινωνία ακόμη και όταν η δημιουργία μιας προϋπάρχουσας υποδομής είναι ανέφικτη ή περιττή. Συνεπώς, μπορούν να ταξινομηθούν περαιτέρω σε μικρότερες ομάδες που απευθύνονται σε συγκεκριμένες εφαρμογές του IoT.

- **Κινητά Ad-hoc Δίκτυα (Mobile Ad-hoc Network, MANET):** Τα MANETs είναι αποδομημένα δίκτυα που επιτρέπουν στις κινητές συσκευές να επικοινωνούν χωρίς την χρήση σταθερής υποδομής. Έχουν εφαρμογές σε δυναμικά σενάρια όπως οι στρατιωτικές επιχειρήσεις, η αντιμετώπιση καταστροφών, όπου οι συσκευές μπορούν να μετακινούνται ελεύθερα και η τοπολογία του δικτύου αλλάζει δυναμικά [24].
- **Δίκτυα Ad-hoc για Οχήματα (Vehicular Ad-hoc Network, VANET):** Τα VANETs περιλαμβάνουν οχήματα που επικοινωνούν μεταξύ τους με σκοπό την βελτίωση της οδικής κυκλοφορίας.. Η δυνατότητα ανταλλαγής πληροφοριών για την κατάσταση της κυκλοφορίας σε πραγματικό χρόνο είναι ένα από τα κύρια πλεονεκτήματα των VANETs. Αυτό επιτρέπει στα αυτοκίνητα να λάβουν προληπτικά μέτρα μόλις αντιληφθούν πιθανούς κινδύνους, όπως συγκρούσεις. Επίσης, υπάρχει βελτίωση της ολικής κίνησης, επιτρέποντας στους οδηγούς να λαμβάνουν αποτελεσματικές αποφάσεις για την πορείας τους [25].
- **Δίκτυα Ad-hoc για Ιπτάμενα Οχήματα (Flying Ad-hoc Network, FANET):** Τα μη επανδρωμένα εναέρια οχήματα (UAVs), γνωστά και ως drones, αποτελούν μια εξελιγμένη κατηγορία δικτύων γνωστών ως FANETs, τα οποία αποτελούνται από drones που συνδέονται προσωρινά μεταξύ τους για να σχηματίσουν δυναμικά δίκτυα επικοινωνίας. Τα δίκτυα αυτά είναι φτιαγμένα για να εκτελούν συνεργατικές επιχειρήσεις, αξιοποιώντας τις ειδικές ικανότητες που παρέχουν. Ένα από τα βασικά πλεονεκτήματα είναι η γρήγορη ανάπτυξή τους. Τα UAVs είναι κατάλληλα για εφαρμογές όπως η επιτήρηση χώρων, η αντιμετώπιση έκτακτης ανάγκης και η περιβαλλοντική παρακολούθηση. Είναι πολύ χρήσιμα σε καταστάσεις που απαιτούν γρήγορες αντιδράσεις, λόγω της ικανότητας τους να παρέχουν εναέρια κάλυψη σε μεγάλες περιοχές [26].
- **Θαλάσσια Ad-hoc Δίκτυα (Sea Ad-hoc Network, SANET):** Τα SANETs σχηματίζονται από κόμβους σκαφών, συμπεριλαμβανομένων πλοίων και υποβρύχιων οχημάτων, χωρίς την ανάγκη σταθερής υποδομής. Μια από τις κύριες χρήσεις των SANETs είναι η χαρτογράφηση, καθώς μπορούν να εφαρμοστούν για τη συλλογή γεωγραφικών πληροφοριών σε απομακρυσμένες θαλάσσιες περιοχές. Επιπλέον, προσφέροντας δεδομένα σχετικά με τα θαλάσσια ρεύματα και την ποιότητα του νερού, υποστηρίζουν την περιβαλλοντική παρακολούθηση. Επιπρόσθετα, υποστηρίζουν ερευνητικές δραστηριότητες σε τομείς όπως η ωκεανογραφία και η θαλάσσια βιολογική έρευνα, προσφέροντας ένα ευέλικτο και αποτελεσματικό μέσο για τη συλλογή δεδομένων και τη διεξαγωγή πειραμάτων σε δύσκολα περιβάλλοντα [27].




Σχήμα 2.2: *Κατηγορίες Ad-hoc Δικτύων* [28]

- **Δορυφορικά Δίκτυα:** Οι δορυφορικές επικοινωνίες ξεχωρίζουν ως καθοριστικά στοιχεία που προωθούν την συνδεσιμότητα του IoT σε όλη την έκταση του πλανήτη. Στις μεγάλες περιοχές όπου τα επίγεια δίκτυα συναντούν εμπόδια, τα δορυφορικά δίκτυα χρησιμοποιούν τις δυνατότητες τους για να καλύψουν αποτελεσματικά τα κενά επικοινωνίας. Προκειμένου να διασφαλιστεί ένα ευρύ και αξιόπιστο τοπίο, τα δίκτυα καθίστανται απαραίτητα για την αντιμετώπιση των προκλήσεων που θέτουν τα απομακρυσμένα, απομονωμένα ή γεωγραφικά πολύπλοκα περιβάλλοντα [29].
- **Κυψελοειδή Δίκτυα:** Με την ευρεία κάλυψη τους και την ικανότητα τους να υποστηρίζουν ένα ευρύ φάσμα εφαρμογών σε διάφορα πλαίσια, τα κυψελοειδή δίκτυα αποτελούν βασική τεχνολογία της ασύρματης συνδεσιμότητας. Εξελισσόμενα μέσα από γενιές, από το 3G και πλέον στο ανερχόμενο 6G, τα δίκτυα αυτά έχουν καταστεί απαραίτητα για την σύγχρονη επικοινωνία και για τον κόσμο του IoT. Παρέχουν την βάση για πολλές εφαρμογές IoT, που κυμαίνονται από τα έξυπνα σπίτια και τον βιομηχανικό αυτοματισμό εως την υγειονομική περίθαλψη και την έξυπνη γεωργία [30].
- **Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensors Network, WSN):** Τα WSNs κατέχουν ξεχωριστή θέση μεταξύ των διαφόρων ασύρματων τεχνολογιών, επειδή είναι αφιερωμένα στην συλλογή δεδομένων από το εξωτερικό περιβάλλον σε πραγματικό χρόνο. Αποτελούνται από χωρικά διασκορπισμένους, αυτόνομους αισθητήρες που συνεργάζονται για να παρατηρούν και να συλλέγουν δεδομένα για το περιβάλλον τους [7]. Τα WSNs γίνονται όλο και πιο διαδεδομένα σε πολλές εφαρμογές, όπως η γεωργία, η υγειονομική περίθαλψη και η περιβαλλοντική παρακολούθηση, χάρη στο χαμηλό κόστος της τεχνολογίας των αισθητήρων [31].

## 2.4 Τοπολογίες

Η αρχιτεκτονική για την σύνδεση των συσκευών μεταξύ τους στο IoT, προκύπτει μέσω μιας ποικιλίας τοπολογιών δικτύου. Αυτές οι τοπολογίες καθορίζουν τον τρόπο με τον οποίο οι συσκευές συνδέονται και ανταλλάσσουν δεδομένα. Οι κύριες τοπολογίες δικτύου για εφαρμογές IoT με βάση την επικρατέστερη είναι οι εξής:

- **Τοπολογία Αστέρα (Star Topology):** Ένας κεντρικός κόμβος συνδέεται με κάθε συσκευή σε σχήμα αστέρα, η οποία βελτιώνει την αρχιτεκτονική και επιτρέπει την ομαλή επικοινωνία. Λόγω της απλής αρχιτεκτονικής της, η τοπολογία αστέρα είναι μια χρήσιμη επιλογή για διάφορες εφαρμογές του IoT. Παρόλα αυτά, είναι ευάλωτη σε περίπτωση αποτυχίας του κεντρικού κόμβου. Σε περίπτωση δυσλειτουργίας ή αποσύνδεσης του κεντρικού κόμβου, ολόκληρο το δίκτυο μπορεί να επηρεαστεί, περιορίζοντας τη διαθεσιμότητα των υπηρεσιών [32].
- **Τοπολογία Πλέγματος (Mesh Topology):** Η τοπολογία πλέγματος εμφανίζεται ως μια ανθεκτική και δυναμική αρχιτεκτονική. Κάθε κόμβος έχει την δυνατότητα να συνδεθεί με πολλαπλούς κόμβους με αποτέλεσμα, για την αναμετάδοση ενός μηνύματος να υπάρχουν πολλαπλά μονοπάτια [33]. Η τοπολογία πλέγματος έχει πλεονεκτήματα αλλά κατά την αξιολόγηση του για την υλοποίηση σε εφαρμογές IoT, θα πρέπει να λαμβάνονται υπόψη οι πιθανές απαιτήσεις σε πόρους [32].
- **Σημείο προς Σημείο (Point-to-Point, P2P):** Η τοπολογία P2P χρησιμοποιεί μια κατανεμημένη και αποκεντρωμένη αρχιτεκτονική που επιτρέπει στις συσκευές να επικοινωνούν απευθείας μεταξύ τους, εξαλείφοντας την ανάγκη για ενδιάμεσους κόμβους. Αυτή η τοπολογία έχει πολλά πλεονεκτήματα για τον τομέα του IoT, καθιστώντας τις εφαρμογές πιο ευέλικτες και προσαρμόσιμες. Επιπλέον, αυτή η αποκεντρωμένη προσέγγιση ενισχύει την επεκτασιμότητα, επιτρέποντας την ομαλή ενσωμάτωση νέων συσκευών χωρίς καθυστέρηση [34].
- **Daisy Chain:** Οι συσκευές συνδέονται με διαδοχικό τρόπο για την δημιουργία μιας γραμμικής αλυσίδας στην οποία κάθε συσκευή μπορεί να επικοινωνεί με κάθε άλλη συσκευή που βρίσκεται σε κοντινή απόσταση. Αυτή η τοπολογία είναι χρήσιμη σε περιπτώσεις όπου είναι απαραίτητη μια ευθύγραμμη ροή δεδομένων. Το μειονέκτημα της είναι ότι μπορεί να είναι ευαίσθητη σε διακοπές. Εάν μια συσκευή στην αλυσίδα παρουσιάσει βλάβη, αυτό μπορεί να έχει αντίκτυπο στην επικοινωνία των επόμενων συσκευών [12], [35].
- **Τοπολογία Δέντρου Συστάδων (Cluster Tree Topology):** Η Cluster Tree τοπολογία τοποθετεί τις συσκευές στρατηγικά, εκμεταλλεύοντας τα πλεονεκτήματα που προσφέρουν η ομαδοποίηση και οι δομές δέντρων [36]. Σε αυτή την διάταξη οι συσκευές είναι οργανωμένες σε συστάδες και κάθε συστάδα διοικείται από ένα καθορισμένο κόμβο-επικεφαλή. Μία ιεραρχική δενδροειδής δομή σχηματίζεται στην συνέχεια από τον κάθε επικεφαλή, επιτρέποντας την αποτελεσματική συγκέντρωση και μετάδοση των δεδομένων. Αυτή η τοπολογία είναι επωφελής για εφαρμογές μεγάλης κλίμακας και περιορισμένων πόρων, επειδή διευκολύνει την αποτελεσματική διαχείριση τους [32].

## 2.5 Επίλογος

Σε αυτή την λεπτομερή εξέταση των βάσεων του δικτύου IoT, παρουσιάστηκαν τόσο τα ενσύρματα όσο και τα ασύρματα δίκτυα. Περιγράφηκε το ευρύ φάσμα επιλογών συνδεσιμότητας που είναι διαθέσιμες για την ανάπτυξη του IoT, που κυμαίνονται από την αξιοπιστία των ενσύρματων τεχνολογιών και μέσων όπως είναι το Ethernet, οι οπτικές ίνες, το DSL και το PLC έως την προσαρμοστικότητα των ασύρματων τεχνολογιών όπως τα WBAN, WPAN, WLAN, WMAN, WWAN, τα ad-hoc δίκτυα, οι δορυφορικές επικοινωνίες, τα κυψελοειδή δίκτυα και τα WSN. Επιπλέον, η ανάλυση διαφόρων τοπολογιών δικτύου, συμπεριλαμβανομένων των τοπολογιών αστέρα, πλέγματος, P2P, daisy chain και δέντρου συστάδων, κατέδειξε σημαντικούς αρχιτεκτονικούς παράγοντες που πρέπει να λαμβάνονται υπόψη κατά την ανάπτυξη επεκτάσιμων και ανθεκτικών υποδομών IoT. Η κατανόηση των βασικών αρχών του δικτύου θα είναι πάντα απαραίτητη για την επιτυχία των αναπτύξεων του IoT, καθώς το περιβάλλον του αναπτύσσεται με γοργούς ρυθμούς.

# 3. Ανάλυση του IoT

## 3.1 Εισαγωγή

Η κατανόηση των λεπτομερειών αυτού του διασυνδεδεμένου κόσμου, απαιτεί την γνώση των θεμελιωδών στοιχείων, των αρχιτεκτονικών και των τεχνολογιών του IoT. Αυτή η λεπτομερής εξέταση εμβαθύνει στους αισθητήρες, τους ενεργοποιητές και τα πολύπλοκα επίπεδα επικοινωνίας και υπολογισμού που συνθέτουν το IoT. Αποκτούμε μία αντίληψη των δομικών πλαισίων που υποστηρίζουν την ανάπτυξη του IoT, αναλύοντας προσεκτικά τις αρχιτεκτονικές του IoT, συμπεριλαμβανομένων των γνωστών μοντέλων αρχιτεκτονικής τριών, τεσσάρων, πέντε, έξι και επτά επιπέδων.

Το κεφάλαιο περιλαμβάνει επίσης τις τεχνολογίες που είναι κρίσιμες για την λειτουργικότητα κάθε επιπέδου στις αρχιτεκτονικές του IoT. Εμβαθύνει στις επιλογές συνδεσιμότητας που απαιτούνται για την οργάνωση των συστημάτων IoT, από τις θεμελιώδεις τεχνολογίες που επιτρέπουν την καταγραφή των δεδομένων στο επίπεδο αντίληψης έως τις διάφορες τεχνολογίες επικοινωνίας που υποστηρίζουν την μετάδοση των δεδομένων και την δικτύωση. Στην συνέχεια, το θέμα μεταφέρεται στο επίπεδο εφαρμογής, τονίζοντας την σημασία της αποτελεσματικής ανταλλαγής των δεδομένων.

Το κεφάλαιο ολοκληρώνεται με την εξέταση πρακτικών εφαρμογών του IoT σε διάφορους κλάδους, όπως το λιανικό εμπόριο, η υγειονομική περίθαλψη, η γεωργία, το έξυπνο δίκτυο, τα έξυπνα σπίτια, οι μεταφορές και η αυτοκινητοβιομηχανία.

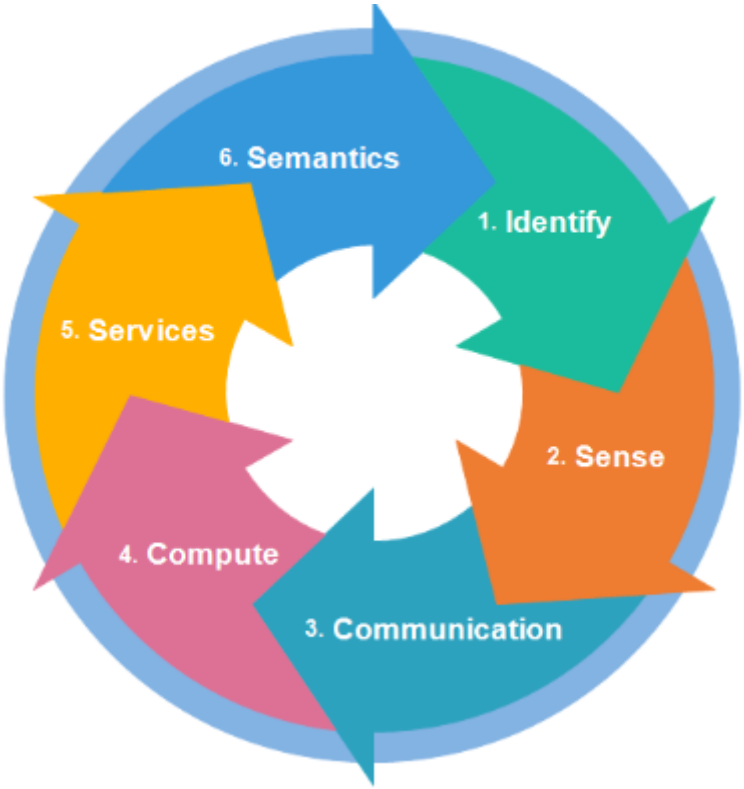
## 3.2 Στοιχεία του IoT

Όντας ένα πολύπλοκο περιβάλλον το IoT, απαιτεί μία προσεκτική μελέτη στα βασικά του στοιχεία, με τους αισθητήρες και τους ενεργοποιητές να αποτελούν βασικούς παράγοντες στην διαμόρφωση του ψηφιακού κόσμου. Η αναγνώριση και η ανίχνευση εκτελούνται από αισθητήρες, οι οποίοι λειτουργούν ως τα μάτια και τα αυτιά αυτού του δικτυωμένου συστήματος. Αυτές οι συσκευές είναι κατασκευασμένες για να καταγράφουν και να αναλύουν πραγματικά δεδομένα, μετατρέποντας τον εξωτερικό κόσμο σε ένα χρήσιμο πληροφοριακό περιβάλλον. Οι ενεργοποιητές, οι οποίοι αντιπροσωπεύουν τους αντιδραστικούς παράγοντες της αρχιτεκτονικής του IoT μπορούν να θεωρηθούν ως ο αντίθετος μηχανισμός ενός αισθητήρα. Χρησιμεύουν ως μετασχηματιστική δύναμη, μετατρέποντας την ενέργεια σε ακριβή κίνηση, ωθώντας έτσι τα μηχανικά συστήματα σε κάποια δράση. Δράσεις ενός συστήματος μπορεί να είναι ο έλεγχος ενός φυσικού μηχανισμού, η ρύθμιση της θερμοκρασίας ή της φωτεινότητας και οι φυσικές κινήσεις του μηχανήματος. Οι ενεργοποιητές, είτε τροφοδοτούνται από ηλεκτρικό ρεύμα, υδραυλικό υγρό ή άλλες πηγές ενέργειας, είναι απαραίτητοι για την παραγωγή γραμμικών, περιστροφικών ή ταλαντωτικών κινήσεων. Αυτές οι συσκευές έχουν μικρή εμβέλεια επικοινωνίας και συνήθως επικοινωνούν με ταχύτητα μικρότερη από 1 Mbps. Η τεχνολογική αγορά κυριαρχείται από τρεις κύριους τύπους ενεργοποιητών [37], [38]:

1. **Ηλεκτρικοί ενεργοποιητές:** Περιλαμβάνουν βηματικούς κινητήρες, κινητήρες εναλλασσόμενου και συνεχούς ρεύματος και σωληνοειδή.
2. **Υδραυλικοί ενεργοποιητές:** Χρησιμοποιούν υδραυλικό υγρό για την εκκίνηση της κίνησης.
3. **Πνευματικοί ενεργοποιητές:** Χρησιμοποιούν πεπιεσμένο αέρα για την εκκίνηση της κίνησης.

Όπως παρουσιάζεται στο Σχήμα 3.1, η ταυτοποίηση (identify), η ανίχνευση (sense), η επικοινωνία (communication), ο υπολογισμός (compute), οι υπηρεσίες (services) και η σημασιολογία

(semantic) είναι τα δομικά στοιχεία πάνω στα οποία βασίζεται το IoT. Όλα συνεργάζονται αρμονικά μεσα σε αυτό το δυναμικό περιβάλλον για να φέρουν εις πέρας την ιδέα του διασυνδεδεμένου κόσμου.




Σχήμα 3.1: *Τα στοιχεία του IoT* [39]

### 3.2.1 Ταυτοποίηση

Το κρίσιμο στοιχείο της ταυτοποίησης θέτει τις βάσεις για την ομαλή επικοινωνία και την αλληλεπίδραση στον κόσμο του IoT. Η ακριβής και σαφής ταυτοποίηση καθίσταται ζωτικής σημασίας σε αυτό το δικτυωμένο περιβάλλον όπου καθημερινά αντικείμενα και μηχανήματα υψηλής τεχνολογίας αλληλεπιδρούν μαζί. Η ονοματοδοσία, που αντιπροσωπεύεται από τεχνολογίες όπως ο ηλεκτρονικός κωδικός προϊόντος (Electronic Product Code, EPC), είναι ένας τρόπος για να δοθεί σε κάθε συσκευή IoT ένα ψηφιακό αποτύπωμα που τις κάνει να ξεχωρίζουν η μία από την άλλη. Επιπλέον, η διευθυνσιοδότηση η οποία βασίζεται στα πρωτόκολλα IPv4/IPv6 (Internet Protocol version 4 / Internet Protocol version 6), προσφέρουν μία μοναδική διεύθυνση για την κάθε συσκευή. Το εύρος των διευθύνσεων IPv4 έχουν αγγίξει τα όρια από την εκθετική αύξηση των συσκευών IoT, γεγονός που αναδεικνύει την ανάγκη υιοθέτησης του IPv6 χάρη στην δυνατότητα διευθυνσιοδότησης με αριθμούς 128 bit σε σχέση με τα 32 bit που είχε το IPv4 [39].

### 3.2.2 Αίσθηση

Αίσθηση είναι ο όρος που χρησιμοποιείται για να περιγράψει πόσο εντυπωσιακό είναι το γεγονός ότι οι συσκευές IoT μπορούν να αντιλαμβάνονται, να συλλέγουν και να αναλύουν δεδομένα από το περιβάλλον τους. Η βασική λειτουργία αυτού του στοιχείου είναι να παρέχει στις συσκευές μία ποικιλία αισθητήρων, ώστε να μπορούν να αντιλαμβάνονται και να αντιδρούν στις μεταβολές του περιβάλλοντος τους [40].

### 3.2.3 Επικοινωνία

Στο IoT, η επικοινωνία είναι απαραίτητη για την ομαλή αλληλεπίδραση μεταξύ των συσκευών και την ανταλλαγή δεδομένων. Το στοιχείο αυτό περιλαμβάνει μία σειρά από πρωτόκολλα επικοινωνίας και τεχνολογίες που επιτρέπουν στις συσκευές να στέλνουν, να λαμβάνουν και να επεξεργάζονται αποτελεσματικά τα δεδομένα. Η επιλογή των τεχνολογιών επικοινωνίας εξαρτάται από παράγοντες όπως η εμβέλεια, ο ρυθμός μετάδοσης των δεδομένων και η ενεργειακή απόδοση. Παραδείγματα αποτελούν οι ασύρματες τεχνολογίες μικρής εμβέλειας, όπως το Bluetooth και το Zigbee, καθώς και οι λύσεις μεγάλης εμβέλειας, όπως τα κυψελοειδή δίκτυα [39].

### 3.2.4 Υπολογιστικές Ικανότητες

Ο υπολογισμός αναφέρεται στον χειρισμό των δεδομένων που συλλέγονται από διάφορα αντικείμενα με την χρήση των αισθητήρων. Ο κύριος στόχος είναι η αφαίρεση των περιττών πληροφοριών, προκειμένου να γίνει πιο αποτελεσματική χρήση. Για την εκτέλεση αυτού του υπολογιστικού ρόλου, έχει σχεδιαστεί μία ποικιλία από πλατφόρμες υλικού (hardware), όπως το Arduino, το Raspberry Pi και το Intel Galileo. Ταυτόχρονα, μία σειρά από πλατφόρμες λογισμικού (software), συμπεριλαμβανομένων των Tiny OS, Lite OS και Android, συμβάλλουν στην αποτελεσματική επεξεργασία των δεδομένων, διαμορφώνοντας ένα ολοκληρωμένο περιβάλλον για τις IoT εφαρμογές [19], [39].

### 3.2.5 Υπηρεσίες

Οι υπηρεσίες, οι οποίες παρέχουν μία σειρά δυνατοτήτων από την αποθήκευση και την ανάκτηση των δεδομένων εως την ανάλυση σε πραγματικό χρόνο και την αυτοματοποίηση, είναι απαραίτητες για την βελτίωση της συνολικής εμπειρίας του IoT. Οι υπηρεσίες IoT κατατάσσονται σε τέσσερις διαφορετικές κατηγορίες [19], [39]:

1. **Υπηρεσίες ταυτότητας (Identity-related Services):** Οι υπηρεσίες που σχετίζονται με την ταυτότητα διαδραματίζουν καθοριστικό ρόλο στη διαχείριση και τον καθορισμό της ταυτότητας των συσκευών IoT.
2. **Υπηρεσίες συγκέντρωσης πληροφοριών (Information-aggregation Services):** Οι υπηρεσίες για την συγκέντρωση πληροφοριών είναι απαραίτητες για την συλλογή, την οργάνωση και την επεξεργασία των δεδομένων. Αυτές οι υπηρεσίες συλλέγουν μη επεξεργασμένα δεδομένα από αισθητήρες και συσκευές, τα μετατρέπουν σε χρήσιμες πληροφορίες και τα προωθούν στην επόμενη υπηρεσία έτσι ώστε να ληφθούν αποφάσεις.
3. **Υπηρεσίες συνεργατικής ευαισθητοποίησης (Collaborative-Aware Services):** Οι πληροφορίες που συλλέγονται από τις υπηρεσίες συγκέντρωσης πληροφοριών, προωθούνται στις υπηρεσίες συνεργατικής ευαισθητοποίησης. Οι υπηρεσίες αυτές επικεντρώνονται στην ανάλυση των συλλεχθέντων δεδομένων και στην παροχή ενημερωμένων απαντήσεων στις εμπλεκόμενες συσκευές.
4. **Πανταχού παρούσες υπηρεσίες (Ubiquitous Services):** Οι πανταχού παρούσες υπηρεσίες εγγυώνται συνεχείς λειτουργικότητα σε διάφορες συνθήκες και περιβάλλοντα. Προκειμένου να βελτιώσουν την συνολική εμπειρία του χρήστη, παρέχουν εξατομικευμένες υπηρεσίες για να εξασφαλίσουν πανταχού παρούσα συνδεσιμότητα.

### 3.2.6 Σημασιολογία

Η σημασιολογία είναι υπεύθυνη για την διαχείριση των εργασιών και για την εξαγωγή των πληροφοριών από τις συνδεδεμένες συσκευές. Η σημασιολογία είναι ο "εγκέφαλος" του IoT. Περιλαμβάνει την λήψη διαφόρων δεδομένων, ώστε να μπορεί να λαμβάνει αποφάσεις και να στέλνει προσαρμοσμένα μηνύματα στις συσκευές που είναι συνδεδεμένες. Εμπεριέχει επίσης την διαχείριση των πόρων, την μοντελοποίηση των πληροφοριών και την εξαγωγή πληροφοριών από την αλληλεπίδραση των συσκευών. Ο κρίσιμος ρόλος της σημασιολογίας στο IoT αναδεικνύεται από τεχνολογίες όπως το Πλαίσιο Περιγραφής Πόρων (Resource Description Framework, RDF) και η Γλώσσα Οντολογίας Ιστού (Web Ontology Language, OWL), οι οποίες επιτρέπουν στην σημασιολογία να στέλνει ακριβή αιτήματα στους σωστούς πόρους [19].

## 3.3 Αρχιτεκτονικές IoT

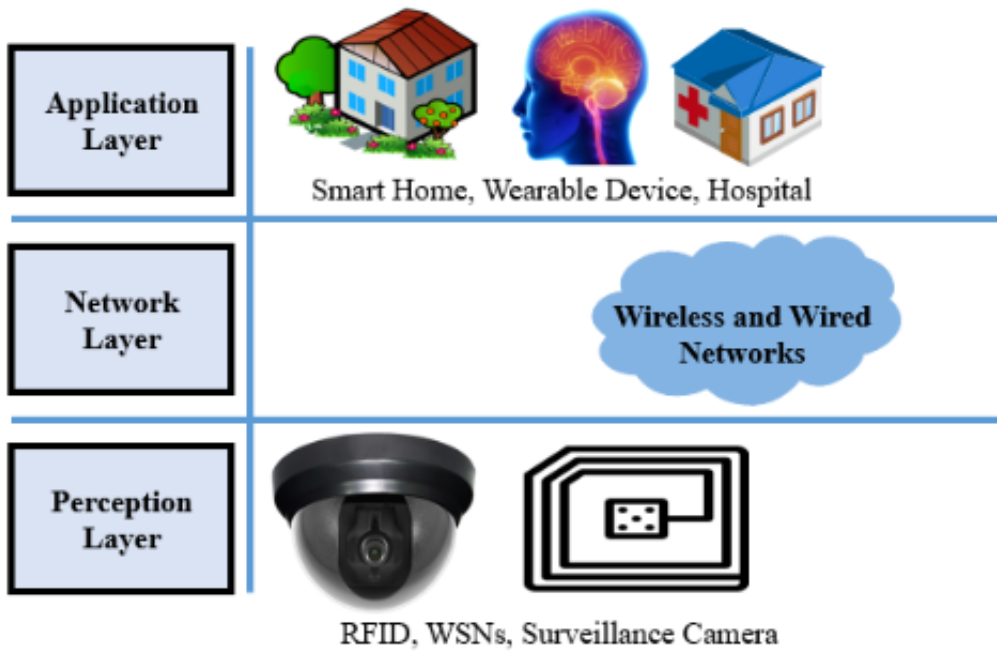
Το IoT διακρίνεται από ένα ευρύ φάσμα αρχιτεκτονικών μοντέλων, καθένα από τα οποία παρέχει μια ξεχωριστή άποψη για τον συντονισμό των διασυνδεδεμένων συσκευών και την ανταλλαγή πληροφοριών. Ωστόσο, η επιστημονική κοινότητα έχει προτείνει διάφορες πολυεπίπεδες προσεγγίσεις, οι οποίες στην πλειονότητα τους μετρούν από τρία έως επτά επίπεδα. Αυτό οφείλεται στο γεγονός ότι οι μελετητές και οι ερευνητές δεν έχουν καταλήξει σε ένα οριστικό συμπέρασμα σχετικά με το πόσα επίπεδα πρέπει να αποτελείται η αρχιτεκτονική του IoT επειδή η καθεμία έχει μοναδικά οφέλη και ιδιαιτερότητες.

Η παρούσα έρευνα χρησιμοποιεί μία εστιασμένη διερεύνηση της αρχιτεκτονικής τριών επιπέδων, η οποία αποτελείται από τα επίπεδα αντίληψης (perception), δικτύου (network) και εφαρμογής (application), ως τον κύριο ερευνητικό της μονοπάτι. Παρόλα αυτά, το παρόν υποκεφάλαιο επεκτείνεται για να εξετάσει και τις υπόλοιπες αρχιτεκτονικές, επιδιώκοντας να αποκαλύψει τα πιθανά πλεονεκτήματα των πιο πολύπλοκων δομών.

Ξεκινώντας, η προσέγγιση τριών επιπέδων αποτελείται από τα ακόλουθα επίπεδα [5], [10], [39], [40]:

1. **Επίπεδο αντίληψης:** Το επίπεδο αντίληψης είναι το χαμηλότερο επίπεδο στην ιεραρχία και χρησιμοποιώντας μια ποικιλία αισθητήρων και ενεργοποιητών, παρουσιάζεται ως το κρίσιμο σημείο σύνδεσης του φυσικού και του ψηφιακού κόσμου. Αυτό το επίπεδο έχει ως καθήκον τον εντοπισμό των συσκευών και την συλλογή των δεδομένων από αυτές. Οι βασικές τεχνολογίες αισθητήρων αυτού του επιπέδου περιλαμβάνουν RFID για την αναγνώριση των συσκευών, συστήματα καμερών για την καταγραφή οπτικών δεδομένων, αισθητήρες θερμοκρασίας που είναι απαραίτητοι για την παρακολούθηση του περιβάλλοντος και αισθητήρες που είναι ικανοί να ανιχνεύουν την παρουσία ή μη κοντινών αντικειμένων. Χρησιμοποιώντας τεχνολογίες όπως σαρωτές Barcode/QR code για την ταυτοποίηση αντικειμένων και GPS για τον ακριβή γεωγραφικό εντοπισμό, το επίπεδο αντίληψης υπερέχει σε λειτουργίες που σχετίζονται με τον εντοπισμό και την ταυτοποίηση εκτός από την συλλογή δεδομένων. Επίσης μία κομβική πτυχή της λειτουργικότητας αυτού του επιπέδου είναι η προεπεξεργασία, όπου βελτιώνει και προετοιμάζει τα δεδομένα για την μετάδοση σε ανώτερα επίπεδα. Οι μικροελεγκτές που είναι ενσωματωμένοι σε συσκευές αισθητήρων παίζουν καθοριστικό ρόλο στην επεξεργασία και την μετατροπή αναλογικών σημάτων σε ψηφιακές μορφές [5]. Το επίπεδο αντίληψης είναι ουσιαστικά το θεμέλιο του IoT, διασφαλίζοντας ότι η ψηφιακή απεικόνιση του πραγματικού κόσμου είναι ακριβής και ουσιαστική.

2. **Επίπεδο δικτύου:** Ένα από τα πιο σημαντικά μέρη της αρχιτεκτονικής του IoT είναι το επίπεδο δικτύου, το οποίο συνδέει και επικοινωνεί με τις διάφορες διασυνδεδεμένες συσκευές. Βρίσκεται μεταξύ των επιπέδων αντίληψης και εφαρμογής και αποτελεί μία γέφυρα επικοινωνίας. Ο κύριος στόχος του είναι η μεταφορά των πληροφοριών που λαμβάνονται από τις συσκευές, στην μονάδα επεξεργασίας πληροφοριών ή σε ανώτερες μονάδες λήψης αποφάσεων. Κρίσιμες διεργασίες όπως η ανάλυση, η εξόρυξη δεδομένων και η κωδικοποίηση πραγματοποιούνται σε αυτή την μετάδοση, η οποία έρχεται εις πέρας τόσο από ενσύρματα όσο και από ασύρματα κανάλια. Σημαντικές τεχνολογίες δικτύωσης, όπως το Bluetooth, Wi-Fi, ZigBee και LoRa, αξιοποιούνται για την κάλυψη συγκεκριμένων αναγκών επικοινωνίας [5].
3. **Επίπεδο εφαρμογής:** Τοποθετημένο στην κορυφή της στοίβας, το επίπεδο εφαρμογών διαδραματίζει καθοριστικό ρόλο με διακριτούς σκοπούς και αρμοδιότητες. Ο κύριος στόχος του είναι η διαχείριση και η παροχή εφαρμογών, με την χρήση του τεράστιου όγκου δεδομένων που λαμβάνονται από το επίπεδο αντίληψης και επεξεργάζονται από την μονάδα επεξεργασίας πληροφοριών. Το αποτέλεσμα είναι η παροχή εξατομικευμένων υπηρεσιών που ανταποκρίνονται στις ξεχωριστές απαιτήσεις και προτιμήσεις κάθε τελικού χρήστη σε όλο το δίκτυο. Εκτός από την βελτίωση της εμπειρίας των χρηστών, αυτή η προσαρμοσμένη στρατηγική βοηθά τους ανθρώπους να δημιουργήσουν βαθύτερους δεσμούς με τις εφαρμογές που επηρεάζουν την αλληλεπίδραση τους με το IoT [5].



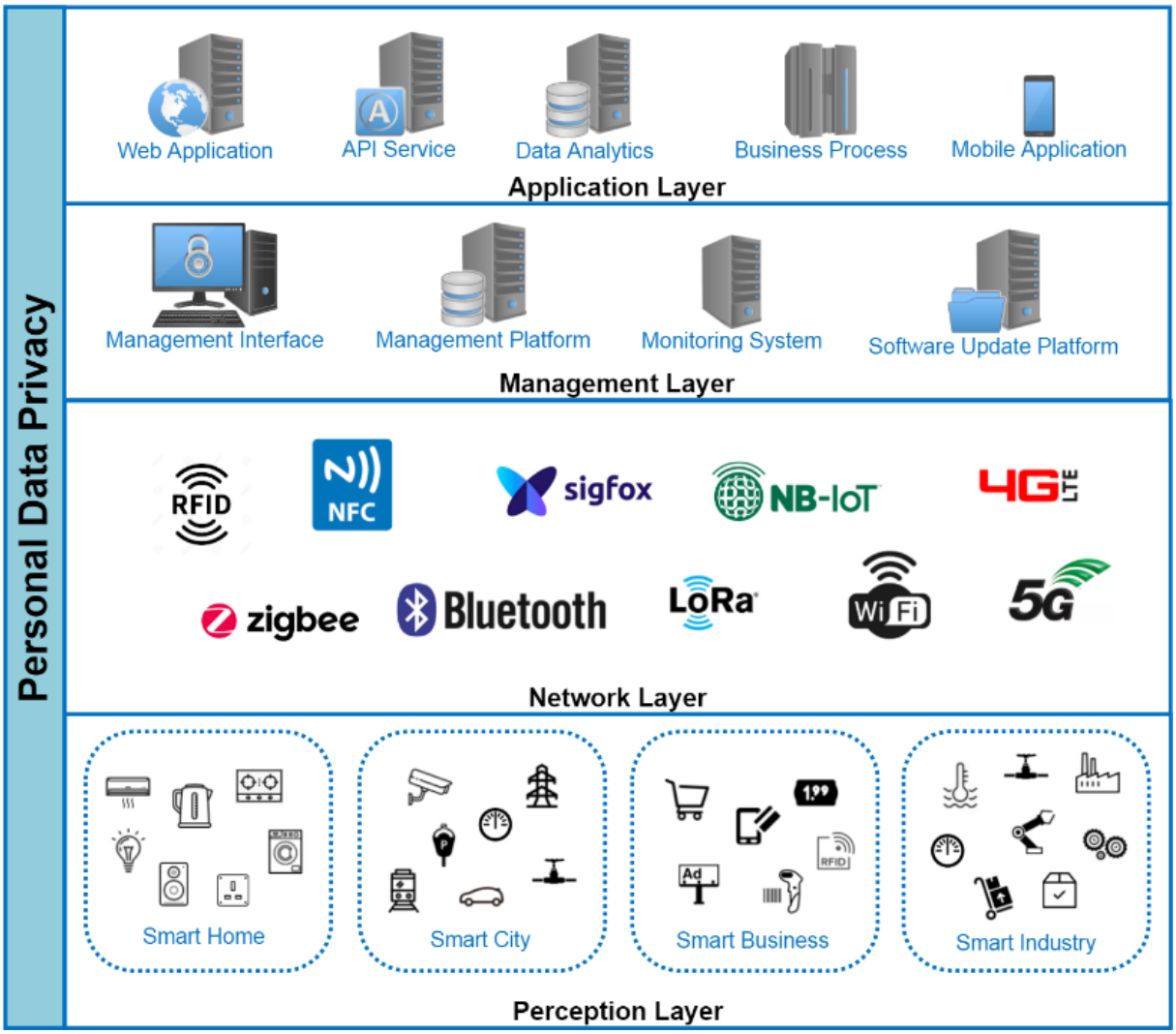

Σχήμα 3.2: *Η αρχιτεκτονική τριών επιπέδων του IoT* [39]

Καθώς μεταβαίνουμε από την γνωστή αρχιτεκτονική τριών επιπέδων στα πιο προηγμένα μοντέλα αρχιτεκτονικής, υπάρχει μια αξιοσημείωτη βελτίωση που πρέπει να αναφέρουμε. Αυτές οι αρχιτεκτονικές εξελίξεις προσθέτουν νέα επίπεδα και βελτιώνουν την κατανόηση της λειτουργίας των συστημάτων IoT. Αυτά τα πρόσθετα επίπεδα βοηθάνε στο να χρησιμοποιηθεί η κάθε μία αρχιτεκτονική σε πιο εξειδικευμένες εφαρμογές.

Η μετάβαση από την αρχιτεκτονική τριών επιπέδων στην αρχιτεκτονική τεσσάρων επιπέδων διατηρεί τις βασικές λειτουργίες των επιπέδων αντίληψης και δικτύου και προσθέτει το καινούργιο επίπεδο διαχείρισης μεταξύ των επιπέδων δικτύου και εφαρμογής. Το επίπεδο αντίληψης, που

περιλαμβάνει αισθητήρες και συσκευές, συνεχίζει τον ρόλο του στην συλλογή των ακατέργαστων δεδομένων από το περιβάλλον. Ταυτόχρονα, το επίπεδο δικτύου διαχειρίζεται αποτελεσματικά την μετάδοση των δεδομένων και την επικοινωνία, εξασφαλίζοντας συνδεσιμότητα και δρομολόγηση.

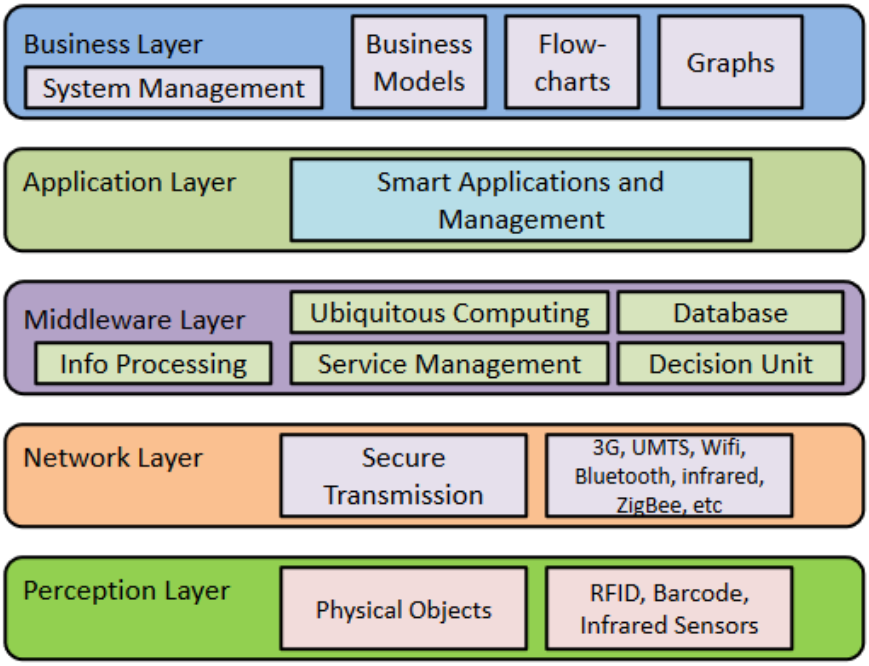
Το επίπεδο διαχείρισης (management layer) έχει ως βασική λειτουργία την αυτόνομη διαχείριση των συσκευών με την έννοια της παροχής, της παρακολούθησης, της ενημέρωσης, του ελέγχου και της εφαρμογής μέτρων ασφαλείας στις συσκευές IoT. Με εξαίρεση τις διαφορετικές διαδικασίες διαχείρισης που πραγματοποιούνται πριν από την παροχή των δεδομένων στον τελικό χρήστη για αλληλεπίδραση, το επίπεδο εφαρμογής είναι ουσιαστικά το ίδιο. Σε αυτό το επίπεδο έχουν πρόσβαση κυρίως οι τελικοί χρήστες μέσω διαδικτυακών και κινητών εφαρμογών. Τα χαρακτηριστικά του είναι αξιοσημείωτα επειδή υπερβαίνουν το λογισμικό του τελικού χρήστη και περιλαμβάνουν υπηρεσίες backend, όπως η ανάλυση δεδομένων big-data, υπηρεσίες API, εφαρμογή του ML και μοντελοποίηση τεχνητής νοημοσύνης (Artificial Intelligence, AI) [39], [41], [42].




Σχήμα 3.3: *Η αρχιτεκτονική τεσσάρων επιπέδων του IoT* [41]

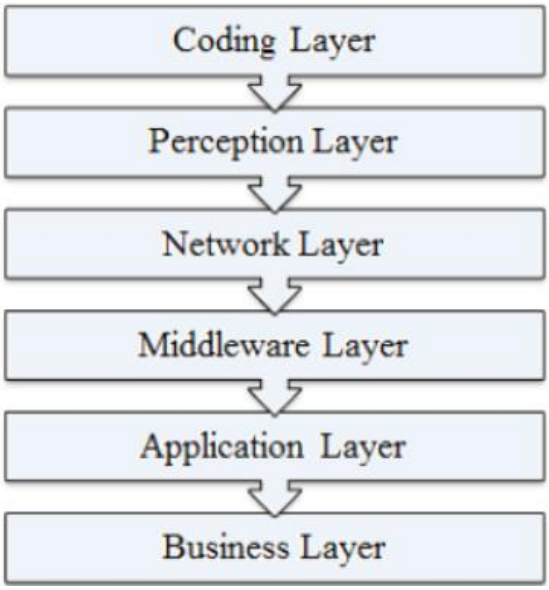
Στην αρχιτεκτονική πέντε επιπέδων, το επιχειρηματικό επίπεδο (business layer) αναλαμβάνει στρατηγικό ρόλο, εκτελώντας ποικίλα καθήκοντα για την διαμόρφωση της αποτελεσματικότητας του συστήματος. Αυτό το επίπεδο είναι υπεύθυνο για την ανάπτυξη ενός πλήρους επιχειρηματικού μοντέλου, χρησιμοποιώντας ως βάση τα δεδομένα που λαμβάνονται από το επίπεδο εφαρμογής. Το επιχειρηματικό επίπεδο στοχεύει στην αναπαράσταση της πολυπλοκότητας του συστήματος IoT,

μετατρέποντας τα δεδομένα σε χρήσιμες πληροφορίες, χρησιμοποιώντας διάφορα εργαλεία, όπως γραφήματα και διαγράμματα ροής δεδομένων. Πέρα από την μοντελοποίηση, επίσης εμπλέκεται και στις υπόλοιπες πτυχές του κύκλου ζωής ενός συστήματος, συμπεριλαμβανομένου του σχεδιασμού, της ανάλυσης, της υλοποίησης, της αξιολόγησης, της παρακολούθησης και της συνεχούς ανάπτυξης. Επιπλέον, αναλαμβάνει τον κρίσιμο ρόλο της επίβλεψης και του ελέγχου των τεσσάρων υποκείμενων επιπέδων για να εγγυάται μέγιστη απόδοση. Η ικανότητα του επιπέδου επιχειρηματικότητας να βοηθά στην λήψη αποφάσεων, προσφέροντας εύστοχες πληροφορίες που καθοδηγούν στις στρατηγικές αποφάσεις, είναι ένα από τα ιδιαίτερα χαρακτηριστικά του. Τέλος, είναι απαραίτητο για την μεγιστοποίηση των επενδυτικών επιλογών και τον συντονισμό των έργων IoT [19], [43].




Σχήμα 3.4: *Η αρχιτεκτονική πέντε επιπέδων του IoT* [44]

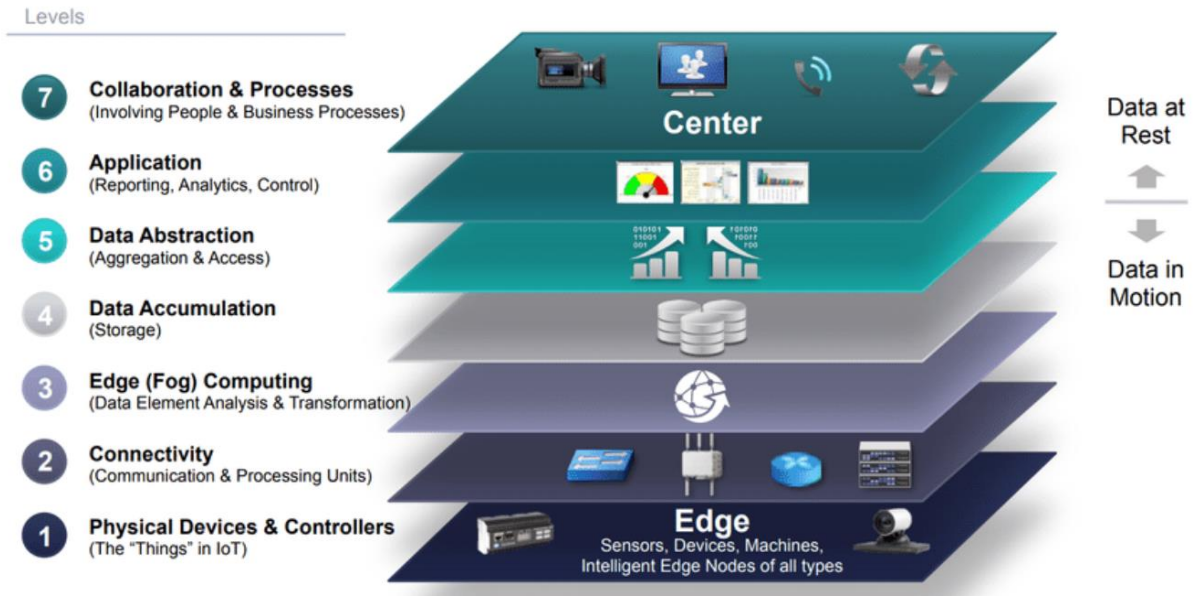
Αν και υπάρχει η αρχιτεκτονική έξι επιπέδων, δεν είναι τόσο δημοφιλής όσο μοντέλα όπως οι αρχιτεκτονικές τριών, τεσσάρων και πέντε επιπέδων. Αποτελείται συνήθως από τα επίπεδα της κωδικοποίησης (coding layer), της αντίληψης, του δικτύου, της διαχείρισης, της εφαρμογής και της επιχείρησης. Αυτό το μοντέλο εισάγει το επιπλέον επίπεδο της κωδικοποίησης για την βελτίωση της αναγνώρισης των αντικειμένων και της διαχείρισης του συστήματος [45], [46].




Σχήμα 3.5: *Η αρχιτεκτονική έξι επιπέδων του IoT* [46]

Τελευταία αρχιτεκτονική που θα παρουσιάσουμε είναι το μοντέλο των επτά επιπέδων. Είναι ένα ολοκληρωμένο μοντέλο που έχει σχεδιαστεί για να αντιμετωπίζει τις πολυπλοκότητες των σύγχρονων συστημάτων IoT, καθιστώντας το έναν αξιοσημείωτο διεκδικητή στον τομέα της αρχιτεκτονικής. Πέρα από την ακαδημαϊκή αναγνώριση, έχει προσελκύσει και κορυφαίες εταιρείες του χώρου. Μία από αυτές είναι η Cisco, όπου και χρησιμοποιεί την αρχιτεκτονική επτά επιπέδων για να αναδείξει την εφαρμοσιμότητα και την υιοθέτηση της στον τομέα αυτό. Σύμφωνα με την μελέτη [47], τα επίπεδα χωρίζονται ως εξής:

1. **Επίπεδο φυσικών συσκευών:** Περιλαμβάνει τις φυσικές συσκευές, όπως και στις προηγούμενες προσεγγίσεις.
2. **Επίπεδο συνδεσιμότητας:** Η συνδεσιμότητα, η οποία δίνει έμφαση στην ομαλή μεταφορά των δεδομένων, συμβαδίζει με τις προαναφερθείσες αρχιτεκτονικές.
3. **Επίπεδο Edge/Fog Computing:** Το επίπεδο Edge/Fog Computing είναι απαραίτητο για την μετατροπή και την ανάλυση των δεδομένων έτσι ώστε να καταστούν πιο αξιοποιήσιμα για το επίπεδο συσσώρευσης.
4. **Επίπεδο συσσώρευσης δεδομένων:** Στο επίπεδο συσσώρευσης δεδομένων εστιάζεται η ακρίβεια στην μεταφορά των δεδομένων, δίνοντας προτεραιότητα στην αξιοπιστία της ροής. Αυτό το επίπεδο λειτουργεί με στόχο την μετατροπή των δεδομένων σε μορφή χρήσιμη για τις εφαρμογές.
5. **Επίπεδο αφαίρεσης δεδομένων:** Η διαδικασία προετοιμασίας των δεδομένων για ανάλυση μέσω της εφαρμογής τεχνικών ML και εξόρυξης δεδομένων πραγματοποιείται στο επίπεδο αφαίρεσης δεδομένων. Έχει ως κύριο στόχο την βελτιστοποίηση της χρήσης των δεδομένων, ώστε να μπορούν να υποστηρίξουν την ευκολότερη ανάπτυξη των εφαρμογών, επιτυγχάνοντας παράλληλα υψηλότερα επίπεδα επιδόσεων.
6. **Επίπεδο εφαρμογής:** Το επίπεδο εφαρμογής εξακολουθεί και σε αυτό το μοντέλο αρχιτεκτονικής να είναι η διεπαφή που χρησιμοποιούν οι τελικοί χρήστες για να έχουν πρόσβαση στις πληροφορίες που συλλέγονται από τις εφαρμογές του IoT.
7. **Επίπεδο συνεργασίας και διαδικασιών:** Στο επίπεδο συνεργασίας και διαδικασιών περιλαμβάνονται οι οντότητες που χρησιμοποιούν τα δεδομένα. Επίσης είναι υπεύθυνο για την εκτέλεση προσαρμοσμένων εφαρμογών.




Σχήμα 3.6: *Η αρχιτεκτονική επτά επιπέδων του IoT - Cisco* [47]

## 3.4 Τεχνολογίες Ενεργοποίησης

Με βάση το ευρύ φάσμα αρχιτεκτονικών που εξετάστηκαν, το παρόν υποκεφάλαιο εμβαθύνει στην αρχιτεκτονική τριών επιπέδων που αποτελεί την βάση για πολλά συστήματα IoT. Αναγνωρίζοντας τον κρίσιμο ρόλο της στην διαμόρφωση του περιβάλλοντος IoT, θα διερευνηθούν οι τεχνολογίες και τα πρωτόκολλα που λειτουργούν σε κάθε επίπεδο αυτής της αρχιτεκτονικής.

### 3.4.1 Φυσικό επίπεδο

Καθώς εξετάζονται οι βασικές τεχνολογίες που ενεργοποιούν το επίπεδο αντίληψης των συστημάτων του IoT, είναι σαφές ότι η πολυπλοκότητα και η ποικιλομορφία αυτών των τεχνολογιών είναι κρίσιμες για τον καθορισμό των δυνατοτήτων του IoT. Οι τεχνολογίες που παρατίθενται παρακάτω αποτελούν την βάση του επιπέδου αντίληψης, καθεμία από τις οποίες διαδραματίζει ξεχωριστό ρόλο στην ικανότητα του IoT να αντιλαμβάνεται, να κατανοεί και να αλληλεπιδρά με το περιβάλλον.

- **RFID:** Το RFID είναι μία βασική τεχνολογία που χρησιμοποιείται για την παρακολούθηση, την ταυτοποίηση και την δικτύωση των συσκευών. Είναι ουσιαστικά μία μέθοδος συλλογής και μετάδοσης δεδομένων που χρησιμοποιεί σήματα ραδιοσυχνοτήτων για να επιτρέψει την επικοινωνία μεταξύ ηλεκτρονικών ετικετών (tags) και αναγνωστών (readers) [5]. Η εφεύρεση του RFID ξεκίνησε κατά την διάρκεια του Β' Παγκοσμίου Πολέμου, όταν απαιτήθηκε ένα νέο σύστημα ταυτοποίησης. Το σύστημα ταυτοποίησης φίλου ή εχθρού (Identification of Friend and Foe, IFF), η πρώτη τεχνολογία που έμοιαζε με την τεχνολογία RFID, δημιουργήθηκε με την ιδέα της χρήσης ραδιοκυμάτων για την ταυτοποίηση φιλικών αεροπλάνων. Το RFID άρχισε να χρησιμοποιείται ευρέως στο εμπόριο την δεκαετία του 1990 με την είσοδο του στις αλυσίδες εφοδιασμού. Σήμερα, η τεχνολογία RFID αποτελεί κρίσιμο στοιχείο του IoT, προωθώντας την καινοτομία σε πολλούς κλάδους και φέρνοντας επανάσταση στον τρόπο με τον οποίο αλληλεπιδρούμε με τα αντικείμενα [48].

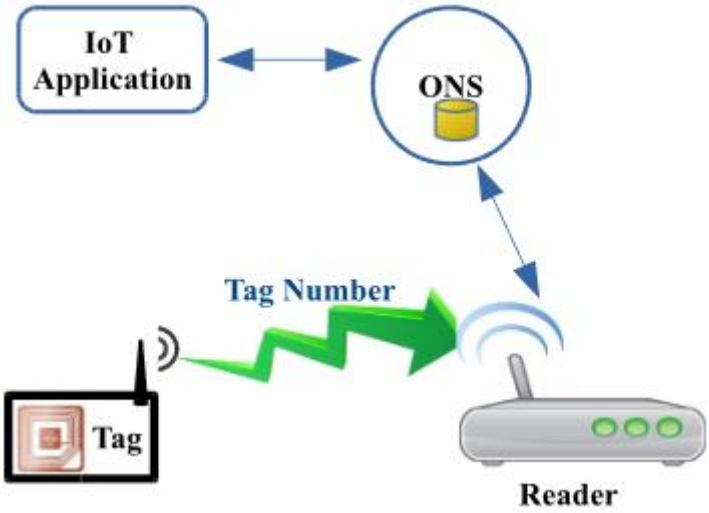
Τα RFID tags είναι ηλεκτρονικά tags που διαθέτουν κεραία και ένα μοναδικό αναγνωριστικό τα οποία αποτελούν βασικά στοιχεία στον τομέα της αναγνώρισης μέσω ραδιοσυχνοτήτων. Αυτό το μοναδικό αναγνωριστικό είναι ο ηλεκτρονικός κωδικός προϊόντος (Electronic Product Code, EPC), ο οποίος ενισχύει την ακρίβεια και την αποτελεσματικότητα της τεχνολογίας RFID. Ο EPC βρίσκεται μέσα στο RFID tag και χρησιμοποιείται κυρίως για την διαχείριση της εφοδιαστικής αλυσίδας [19]. Σε ένα σύστημα RFID, τα tags είναι απαραίτητα για την αναγνώριση, τον εντοπισμό και την επικοινωνία των αντικειμένων. Τα tags χωρίζονται σε τρεις κατηγορίες [5], [6], [48], [49]:

1. **Παθητικά Tags:** Λαμβάνουν την ενέργεια τους από τα ραδιοκύματα που εκπέμπουν οι RFID readers όταν επικοινωνούν. Αυτά τα tags μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς επειδή είναι οικονομικά και ενεργειακά αποδοτικά, ιδίως σε περιπτώσεις όπου οι συνεχείς πηγές ενέργειας μπορεί να μην είναι εφικτές.
2. **Ημι-παθητικά Tags:** Βασίζονται σε RFID readers για την επικοινωνία, ενώ χρησιμοποιούν μια ενσωματωμένη μπαταρία για την τροφοδοσία τους.
3. **Ενεργά Tags:** Είναι σε θέση να στέλνουν σήματα χωρίς την τροφοδοσία του reader, επειδή διαθέτουν ανεξάρτητη πηγή ενέργειας, συνήθως μπαταρία. Τα ενεργά tags, είναι χρήσιμα για δυναμικές και κινητές εφαρμογές λόγω της αυτονομίας τους, η οποία επιτρέπει μεγαλύτερες εμβέλειες επικοινωνίας.

Οι RFID readers, λειτουργούν ως σύνδεσμος μεταξύ του πραγματικού και του ψηφιακού κόσμου, διαβάζοντας τα RFID tags και αντλώντας σημαντικά δεδομένα από αυτά. Αφού συλλεχθούν, τα δεδομένα αυτά εισέρχονται στην βάση δεδομένων, έναν κεντρικό τόπο αποθήκευσης που είναι απαραίτητος για την διαχείριση και την καταγραφή του τεράστιου όγκου δεδομένων που παράγεται [6].

Το RFID βασίζεται σε σήματα ραδιοσυχνοτήτων, τα οποία χρησιμοποιούν μια ποικιλία συχνοτήτων για να διευκολύνουν την επικοινωνία μεταξύ των RFID tags και readers. Αυτό υπογραμμίζει την σημασία της διάκρισης των διαφόρων εμπλεκόμενων συχνοτήτων, επιτρέποντας την λήψη τεκμηριωμένων αποφάσεων για την επιλογή της καλύτερης συχνότητας για μία συγκεκριμένη εφαρμογή. Οι ερευνητές στο [48], κατηγοριοποιούν τις ραδιοσυχνότητες ως εξής:

1. **RFID χαμηλής συχνότητας (Low Frequency RFID, LF RFID):** Χρησιμοποιεί το εύρος συχνοτήτων 125 kHz και 134.2 kHz. Το LF RFID είναι γνωστό για τις μικρές αποστάσεις ανάγνωσης μερικών εκατοστών. Αυτή η συχνότητα χρησιμοποιείται ευρέως σε εφαρμογές όπως η ταυτοποίηση και η παρακολούθηση ζώων.
2. **RFID υψηλής συχνότητας (High Frequency RFID, HF RFID):** Λειτουργεί σε συχνότητες περίπου 13.56 MHz. Λόγω της μέτριας εμβέλειας ανάγνωσης (≈50 εκατοστά), το HF RFID μπορεί να χρησιμοποιηθεί σε διάφορες εφαρμογές όπως η διαχείριση της εφοδιαστικής αλυσίδας, τα συστήματα ελέγχου πρόσβασης και τα ανέπαφα συστήματα πληρωμών.
3. **RFID υπερυψηλής συχνότητας (Ultra High Frequency RFID, UHF RFID):** Συχνότητες από 300 MHz έως 3 GHz μπορούν να χρησιμοποιηθούν, αλλά κυρίαρχες ζώνες είναι οι 860–956 MHz. Επειδή το UHF RFID έχει μεγαλύτερη εμβέλεια ανάγνωσης (≈6 μέτρα), είναι ιδανικό για εφαρμογές λιανικής πώλησης και βιομηχανίας.




Σχήμα 3.7: *Σύστημα RFID* [19]

- **Παγκόσμιο σύστημα εντοπισμού θέσης (Global Positioning System, GPS):** Στην κορυφή για τον εντοπισμό θέσης βρίσκεται η τεχνολογία GPS, ένα σύστημα ραδιοπλοήγησης που βασίζεται σε γεωστατικούς δορυφόρους. Ο κύριος σκοπός του είναι να παρέχει στους χρήστες ακριβείς πληροφορίες σχετικά με την θέση, την ταχύτητα και τον χρόνο τους. Ο δέκτης GPS είναι το κεντρικό στοιχείο της λειτουργίας του GPS. Αυτό το κρίσιμο στοιχείο λαμβάνει σήματα από τους δορυφόρους και μετρά με ακρίβεια κάθε επιμέρους χρονική καθυστέρηση. Ο δέκτης GPS προσδιορίζει την ακριβή θέση του χρήστη στην επιφάνεια της Γης χρησιμοποιώντας αυτές τις χρονικές καθυστερήσεις σε συνδυασμό με τα καθιερωμένα χαρακτηριστικά διάδοσης των ραδιοκυμάτων για τον προσδιορισμό των αποστάσεων από κάθε γεωστατικό δορυφόρο [50].

### 3.4.2 Επίπεδο Δικτύου

Η έρευνα στρέφει την προσοχή της στο επίπεδο δικτύου μετά την εξέταση των θεμελιωδών τεχνολογιών του επιπέδου αντίληψης. Το επίπεδο αυτό αποτελεί την υποδομή που επιτρέπει την εφαρμογή των συσκευών IoT σε πραγματικά σενάρια και είναι απαραίτητο για την επικοινωνία μεταξύ των συσκευών και την ανταλλαγή δεδομένων. Παρακάτω περιγράφονται οι τεχνολογίες του επίπεδου δικτύου με βάση την εμβέλεια τους.

- **Bluetooth (BL):** Το BL βασίζεται στο IEEE 802.15.1 και κυκλοφόρησε στην αρχή ως πρότυπο ασύρματη επικοινωνία μικρής εμβέλειας. Έκτοτε, αναπτύχθηκε με κάθε νέα έκδοση για να ικανοποιήσει τις αυξανόμενες ανάγκες για συνδεσιμότητα σε μία ποικιλία εφαρμογών, από προσωπικές συσκευές μέχρι εμπορικές υλοποιήσεις του IoT [50].

  Με την εισαγωγή της λειτουργίας της υψηλής ταχύτητας (High-Speed, HS), το BL 3.0 αύξησε σημαντικά τους ρυθμούς μεταφοράς δεδομένων. Αυτή η έκδοση κατέστησε δυνατή την ταχύτερη ανταλλαγή δεδομένων έως και 24 Mbps. Με εμβέλεια έως και 10 μέτρα, το BL 3.0 λειτουργούσε στην ζώνη συχνοτήτων 2.4 GHz [50], [51].

  Το πρότυπο Bluetooth Low Energy (BLE), που εισήχθη με το Bluetooth 4.0, άλλαξε εντελώς το τοπίο των ασύρματων επικοινωνιών. Σχεδιασμένο για εφαρμογές IoT χαμηλής κατανάλωσης ενέργειας, το BLE παρείχε αξιοσημείωτα πλεονεκτήματα όπως χαμηλότερη κατανάλωση ενέργειας και μεγαλύτερη διάρκεια ζωής της μπαταρίας. Οι συσκευές όπως τα ασύρματα ακουστικά, τα έξυπνα ρολόγια και οι έξυπνοι αισθητήρες έγιναν εφικτά χάρη στο

BLE 4.0, το οποίο έχει κάλυψη εμβέλειας έως 100 μέτρων και ενεργειακά αποδοτική βελτιστοποίηση της ισχύος μετάδοσης [19], [52].

Με την κυκλοφορία του BL 5.0, υπήρξε μία σημαντική εξέλιξη στον τομέα, παρέχοντας αξιοσημείωτες αυξήσεις στην χωρητικότητα μετάδοσης, στους ρυθμούς μεταφοράς δεδομένων και στην εμβέλεια. Το BL 5.0 άνοιξε νέες δυνατότητες για την ανάπτυξη του IoT σε ευρύτερες περιοχές με την βελτιωμένη εμβέλεια κάλυψης έως και 200 μέτρα. Επιπλέον, διπλασίασε τους ρυθμούς μεταφοράς δεδομένων σε σχέση με τις προηγούμενες εκδόσεις του BLE, με δυνατότητα έως και 2 Mbps [50], [51].

- **Επικοινωνία κοντινού πεδίου (Near Field Communication, NFC):** Το NFC είναι τεχνολογία ασύρματης επικοινωνίας μικρής εμβέλειας και επιτρέπει την ανταλλαγή δεδομένων μεταξύ συσκευών που πλησιάζονται μεταξύ τους σε απόσταση λίγων εκατοστών (≈4 εκατοστά) [49]. Χρησιμοποιώντας την περιοχή συχνοτήτων 13.56 MHz, το NFC παράγει ραδιοκύματα, η οποία διευκολύνει την επικοινωνία. Με ρυθμούς μεταφοράς δεδομένων που κυμαίνονται από 106 kbps έως 848 kbps, το NFC παρέχει ευκολία χρήσης και απλότητα στην ανταλλαγή δεδομένων παρά την περιορισμένη εμβέλεια του. Επιπλέον, είναι κατάλληλο για συσκευές που λειτουργούν με μπαταρία λόγω του σχεδιασμού λειτουργίας χαμηλής κατανάλωσης ενέργειας [37], [50].
- **ZigBee:** Το ZigBee είναι μια δημοφιλής τεχνολογία ασύρματης επικοινωνίας για εφαρμογές χαμηλής ισχύος και χαμηλού ρυθμού δεδομένων, όπως ο βιομηχανικός έλεγχος, τα WSN και ο οικιακός αυτοματισμός. Βασίζεται στο πρότυπο IEEE 802.15.4 και ξεχωρίζει για την μεγάλη διάρκεια ζωής της μπαταρίας και την χαμηλή κατανάλωση ενέργειας. Ανάλογα με το περιβάλλον, οι συσκευές ZigBee μπορούν να μεταδίδουν δεδομένα σε απόσταση 10-100 μέτρων. Χρησιμοποιεί τρεις διαφορετικές ζώνες συχνοτήτων για την λειτουργία του ανά γεωγραφική περιοχή [14], [31]:
    1. **Παγκοσμίως:** Ζώνη 2.4 GHz με ρυθμούς δεδομένων 250 kbps
    2. **Αμερική:** Ζώνη 915 GHz με ρυθμούς δεδομένων 40 kbps
    3. **Ευρώπη:** Ζώνη 868 GHz με ρυθμούς δεδομένων 20 kbps
- **IPv6 over Low-Power WPAN (6LoWPAN):** Το 6LoWPAN είναι ένα πρωτόκολλο επικοινωνίας που ακολουθεί το πρότυπο IEEE 802.15.4 και καθιστά δυνατή την αποστολή πακέτων IPv6 σε ασύρματα δίκτυα με χαμηλή ισχύ και χαμηλό εύρος ζώνης. Αναπτύχθηκε για να καλύψει την ανάγκη δημιουργίας συνδέσεων για συσκευές με χαμηλή ισχύ και περιορισμένους πόρους, ιδίως σε εφαρμογές IoT, όπου τα παραδοσιακά πρωτόκολλα δικτύωσης IP (Internet Protocol) απαιτούν περισσότερους πόρους [38], [49]. Οι συσκευές 6LoWPAN έχουν εμβέλεια μετάδοσης 100 μέτρα, λειτουργούν κυρίως στην ζώνη ISM (Industrial, Scientific, and Medical) των 2.4 GHz και έχουν εύρος ρυθμών δεδομένων στα 250 kbps. Η χαμηλή κατανάλωση ενέργειας του 6LoWPAN είναι ένα από τα κύρια χαρακτηριστικά του, το οποίο είναι κρίσιμο για την παράταση της διάρκειας ζωής της μπαταρίας των συσκευών IoT [51].

Το πρωτόκολλο δρομολόγησης για δίκτυα χαμηλής ισχύος και απωλειών (Routing Protocol for Low-Power and Lossy Networks, RPL) είναι ένα ευρέως χρησιμοποιούμενο πρωτόκολλο στο 6LoWPAN που χρησιμοποιείται για την δημιουργία και την διατήρηση των μονοπατιών δρομολόγησης μεταξύ των συσκευών. Οι προσανατολισμένοι κατευθυνόμενοι άκυκλοι γράφοι (Destination Oriented Directed Acyclic Graph, DODAG) δημιουργούνται από το RPL για να αναπαραστήσουν την τοπολογία του δικτύου και για να επιτρέψουν την

αποτελεσματική δρομολόγηση των πακέτων. Στα ασύρματα δίκτυα χαμηλής ισχύος, ο κύριος σκοπός του RPL και του DODAG είναι να καταστεί δυνατή η αξιόπιστη και ενεργειακά αποδοτική δρομολόγηση, επιτρέποντας στις συσκευές να επικοινωνούν αποτελεσματικά, ενώ καταναλώνουν λιγότερη ενέργεια και πόρους [6], [19].

- **Z-Wave:** Το Z-Wave είναι μία ευρέως χρησιμοποιούμενη τεχνολογία ασύρματης επικοινωνίας στο IoT που αναπτύχθηκε από τη ZenSys. Λειτουργεί σε πολλαπλές συχνότητες ανάλογα με την γεωγραφική περιοχή, συνήθως γύρω στα 900 MHz. Οι εμβέλειες μετάδοσης του Z-Wave μπορούν να φτάσουν τα 30 μέτρα σε εσωτερικούς χώρους και έως και τα 100 μέτρα σε εξωτερικούς χώρους, ανάλογα με το περιβάλλον. Όσον αφορά τον ρυθμό δεδομένων, λειτουργεί μεταξύ 9.6 kbps και 100 kbps, θέτοντας την αξιοπιστία και την οικονομία ενέργειας πάνω από την μετάδοση δεδομένων υψηλής ταχύτητας. Λόγω της φήμης του για την αξιοπιστία, την προσιτή τιμή και την χαμηλή κατανάλωση ενέργειας, το Z-Wave είναι μια δημοφιλής επιλογή για λύσεις IoT, ειδικά στον οικιακό αυτοματισμό [14], [31].
- **Wi-Fi:** Το Wi-Fi είναι μία ασύρματη τεχνολογία, το οποίο έχει τις ρίζες του στα πρότυπα IEEE 802.11 και επιτρέπει στις συσκευές να επικοινωνούν ασύρματα, απελευθερώνοντας τες από τους περιορισμούς των φυσικών συνδέσεων [53]. Ανάλογα με το χρησιμοποιούμενο πρότυπο IEEE 802.11, μπορεί να υποστηρίξει ένα ευρύ φάσμα ρυθμών μεταφοράς δεδομένων, που κυμαίνονται από 11 Mbps έως 40 Gbps. Μπορεί να καλύψει ένα ευρύ φάσμα απαιτήσεων επικοινωνίας, συμπεριλαμβανομένων εφαρμογών που απαιτούν μεγάλο εύρος ζώνης εκτός από την κανονική περιήγηση στο διαδίκτυο. Το Wi-Fi προσφέρει ευελιξία διπλής ζώνης που λειτουργεί στις ζώνες συχνοτήτων 2.4 GHz και 5 GHz, η οποία βελτιστοποιεί την επιλογή καναλιών, μειώνει τις παρεμβολές και βελτιώνει την συνολική απόδοση. Η ανάπτυξη του Wi-Fi 5 (802.11ac), το οποίο έχει ρυθμό δεδομένων έως και 6.39 Gbps, στο Wi-Fi 6 (802.11ax), το οποίο έχει ρυθμό δεδομένων έως και 9.6 Gbps, και η επερχόμενη αναβάθμιση στο Wi-Fi 7 (802.11be), το οποίο προβλέπεται να αυξήσει ακόμη περισσότερο τον ρυθμό δεδομένων σε 40 Gbps, καταδεικνύει την αφοσίωση για την βελτίωση των δυνατοτήτων που απαιτούνται για την κάλυψη των αυξανόμενων αναγκών των εφαρμογών IoT [50], [51]. Εκτός από την ανάδειξη της αυξημένης αποδοτικότητας και αξιοπιστίας της συνδεσιμότητας, η εξέλιξη αυτή δείχνει μια αξιοσημείωτη αύξηση των ρυθμών μετάδοσης των δεδομένων, υποδεικνύοντας ότι υπάρχει η απαραίτητη υποδομή για την διαχείριση των τεράστιων ποσοτήτων δεδομένων που παράγονται από τις συσκευές IoT και επιτρέποντας ομαλότερες, ταχύτερες και πιο αξιόπιστες επικοινωνίες.

  Ένα ενδιάμεσο σημείο πρόσβασης, δεν είναι απαραίτητο για την επικοινωνία P2P χάρη στο Wi-Fi Direct, ένα χαρακτηριστικό της τεχνολογίας Wi-Fi. Το Wi-Fi Direct είναι ένα εργαλείο για την άμεση επικοινωνία μεταξύ των συσκευών στο IoT όταν δεν υπάρχει παραδοσιακή υποδομή δικτύου [50].

  Ενσωματωμένο στο πρότυπο 802.11ah, το Wi-Fi HaLow είναι μια εξειδικευμένη ασύρματη λύση που έχει σχεδιαστεί για να ικανοποιεί τις μοναδικές ανάγκες του IoT. Είναι μία τεχνολογία ζώνης συχνοτήτων κάτω του 1 GHz, η οποία είναι μοναδική στο ότι έχει καλύτερη διείσδυση μέσα από εμπόδια και μεγαλύτερη εμβέλεια, γεγονός που την καθιστά ιδανική για ένα ευρύ φάσμα εφαρμογών του IoT. Επίσης το Wi-Fi HaLow δίνει έμφαση στην χαμηλή κατανάλωση ενέργειας, χαρακτηριστικό κρίσιμο για τις εφαρμογές των WSNs [38].

Πίνακας 3.1: Περίληψη των διαφόρων χαρακτηριστικών της οικογένειας 802.11 [51].

| Amendment | Naming Convention | Year | Operating Band | Max Bandwidth | Max Data Rate | PHY | MAC |
|---|---|---|---|---|---|---|---|
| 802.11b | Wi-Fi 1 | 1999 | 5 GHz | 22 MHz | 11 Mbps | DSSS | DCF [1] |
| 802.11a | Wi-Fi 2 | 1999 | 2.4 GHz | 20 MHz | 54 Mbps | OFDM | DCF |
| 802.11g | Wi-Fi 3 | 2003 | 2.4 GHz | 20 MHz | 54 Mbps | MIMO-OFDM | DCF |
| 802.11n | Wi-Fi 4 | 2008 | 2.4/5 GHz | 40 MHz | 600 Mbps | OFDM | DCF + EDCA [2], frame aggregation, BA [3] |
| 802.11ac | Wi-Fi 5 | 2014 | 5 GHz | 40 MHz | 6.39 Gbps | 256-QAM, OFDM, DL MIMO, channel bounding | DCF + EDCA, frame aggregation, BA |
| 802.11ah | Wi-Fi HaLow | 2017 | sub-1 GHz | 16 MHz | 347 Mbps | OFDM, DL-MU MIMO | EDCA, TWT, RAW [4] |
| 802.11ax | Wi-Fi 6 | 2019 2020 (6E) | 2.4/5 GHz, 6 GHz for Wi-Fi 6E | 160 MHz | 9.6 Gbps | OFDMA, UL/DL MIMO, channel bounding | DCF + EDCA, frame aggregation, BA, TWT [5], MU channel access |
| 802.11be | Wi-Fi 7 | 2024 | 2.4/5/6 GHz | 320 MHz | 40 Gbps | 4096-QAM, Coordinated OFDMA, UL/DL MIMO | HARQ [6] multi-link aggregation, Multi link operation, ... |

Τελευταίο και αξιοσημείωτο IEEE πρότυπο για το IoT, είναι το 802.11p. Ο σκοπός του 802.11p είναι να καλύψει τις μοναδικές ανάγκες επικοινωνίας οχημάτων στα Ευφυή Συστήματα Μεταφορών (Intelligent Transportation System, ITS). Το 802.11p δημιουργεί ένα εξειδικευμένο και αποτελεσματικό δίκτυο, επιτρέποντας την άμεση επικοινωνία μεταξύ οχημάτων (Vehicle-to-Vehicle, V2V) και μεταξύ οχημάτων και οδικών υποδομών (Vehicle-to-Infrastructure, V2I) στην ζώνη συχνοτήτων 5.9 GHz [53].

- **WiMAX:** Το πρότυπο IEEE 802.16 αποτελεί τη βάση για την τεχνολογία ασύρματων επικοινωνιών που είναι γνωστή ως WiMAX, ή Παγκόσμια Διαλειτουργικότητα για Μικροκυματική Πρόσβαση. Αυτή η τεχνολογία, η οποία παρέχει ευρυζωνική συνδεσιμότητα υψηλής ταχύτητας μέσω ασύρματων δικτύων, αναφέρεται συχνά ως 4G. Με μέγιστες ταχύτητες εκατοντάδων megabits ανά δευτερόλεπτο, το WiMAX μπορεί να προσφέρει υψηλές ταχύτητες όσον αφορά τον ρυθμό δεδομένων. Ωστόσο, ανάλογα με το σενάριο υλοποίησης, οι πραγματικοί ρυθμοί δεδομένων ενδέχεται να διαφέρουν [14], [54].
- **NarrowBand IoT (NB-IoT):** Το NB-IoT είναι μια τεχνολογία για LPWAN που έχει τυποποιηθεί από το 3GPP. Σκοπός του είναι να διευκολύνει την αποτελεσματική επικοινωνία μεταξύ των κυψελοειδών δικτύων, προσφέροντας καλύτερη διείσδυση σε εσωτερικούς χώρους, αυξημένη κάλυψη και χαμηλότερη κατανάλωσης ενέργειας. Χρησιμοποιεί κανάλια στενής ζώνης, με εύρος ζώνης 180 kHz, καθιστώντας δυνατή την επικοινωνία σε μεγάλες αποστάσεις. Όσον αφορά του ρυθμούς δεδομένων, μπορεί να προσφέρει 230 kbps downlink και 250 kbps uplink [14]. Το NB-IoT παρέχει διαφορετικούς τρόπου λειτουργίας για διαφορετικά σενάρια υλοποίησης. Κατά την χρήση της λειτουργίας της στενής ζώνης, το NB-IoT λειτουργεί εντός του φάσματος που έχει διατεθεί για εφαρμογές IoT. Η λειτουργία Guardband μεγιστοποιεί την χρήση του φάσματος, κάνοντας χρήση των μη χρησιμοποιούμενων ζωνών συχνοτήτων μεταξύ

των φορέων Long-term Evolution (LTE). Η ρύθμιση Standalone λειτουργεί χωρίς να εξαρτάται από την τρέχουσα κυψελοειδή υποδομή [22], [51].

- **SigFox:** Το SigFox είναι μία λύση για δίκτυα LPWAN με γαλλικές ρίζες. Λειτουργεί με εύρος ζώνης καναλιού 100 MHz, ενώ λειτουργεί στις μη αδειοδοτημένες ζώνης φάσματος, οι οποίες συνήθως κυμαίνονται μεταξύ 915 MHz και 928 MHz. Αυτή η τεχνολογία είναι ιδανική για εφαρμογές IoT, επειδή παρέχει δίκτυο υψηλής χωρητικότητας με ελάχιστη κατανάλωση ενέργειας. Επίσης ξεχωρίζει προσφέροντας μία λύση επικοινωνίας βασισμένη σε λογισμικό που μειώνει αποτελεσματικά το συνολικό κόστος των συνδεδεμένων συσκευών και την κατανάλωση ενέργειας [22].
- **LoRa - LoRaWAN:** Το LoRa, είναι μία τεχνολογία που χρησιμοποιείται στο IoT για εφαρμογές χαμηλής ισχύος και μεγάλης εμβέλειας. Ανάλογα με παράγοντες όπως η τοποθέτηση της κεραίας και οι περιβαλλοντικές συνθήκες, η τεχνολογία LoRa μπορεί να επιτύχει εμβέλειες από 3 έως 15 χιλιόμετρα σε αστικές και αγροτικές περιοχές αντίστοιχα. Λειτουργεί σε μη αδειοδοτημένες ζώνες συχνοτήτων 433 MHz, 868 MHz και 915 MHz. Το LoRaWAN είναι πρωτόκολλο που βασίζεται στην τεχνολογία LoRa. Η έμφαση που δίνει το LoRaWAN στους χαμηλούς ρυθμούς δεδομένων το καθιστά ιδανικό για την αποστολή μικρών φορτίων σε μεγάλες αποστάσεις, όπως τα δεδομένα αισθητήρων [50], [51].

### 3.4.3 Επίπεδο Εφαρμογής

Έχοντας αποκτήσει μια ολοκληρωμένη κατανόηση του ρόλου του επιπέδου εφαρμογής στα συστήματα IoT, η προσοχή στρέφεται τώρα στα συγκεκριμένα πρωτόκολλα εφαρμογής που λειτουργούν σε αυτό το επίπεδο. Με την υποστήριξη των τεχνολογιών που αναφέρονται παρακάτω, κάθε πρωτόκολλο συμβάλλει ξεχωριστά στην ικανότητα του IoT να επεξεργάζεται, να αξιολογεί και να αντιδρά στα δεδομένα που συλλέγονται.

- **Constrained Application Protocol (CoAP):** Το CoAP είναι ένα ειδικό πρωτόκολλο μεταφοράς ιστοσελίδων που προορίζεται για εφαρμογές IoT. Σκοπός του είναι να καταστήσει δυνατή την εύκολη και ελαφριά επικοινωνία συσκευών χαμηλής ισχύος, με άλλες δικτυακές οντότητες. Επειδή το CoAP χρησιμοποιεί User Datagram Protocol (UDP), είναι ιδανικό για συσκευές χαμηλής κατανάλωσης ενέργειας [31].
- **Message Queuing Telemetry Transport (MQTT):** Ένα ελαφρύ πρωτόκολλο ανταλλαγής μηνυμάτων που ονομάζεται MQTT, δημιουργήθηκε για να διευκολύνει την αποτελεσματική επικοινωνία μεταξύ των συσκευών IoT και σε εφαρμογές μηχάνημα-προς-μηχάνημα (Machine-to-Machine, M2M). Το MQTT είναι κατάλληλο για εφαρμογές IoT με περιορισμένους πόρους και σποραδική συνδεσιμότητα, επειδή είναι βελτιστοποιημένο για δίκτυα χαμηλού εύρους ζώνης, υψηλής καθυστέρησης και ασταθή δίκτυα. Σε εφαρμογές όπως έξυπνα σπίτια, βιομηχανικός αυτοματισμός και έξυπνες πόλεις, χρησιμοποιείται για την μετάδοση των δεδομένων από αισθητήρες, ο έλεγχος των συσκευών και η παρακολούθηση σε πραγματικό χρόνο [55].
- **Advanced Message Queuing Protocol (AMQP):** Το AMQP είναι ένα ανοιχτό πρότυπο πρωτόκολλο ανταλλαγής μηνυμάτων και δημιουργήθηκε για να διευκολύνει την αξιόπιστη και διαλειτουργική επικοινωνία μεταξύ των εφαρμογών. Χρησιμοποιείται σε διάφορα σενάρια ανταλλαγής μηνυμάτων, όπως η ροή δεδομένων σε πραγματικό χρόνο και ο διαμοιρασμός των εργασιών [55].
- **Extensible Messaging and Presence Protocol (XMPP):** Το XMPP, το οποίο δημιουργήθηκε αρχικά για την άμεση ανταλλαγή μηνυμάτων, είναι ένα ανοιχτό πρωτόκολλο επικοινωνίας που

στην συνέχεια αναπτύχθηκε ώστε να υποστηρίζει ένα ευρύ φάσμα εφαρμογών επικοινωνίας σε πραγματικό χρόνο. Λόγω του επεκτάσιμου σχεδιασμού του, μπορεί να προσαρμοστεί και να επεκταθεί ώστε να καλύπτει συγκεκριμένες ανάγκες επικοινωνίας, γεγονός που το καθιστά μία ευέλικτη επιλογή για την ανάπτυξη λύσεων επικοινωνίας σε πραγματικό χρόνο σε εφαρμογές IoT [51], [55].

- **Distribution Service (DDS):** Το τυποποιημένο πρωτόκολλο επικοινωνίας DDS, δημιουργήθηκε για την διανομή των δεδομένων σε κατανεμημένα συστήματα σε πραγματικό χρόνο. Χρησιμοποιείται συχνά σε ευαίσθητες στον χρόνο και κρίσιμες για την αποστολή εφαρμογές, όπως αυτόνομα συστήματα, βιομηχανικός αυτοματισμός και υγειονομική περίθαλψη [55].

## 3.5 Εφαρμογές IoT

Το IoT έχει σημαντικό και εκτεταμένο αντίκτυπο σε διάφορους κλάδους, όπως η υγειονομική περίθαλψη όπου μετασχηματίζει την φροντίδα και την παρακολούθηση των ασθενών και η γεωργία όπου μεγιστοποιεί την χρήση των πόρων και ενισχύει την παραγωγικότητα. Βελτιώνει τις εμπειρίες των πελατών και επιταχύνει τις λειτουργίες στο λιανικό εμπόριο και βοηθά την ενεργειακή βιομηχανία να κάνει την μετάβαση σε πιο έξυπνα, πιο βιώσιμα και αξιόπιστα δίκτυα. Οι εφαρμογές IoT μετατρέπουν τα σπίτια και τις πόλεις σε δικτυωμένα έξυπνα περιβάλλοντα που κάνουν την ζωή ευκολότερη, ασφαλέστερη και πιο ενεργειακά αποδοτική.

### 3.5.1 Έξυπνη Υγειονομική Περίθαλψη

Η τεχνολογία του IoT μεταμορφώνει τον τομέα της υγειονομικής περίθαλψης παρέχοντας πρωτοποριακούς τρόπου για την ενίσχυση των ιατρικών αποτελεσμάτων, την επιτάχυνση των διαδικασιών και την βελτίωση της φροντίδας των ασθενών. Το ιατρικό προσωπικό μπορεί να χρησιμοποιεί συσκευές και συστήματα IoT, όπως φορητές συσκευές παρακολούθησης και έξυπνα ιατρικά εμφυτεύματα, για την συλλογή δεδομένων σε πραγματικό χρόνο, την αυτοματοποίηση καθημερινών εργασιών και την δυνατότητα απομακρυσμένης παρακολούθησης των ασθενών. Αυτή η αλλαγή δημιουργεί ένα πιο εξατομικευμένο και αποτελεσματικό περιβάλλον παροχής υγειονομικής περίθαλψης, με δυνατότητες προληπτικής διαχείρισης της υγείας και έγκαιρης ανίχνευσης σε περίπτωση προβλήματος [6].

Ωστόσο, αυτή η τεχνολογική ενσωμάτωση αναδεικνύει επείγοντα ζητήματα ασφαλείας που απαιτούν αυστηρά πρωτόκολλα ασφαλείας για την διατήρηση του απορρήτου των ασθενών και την εγγύηση της ακεραιότητας των ιατρικών συσκευών. Ένας επιτιθέμενος που αποκτά πρόσβαση σε ένα ρομποτικό χειρουργικό σύστημα είναι ένα παράδειγμα ενός πιθανού σεναρίου απειλής που αναδεικνύει τις συνέπειες της αγνόησης των μέτρων ασφαλείας. Υπό αυτές τις συνθήκες, ο επιτιθέμενος μπορεί να αποκτήσει τον έλεγχο και να χρησιμοποιήσει το σύστημα για να προκαλέσει βλάβη ή ακόμη και να θέσει σε κίνδυνο την ζωή των ασθενών. Αντιστοίχως, οι επιτιθέμενοι μπορεί να είναι σε θέση να εισχωρήσουν πλαστές πληροφορίες για την υγεία μέσω μη εξουσιοδοτημένης πρόσβαση σε φορητές οθόνες υγείας, γεγονός που θα μπορούσε να οδηγήσει σε εσφαλμένες διαγνώσεις. Αυτές οι περιπτώσεις υπογραμμίζουν πόσο κρίσιμο είναι να ενσωματωθούν αυστηρά μέτρα ασφαλείας στο περιβάλλον της υγειονομικής περίθαλψης του IoT, προκειμένου να μειωθεί ο κίνδυνος παραβίασης των δεδομένων, οι οποίες μπορεί να έχουν καταστροφικές συνέπειες για την ιδιωτικότητα και την ευημερία των ασθενών.

### 3.5.2 Έξυπνη Γεωργία και Κτηνοτροφία

Στον τομέα της γεωργίας και της κτηνοτροφίας, το IoT φέρνει επανάσταση στις παραδοσιακές πρακτικές, προσφέροντας προηγμένες λύσεις για την γεωργία ακριβείας, την διαχείριση των ζώων και την περιβαλλοντική παρακολούθηση. Μέσω της ενσωμάτωσης των συσκευών IoT, αισθητήρων και της ανάλυσης δεδομένων, οι αγρότες μπορούν να βελτιστοποιήσουν την άρδευση, να αποτρέψουν μυκητιασικές λοιμώξεις και να λάβουν αποφάσεις με βάση τα δεδομένα που συλλέγονται για τις καιρικές συνθήκες σε πραγματικό χρόνο. Για την κτηνοτροφία, το IoT επιτρέπει την παρακολούθηση της κίνησης των ζώων και τις συνθήκες υγείας τους, ενισχύοντας την παραγωγικότητα και την αποδοτικότητα [56].

Παρόλα αυτά, η χρήση του IoT στην γεωργία και την διαχείριση της κτηνοτροφίας δημιουργεί νέες προκλήσεις ασφαλείας. Για παράδειγμα, αν ο επιτιθέμενος αποκτήσει τον έλεγχο του συστήματος IoT που διαχειρίζεται την άρδευση ή τους περιβαλλοντικούς ελέγχους, μπορεί να χειραγωγήσει την παροχή του νερού ή τις περιβαλλοντικές συνθήκες, με πιθανό αποτέλεσμα την αποτυχία των καλλιεργειών. Ομοίως, η μη εξουσιοδοτημένη πρόσβαση σε συστήματα παρακολούθησης των ζώων μπορεί να οδηγήσει σε αλλοίωση των δεδομένων υγείας, προκαλώντας κακή διαχείριση των προγραμμάτων σίτισης και εμβολιασμού.

### 3.5.3 Έξυπνο Λιανικό Εμπόριο

Ο συνδυασμός ψηφιακών καινοτομιών και φυσικών καταστημάτων μεταμορφώνει τον κλάδο του λιανικού εμπορίου. Η αγοραστική εμπειρία αναδιαμορφώνεται από αυτή την αλλαγή, καθιστώντας την πιο διαδραστική και εξατομικευμένη. Φανταστείτε ράφια εξοπλισμένα με αισθητήρες που μπορούν να ελέγχουν αυτόματα τα επίπεδα των αποθεμάτων. Επίσης θα αποτελούνται από έξυπνες οθόνες που μπορούν να προτείνουν συμπληρωματικά προϊόντα με βάση αυτά που αγόρασαν οι πελάτες στο παρελθόν [40].

Υπάρχουν όμως σημαντικά κενά ασφαλείας που εισάγονται από αυτή την μετάβαση προς το έξυπνο λιανικό εμπόριο. Σε περίπτωση που ο επιτιθέμενος καταφέρει να παραβιάσει τους αισθητήρες ή τις έξυπνες οθόνες, θα μπορεί να προκαλέσει αλλοίωση στην απογραφή με την χειραγώγηση των δεδομένων για τον αριθμό των αποθεμάτων. Εναλλακτικά, θα μπορεί να χρησιμοποιήσει τις έξυπνες οθόνες για να προβάλει μη εξουσιοδοτημένες διαφημίσεις ή παραπλανητικές πληροφορίες, γεγονός που θα μπορούσε να βλάψει την φήμη του καταστήματος και να φθείρει την εμπιστοσύνη των πελατών. Ακόμη πιο ανησυχητικό είναι ότι, εάν δεν ακολουθηθούν τα κατάλληλα πρωτόκολλα ασφαλείας, η εκμετάλλευση αυτών των συστημάτων μπορεί να προσφέρει μία είσοδο για πιο ιδιωτικές πληροφορίες, συμπεριλαμβανομένων των στοιχείων των καρτών πληρωμής ή των προσωπικών πληροφοριών που ανήκουν στους πελάτες.

### 3.5.4 Έξυπνο Δίκτυο Ηλεκτρισμού

Η ιδέα του έξυπνου δικτύου ηλεκτρισμού είναι το αποτέλεσμα της ενσωμάτωσης της τεχνολογίας του IoT στην δομή του παραδοσιακού ηλεκτρικού δικτύου, η οποία αντιπροσωπεύει μια δραματική αλλαγή στον τρόπο διανομής και ελέγχου της ενέργειας. Οι εφαρμογές του έξυπνου δικτύου ηλεκτρικής ενέργειας, οι οποίες περιλαμβάνουν την ανάπτυξη αισθητήρων και έξυπνων συσκευών σε όλο το ηλεκτρικό δίκτυο, μεταμορφώνουν την ενεργειακή βιομηχανία. Η μετάβαση προς πιο αποτελεσματικές και αξιόπιστες τεχνικές διαχείρισης της ενέργειας καθίσταται δυνατή χάρη σε αυτές τις τεχνολογίες, οι οποίες παρέχουν ακριβέστερη παρακολούθηση και έλεγχο της διανομής της ηλεκτρικής ενέργειας. Έχοντας στην διάθεση τους δεδομένα σε πραγματικό χρόνο σχετικά με την

κατανάλωση, οι πάροχοι ενέργειας μπορούν να βελτιστοποιήσουν τις λειτουργίες του δικτύου και να εντοπίζουν τις βλάβες, βελτιώνοντας σημαντικά την αξιοπιστία των υπηρεσιών και την ικανοποίηση των πελατών [19].

Όμως, η αναβάθμιση του έξυπνου ηλεκτρικού δικτύου από τις τεχνολογίες IoT επιφέρει επίσης μια σειρά από ζητήματα ασφαλείας που πρέπει να εξεταστούν προσεκτικά. Ο επιτιθέμενος θα μπορεί να χειραγωγήσει την διανομή της ενέργειας αποκτώντας πρόσβαση στα συστήματα ελέγχου. Επίσης, μπορεί να προκαλέσει εκτεταμένες διακοπές ή ακόμη και να θέσει σε κίνδυνο την δημόσια ασφάλεια υπερφοτώνοντας τα κυκλώματα.

### 3.5.5 Έξυπνο Σπίτι

Με την έλευση του IoT, η υλοποίηση του έξυπνου σπιτιού έχει γίνει όλο και πιο δημοφιλής, παρέχοντας στους ιδιοκτήτες άνεση, ευκολία και ακόμη βελτίωση της ενεργειακής απόδοσης. Η απομακρυσμένη παρακολούθηση, ο έλεγχος και η αυτοματοποίηση πολλών λειτουργιών του σπιτιού καθίστανται δυνατές από συσκευές IoT που ενσωματώνονται σε συστήματα ψυχαγωγίας, κάμερες ασφαλείας, συστήματα φωτισμού και οικιακές συσκευές. Βοηθοί με φωνητική ενεργοποίηση, έξυπνοι θερμοστάτες που ρυθμίζουν μόνοι τους τις ρυθμίσεις της θερμοκρασίας με βάση τις προτιμήσεις του χρήστη, έξυπνες κλειδαριές και κάμερες ασφαλείας που βελτιώνουν την ασφάλεια του σπιτιού, καθώς και άλλες οικιακές συσκευές που ενισχύονται από το IoT, αλλάζουν ριζικά και επαναπροσδιορίζουν την οικιακή εμπειρία [40].

Ωστόσο, υπάρχουν μοναδικές επιπτώσεις στην ασφάλεια που συνδέονται με αυτή την επανάσταση που καθοδηγείται από το IoT. Επειδή τα έξυπνα σπίτια είναι δικτυωμένα, ο επιτιθέμενος μπορεί να εκμεταλλευτεί τις ευπάθειες και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση. Για παράδειγμα, μια έξυπνη κάμερα που έχει παραβιαστεί θα μπορούσε να χρησιμοποιηθεί για την παρακολούθηση των κατοίκων χωρίς την γνώση τους ή μια παραβιασμένη έξυπνη κλειδαριά θα μπορούσε να χρησιμοποιηθεί για την φυσικό είσοδο στο σπίτι. Επιπλέον η παραβίαση ενός βοηθού με φωνητική ενεργοποίηση μπορεί να οδηγήσει σε παράνομη συλλογή προσωπικών πληροφοριών και παραβίαση της ιδιωτικής ζωής.

### 3.5.6 Έξυπνα Οχήματα

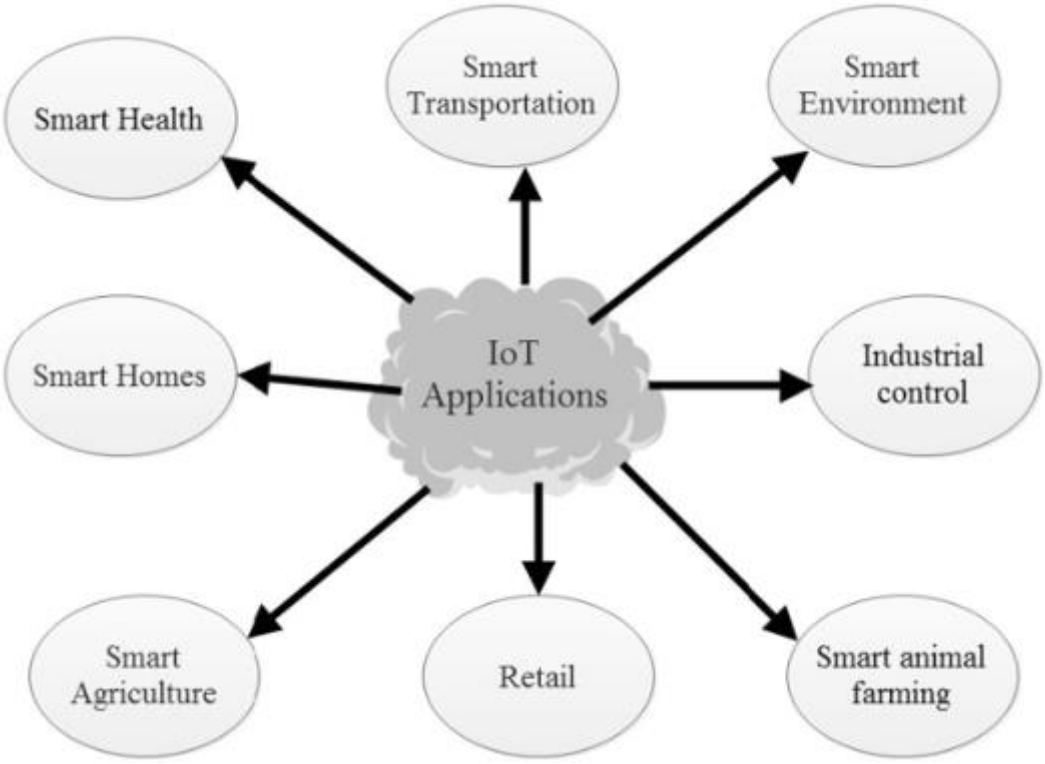
Η εποχή των έξυπνων οχημάτων έχει ξεκινήσει με την ενσωμάτωση της τεχνολογίας IoT στα συστήματα των οχημάτων, σηματοδοτώντας μια σημαντική πρόοδο στην καινοτομία της αυτοκινητοβιομηχανίας. Αυτά τα οχήματα είναι κάτι περισσότερο από απλοί τρόποι μετακίνησης. Πλέον μπορούν να χαρακτηριστούν και έξυπνες μηχανές με την δυνατότητα να συλλέγουν και να ανταλλάσσουν δεδομένα σε πραγματικό χρόνο, εφόσον είναι εξοπλισμένα με διάφορους αισθητήρες, ενεργοποιητές και συστήματα επικοινωνίας. Αυτή η ικανότητα επικοινωνίας βελτιώνει την οδική ασφάλεια και την διαχείριση της κυκλοφορίας [22]. Οι αρχιτεκτονικές ad-hoc χρησιμοποιούνται από τα έξυπνα οχήματα, όπως παρουσιάστηκε σε προηγούμενο κεφάλαιο.

Το γεγονός όμως ότι οι τεχνολογίες IoT ενσωματώνονται στα οχήματα δημιουργεί επίσης νέες προκλήσεις στην ασφάλεια. Για παράδειγμα, αν ο επιτιθέμενος καταφέρει να εισέλθει στο σύστημα επικοινωνίας ενός έξυπνου οχήματος, θα μπορούσε να το χειραγωγήσει για να μπερδέψει τους οδηγούς ή σε χειρότερη περίπτωση να πάρει εξ ολοκλήρου τον έλεγχο του οχήματος. Τέτοιες παραβιάσεις μπορεί να θέσουν σε μεγάλο κίνδυνο την ασφάλεια των άλλων οδηγών καθώς και των επιβατών στο όχημα. Επιπλέον, οι πληροφορίες που συλλέγονται από τα έξυπνα οχήματα μπορεί να υποκλαπούν, θέτοντας σε κίνδυνο την ιδιωτική ζωή των ανθρώπων, αποκαλύπτοντας την τοποθεσία τους.

### 3.5.7 Έξυπνες Μεταφορές

Με την εισαγωγή των έξυπνων οχημάτων και των έξυπνων συστημάτων διαχείρισης της κυκλοφορίας, η ενσωμάτωση του IoT στα συστήματα μεταφορών έχει την δυνατότητα να αλλάξει εντελώς τον τρόπο με τον οποίο οι άνθρωποι μετακινούνται. Αυτές οι εξελίξεις υπόσχονται μια εποχή κατά την οποία οι επιχειρήσεις και οι οργανισμοί που εμπλέκονται στις μεταφορές θα μπορούν να χρησιμοποιούν τεχνολογίες που βασίζονται σε αισθητήρες για να αυξήσουν σημαντικά την συνολική αποτελεσματικότητα των δικτύων μεταφορών. Τα συστήματα αυτά είναι σε θέση να προσαρμόζονται δυναμικά στις μεταβαλλόμενες συνθήκες μέσω της ανάλυσης των δεδομένων σε πραγματικό χρόνο από πολλαπλές πηγές, όπως οχήματα και φωτεινοί σηματοδότες. Αυτό τους επιτρέπει να ανακατευθύνουν την κυκλοφορία ανάλογα με τις ανάγκες [6].

Παρόλα αυτά, υπάρχουν ζητήματα ασφάλειας με αυτή την μετάβαση σε ένα περιβάλλον μεταφορών που ενισχύεται από το IoT. Για παράδειγμα, παραβιασμένα διασυνδεδεμένα συστήματα διαχείρισης της κυκλοφορίας θα μπορούσαν να οδηγήσουν σε χειραγώγηση των σηματοδοτών κυκλοφορίας, γεγονός που θα προκαλούσε αναστάτωση και ενδεχομένως ακόμη και ατυχήματα.




Σχήμα 3.8: *Εφαρμογές IoT* [6]

## 3.6 Επίλογος

Η διερεύνηση του IoT σε αυτό το κεφάλαιο κάλυψε ένα ευρύ φάσμα θεμάτων, συμπεριλαμβανομένων των θεμελιωδών συστατικών του, των αρχιτεκτονικών, των τεχνολογιών που το καθιστούν εφικτό και των πρακτικών εφαρμογών του. Μέσω της ανάλυσης των επιπέδων αρχιτεκτονικής και των τεχνολογιών, έχει δημιουργηθεί μία ισχυρή βάση για την κατανόηση των στοιχείων που εμπλέκονται στην δημιουργία IoT συστημάτων. Επιπλέον, η διερεύνηση των πρακτικών εφαρμογών του IoT σε διάφορους κλάδους υπογραμμίζει την επαναστατική επίδραση των συνδεδεμένων τεχνολογιών σε διάφορους τομείς της ζωής μας.

# 4. Από την Μηχανική στην Βαθιά Μάθηση

## 4.1 Εισαγωγή

Αυτό το κεφάλαιο παρέχει μια κατατοπιστική επισκόπηση των θεμελιωδών εννοιών του ML και του DL, καθώς και των υποκείμενων λειτουργιών τους. Ξεκινά με την εισαγωγή αυτών των τεχνολογιών, εξηγώντας τους ρόλους τους στην σύγχρονη ανάλυση των δεδομένων και τον τρόπο με τον οποίο επιτρέπουν στις μηχανές να μαθαίνουν από δεδομένα, να λαμβάνουν αποφάσεις και να βελτιώνουν τις επιδόσεις τους από μόνες τους. Καθώς η ανάλυση συνεχίζεται, ασχολείται με τις μεθοδολογίες που χρησιμεύουν ως βάση για την λειτουργία αυτών των συστημάτων, με έμφαση στις θεωρητικές προσεγγίσεις που επιτρέπουν στις μηχανές να βελτιώνονται.

Στην συνέχεια, το κεφάλαιο εμβαθύνει σε μία ποικιλία αλγορίθμων ML και DL. Κάθε αλγόριθμος αναλύεται για να αποκαλύψει τόσο τις θεωρητικές του δομές όσο και τις δυνατότητες του για μελλοντικές εφαρμογές, θέτοντας τις βάσεις για τα επόμενα κεφάλαια στα οποία αυτά τα εργαλεία θα χρησιμοποιηθούν για την επίλυση πραγματικών προβλημάτων.

Τέλος, το κεφάλαιο αναφέρεται στις κρίσιμες μετρικές αξιολόγησης που καθορίζουν την αποτελεσματικότητα και την ακρίβεια των μοντέλων ML και DL. Το υποκεφάλαιο υπογραμμίζει τη σημασία αυτών των μετρικών για την αξιολόγηση των πιθανών επιδόσεων των μηχανισμών στον πραγματικό κόσμο.

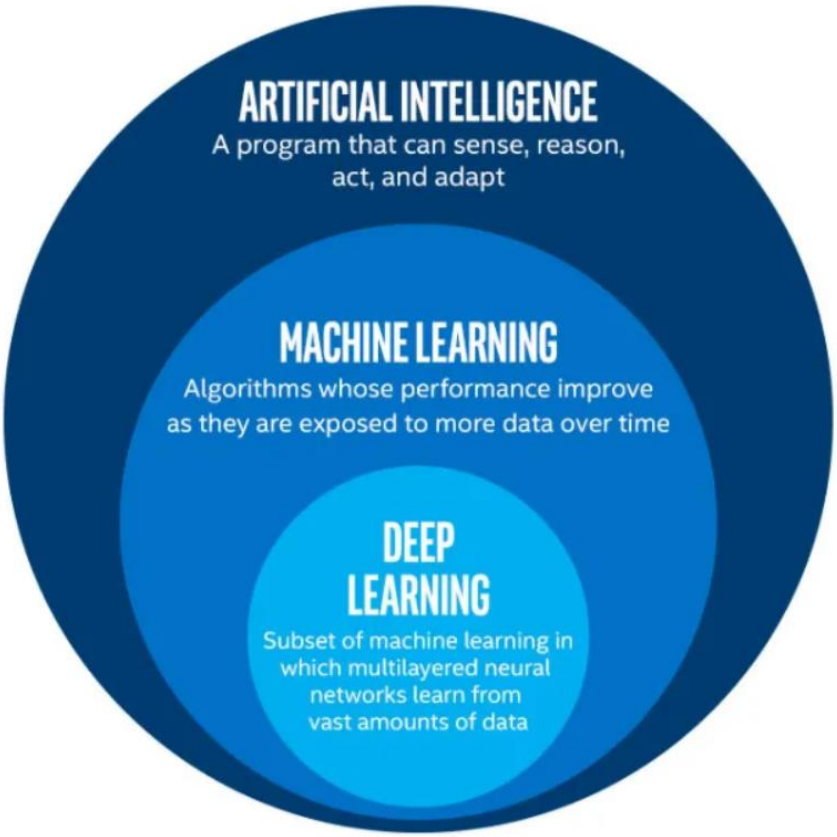
## 4.2 Βασικές Αρχές Μηχανικής Μάθησης και Βαθιάς Μάθησης

Το ML και το DL είναι δύο από τις σημαντικότερες δυνάμεις που οδηγούν την επανάσταση στο σύγχρονο τοπίο της τεχνολογικής προόδου, ειδικά όταν πρόκειται για την ασφάλεια του IoT. Αυτοί οι κλάδοι του AI αποτελούν θεμελιώδη στοιχεία που αλλάζουν τον τρόπο με τον οποίο προσεγγίζεται η κυβερνοασφάλεια με σκοπό να αισθανόμαστε ασφαλής σε αυτό τον δικτυωμένο κόσμο.

Ένα βασικό συστατικό της επιστήμης των δεδομένων και του AI, το ML δίνει στους υπολογιστές και στις μηχανές την ικανότητα να μαθαίνουν μόνοι τους από σύνολα δεδομένων (datasets) και να λαμβάνουν τεκμηριωμένες αποφάσεις με ελάχιστη έως καθόλου ανθρώπινη παρέμβαση [57]. Αυτή η ικανότητα καθίσταται ιδιαίτερα σημαντική όταν πρόκειται για την ασφάλεια του IoT, καθώς η φύση των απειλών όχι μόνο μεταβάλλεται συνεχώς αλλά είναι επίσης πολύ σύνθετη και απρόβλεπτη. Αντιμέτωπες με την επείγουσα ανάγκη για προηγμένους αμυντικούς μηχανισμούς, οι επιστημονικές και τεχνολογικές κοινότητες χρησιμοποιούν σταδιακά το ML ως λύση για την ενίσχυση της ασφάλειας. Σε αντίθεση με τα παραδοσιακά μέτρα ασφαλείας, τα οποία είναι συχνά στατικά και ακολουθούν προκαθορισμένους κανόνες, το ML παρέχει μια ευέλικτη μέθοδο που μπορεί να επεξεργάζεται μεγάλες ποσότητες δεδομένων για τον εντοπισμό και την αξιολόγηση πιθανών αδυναμιών ασφαλείας. Λόγω αυτής της προληπτικής ικανότητας, το ML είναι σε θέση να προβλέψει και να επιλύσει τις ευπάθειες του συστήματος πριν γίνουν εκμεταλλεύσιμες, πέραν της ανίχνευσης και του μετριασμού των απειλών που δεν ήταν προηγουμένως γνωστές. Ως αποτέλεσμα, οι τεχνικές που βασίζονται στο ML αντιπροσωπεύουν μια αλλαγή προς πιο έξυπνες, ευέλικτες και ισχυρές άμυνες, που εγγυώνται ότι το περιβάλλον του IoT θα προστατεύεται συνεχώς [58].

Το DL είναι ένα κρίσιμο υποσύνολο του ML το οποίο ξεχωρίζει ιδιαίτερα στον τομέα της κυβερνοασφάλειας λόγω της ικανότητας του να επεξεργάζεται και να αναλύει τις τεράστιες ποσότητες σύνθετων δεδομένων που παράγονται από τις συσκευές IoT. Παρά την αρχική επικέντρωση της

παρούσας διπλωματικής στο ML για την ασφάλεια των χαμηλών επιπέδων του IoT, η υιοθέτηση του DL οφείλεται κυρίως στην εξαιρετική του ικανότητα να εξάγει χαρακτηριστικά και να αναγνωρίζει μοτίβα. Χρησιμοποιώντας πολυεπίπεδα νευρωνικά δίκτυα, αυτή η προηγμένη μορφή του ML, μιμείται την ικανότητα του ανθρώπινου εγκεφάλου να μαθαίνει από τεράστιες ποσότητες δεδομένων. Ένα σημαντικό χαρακτηριστικό του DL που το διαφοροποιεί από το ML είναι η ικανότητα του να διαχειρίζεται τεράστιες ποσότητες δεδομένων με αποτελεσματικό τρόπο. Η παράλληλη επεξεργαστική ισχύς που παρέχουν οι μονάδες γραφικής επεξεργασίας (Graphics Processing Unit, GPU) αυξάνει περαιτέρω την αποτελεσματικότητα αυτή, με την οποία προκύπτουν πολύ ταχύτεροι χρόνοι εκπαίδευσης. Όταν τα μεγέθη δεδομένων ξεπερνούν ένα ορισμένο όριο, τα μοντέλα ML εμφανίζουν συνήθως ένα σταθερό επίπεδο επιδόσεων, ενώ τα μοντέλα DL αποδίδουν καλύτερα όσο αυξάνονται τα μεγέθη δεδομένων [58]. Αυτό το χαρακτηριστικό του DL σε συνδυασμό με την επιτάχυνση των υπολογισμών με την χρήση των GPUs επιτρέπει στα μοντέλα DL να αποδίδουν εξαιρετικά καλά σε σενάρια με μεγάλα datasets, τα οποία είναι συνηθισμένα στο IoT. Ως εκ τούτου, το DL ενισχύει το ML στην αναζήτηση εξελιγμένων λύσεων κυβερνοασφάλειας, ενώ παράλληλα διευρύνει την ικανότητα των συστημάτων ασφαλείας να προσαρμόζονται και να αναπτύσσονται ανάλογα με την αυξανόμενη πολυπλοκότητα και τον αυξανόμενο όγκο δεδομένων.




Σχήμα 4.1: *Οικογένεια AI* [59].

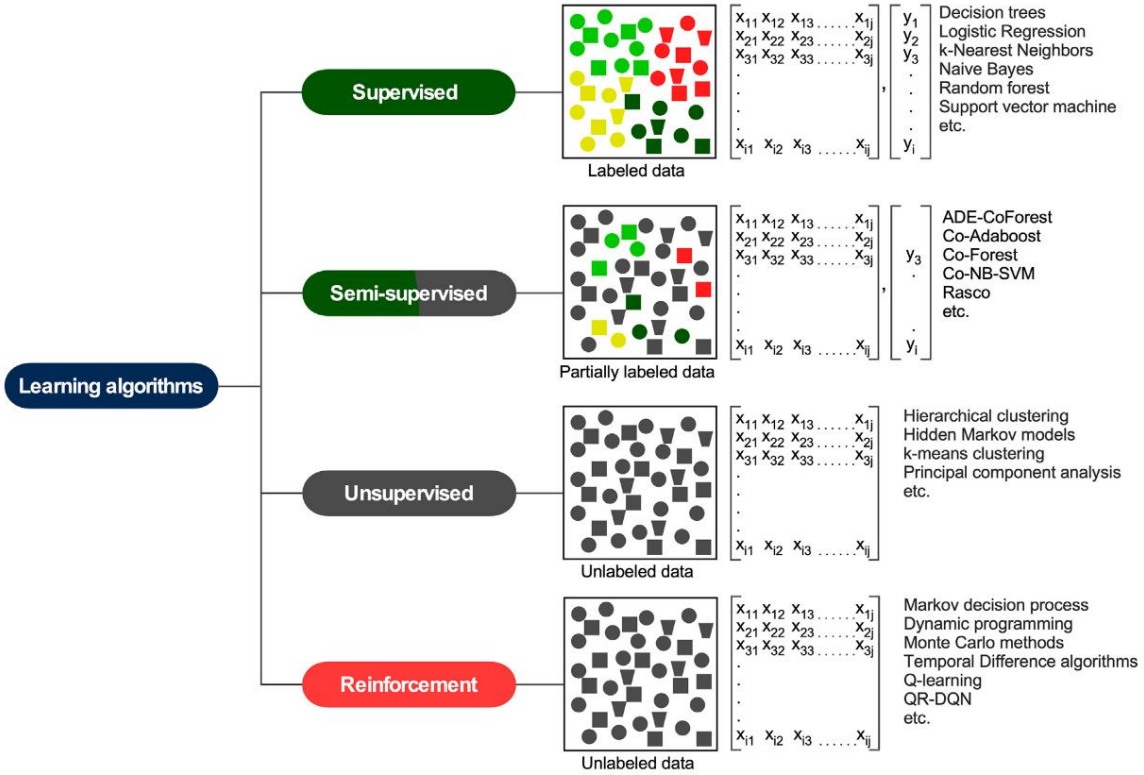
## 4.3 Μεθοδολογίες ML και DL

Οι μεθοδολογίες του ML και του DL χωρίζονται σε διάφορες τεχνικές μάθησης, κάθε μία από τις οποίες έχει ειδικές χρήσεις και πλεονεκτήματα για την ασφάλεια του IoT [58], [60], [61]:

- **Μάθηση με επίβλεψη (Supervised Learning):** Αυτή η τεχνική λειτουργεί καλά για προβλεπτικά καθήκοντα επειδή χρησιμοποιεί δεδομένα με ετικέτες (labels) για την εκπαίδευση

των μοντέλων. Η επιβλεπόμενη μάθηση έχει σημαντικό ρόλο στην ανίχνευση επιθέσεων κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service Attack, DDoS) στο IoT. Μέσω της ανάλυσης των δεδομένων που ταξινομούνται ως "κανονικά" ή "DDoS", το μοντέλο αποκτά την ικανότητα να διακρίνει μεταξύ μοτίβων κακόβουλης και καλοήθους κίνησης.

- **Μάθηση χωρίς επίβλεψη (Unsupervised Learning):** Οι αλγόριθμοι μάθησης χωρίς επίβλεψη, που λειτουργούν χωρίς την ανάγκη επισημειωμένων δεδομένων, ανακαλύπτουν κρυμμένα μοτίβα ή ανωμαλίες μέσα στα δεδομένα. Επειδή η μάθηση χωρίς επίβλεψη μπορεί να εντοπίσει νέες επιθέσεις που δεν έχουν ταξινομηθεί προηγουμένως σε datasets, είναι ιδιαίτερα χρήσιμη για την ασφάλεια του IoT.
- **Μάθηση με ημι-επίβλεψη (Semi-supervised Learning):** Η τεχνική μάθηση με ημι-επίβλεψη χρησιμοποιεί ένα μικρότερο ποσοστό επισημασμένων δεδομένων και ένα μεγαλύτερο ποσοστό μη επισημασμένων δεδομένων, συνδυάζοντας πτυχές της επιβλεπόμενης και της μη επιβλεπόμενης μάθησης. Αυτή η υβριδική προσέγγιση είναι ιδανική σε περιπτώσεις που έχουμε μικρό ποσοστό επισημασμένων δεδομένων.
- **Ενισχυτική μάθηση (Reinforcement Learning):** Η ενισχυτική μάθηση βασίζεται σε ένα σύστημα "ανταμοιβών και ποινών" και διακρίνεται από την έμφαση που δίνει στην μάθηση μέσω της αλληλεπίδρασης με το περιβάλλον. Αυτή η τεχνική λειτουργεί ιδιαίτερα καλά σε δυναμικά και απρόβλεπτα περιβάλλοντα, όπου το μοντέλο μαθαίνει μέσω δοκιμής και λάθους ποια είναι η καλύτερη απόφαση σε μία συγκεκριμένη κατάσταση.




Σχήμα 4.2: *Κατηγοριοποίηση των μεθόδων μάθησης* [62].

## 4.4 Αλγόριθμοι Μηχανικής Μάθησης

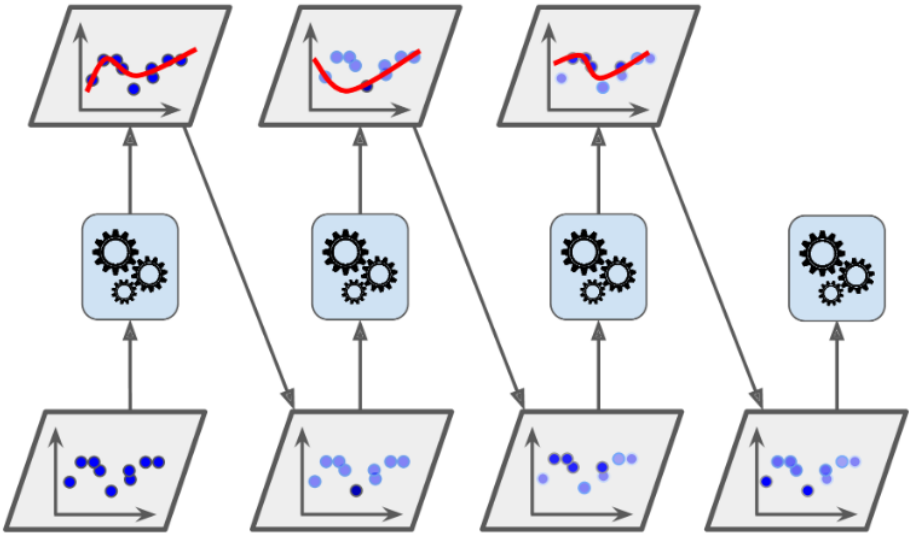
Για την αποτελεσματική προστασία των περιβαλλόντων IoT, οι αλγόριθμοι ML είναι απαραίτητοι για την δημιουργία δυναμικών στρατηγικών κυβερνοασφάλειας. Οι διάφοροι αλγόριθμοι

που έχουν επιτύχει στον εντοπισμό, την πρόβλεψη και την μείωση των κινδύνων κυβερνοασφάλειας είναι οι ακόλουθοι.

- **Decision Tree (DT):** Ένας δημοφιλής αλγόριθμος μάθησης με επίβλεψη τόσο για θέματα παλινδρόμησης όσο και για θέματα ταξινόμησης, τα DT είναι αξιοσημείωτα για την προσαρμοστικότητα τους στον τομέα της μηχανικής μάθησης [57]. Η μέθοδος αυτή χρησιμοποιεί μια δενδροειδή δομή για την μοντελοποίηση των αποφάσεων και των πιθανών αποτελεσμάτων τους. Οι κόμβοι αντιπροσωπεύουν τα χαρακτηριστικά, τα κλαδιά τα αποτελέσματα και οι κόμβοι φύλλων τις ετικέτες των κλάσεων ή τις συνεχείς τιμές [63]. Η απλότητα των DT, τόσο από άποψη υλοποίησης όσο και από άποψη κατασκευής, είναι ένα από τα κύρια πλεονεκτήματα τους. Μπορούν να χειριστούν αποτελεσματικά μεγάλα δείγματα δεδομένων και να προσφέρουν μια σαφή άποψη για την διαδικασία της λήψης των αποφάσεων. Παρά τα πλεονεκτήματα αυτά, τα DT έχουν και ορισμένα μειονεκτήματα. Είναι γεγονός ότι, λόγω του πιθανού μεγέθους τους, μπορεί να χρειάζονται πολύ αποθηκευτικό χώρο, ιδίως όταν έχουν να διαχειριστούν πολύπλοκα datasets. Η εκτεταμένη δομή του δέντρου, αν και περιεκτική, μπορεί να γίνει δυσκίνητη σε εφαρμογές όπου η αποδοτικότητα του χώρου είναι κρίσιμη, για αυτό και απαιτεί σημαντικούς πόρους μνήμης [10], [64].
- **Random Forest (RF):** Το RF είναι ένας αλγόριθμος μάθησης με επίβλεψη που μπορεί να εφαρμοστεί για την βελτίωση της ασφάλειας του IoT [64]. Το RF ξεπερνά τα παραδοσιακά DT όσον αφορά την ακρίβεια και την συνέπεια στις προβλέψεις συνδυάζοντας πολλαπλά DT σε ένα ενιαίο, ολοκληρωμένο μοντέλο. Η ικανότητα του να παρακάμπτει τα προβλήματα με την συσχέτιση των χαρακτηριστικών είναι ένα σημαντικό πλεονέκτημα [58]. Το επιτυγχάνει αυτό με τον τυχαίο διαχωρισμό των χαρακτηριστικών σε μικρότερα δείγματα, εξασφαλίζοντας μια ποικίλη και αντικειμενική διαδικασία λήψης αποφάσεων σε όλο το σύνολο των δέντρων του. Παρά την αποτελεσματικότητα του, η δυνατότητα εφαρμογής του RF σε ορισμένες εφαρμογές πραγματικού χρόνου μπορεί να είναι περιορισμένη, ιδίως σε περιπτώσεις όπου απαιτούνται μεγάλα datasets εκπαίδευσης. Όταν το RF χρησιμοποιείται σε καταστάσεις που απαιτούν γρήγορη ανάλυση σε πραγματικό χρόνο, μπορεί να γίνει απαιτητικό σε πόρους λόγω της ανάγκης δημιουργίας πολλαπλών DT [64], [65].
- **k-Nearest Neighbor (KNN):** Ο αλγόριθμος kNN, γνωστός για την στατιστική μη παραμετρική προσέγγιση του στην επιβλεπόμενη μάθηση, χρησιμοποιεί την ευκλείδεια απόσταση για την αξιολόγηση της απόστασης και της ομοιότητας μεταξύ των σημείων δεδομένων [63]. Η ομαδοποίηση των δεδομένων εκπαίδευσης με βάση προκαθορισμένα κριτήρια αποτελεί βασικό στοιχείο του αλγορίθμου, καθώς επιτρέπει την σύγκριση των εισερχόμενων δεδομένων με τους προκαθορισμένους “k” πλησιέστερους γείτονες για τον προσδιορισμό της ομοιότητας [66]. Γνωστο για την ευκολία χρήσης του, το kNN είναι ένα προσιτό εργαλείο με ευρύ φάσμα εφαρμογών, καθώς είναι προσιτό και εύκολο στην εφαρμογή. Είναι σημαντικό να σημειωθεί ότι μπορεί να είναι χρονοβόρο, ιδίως όταν προσπαθεί να εντοπίσει ανωμαλίες σε μεγάλα datasets. Αυτό μπορεί να οδηγήσει σε προβλήματα τόσο με την ακρίβεια των αποτελεσμάτων όσο και με την υπολογιστική αποδοτικότητα [10], [64].
- **Naive Bayes (NB):** Ο αλγόριθμος NB είναι μια πιθανολογική μέθοδος που βασίζεται στο θεώρημα Bayes και εφαρμόζεται κυρίως όπου χρειάζεται ταξινόμηση σε περιβάλλοντα μάθησης με επίβλεψη [67]. Λειτουργεί υποθέτοντας ότι τα χαρακτηριστικά των δεδομένων εισόδου είναι ανεξάρτητα μεταξύ τους και προβλέποντας την πιθανότητα διαφόρων κλάσεων με βάση αυτά τα χαρακτηριστικά. Η απλότητα του όσον αφορά την εννοιολογική κατανόηση και την πρακτική εφαρμογή είναι ένα από τα κύρια πλεονεκτήματα του. Σε σύγκριση με άλλους

αλγορίθμους μηχανικής μάθησης, μπορεί να λειτουργήσει πιο αποτελεσματικά με λιγότερα δεδομένα, γεγονός που το καθιστά ιδιαίτερα χρήσιμο σε περιπτώσεις όπου η συλλογή μεγάλων dataset είναι δύσκολη [10], [64].

- **Linear Regression (LR):** Ένας θεμελιώδης στατιστικός αλγόριθμος, ο LR χρησιμοποιεί μάθηση με επίβλεψη για να μοντελοποιήσει την γραμμική σχέση μεταξύ μιας εξαρτημένης μεταβλητής και μιας ή περισσότερων ανεξάρτητων μεταβλητών. Μέσω της διαδικασίας προσαρμογής μιας γραμμικής εξίσωσης σε παρατηρούμενα δεδομένα, ο LR μπορεί να χρησιμοποιηθεί για τον εντοπισμό ανωμαλιών στην κυκλοφορία του δικτύου IoT ή για την πρόβλεψη κινδύνων ασφαλείας συγκρίνοντας τις παρατηρούμενες αποκλίσεις από τις αναμενόμενες συμπεριφορές [68], [69].
- **Support Vector Machine (SVM):** Ο εξαιρετικά αποτελεσματικός αλγόριθμος επιβλεπόμενης μάθησης SVM χρησιμοποιείται κυρίως για εφαρμογές ταξινόμησης και λειτουργεί καλά σε περιβάλλοντα υψηλών διαστάσεων. Η εύρεση του ιδανικού υπερεπιπέδου που μεγιστοποιεί το περιθώριο μεταξύ των πλησιέστερων σημείων δεδομένων διαφόρων κλάσεων, γνωστά ως διανύσματα υποστήριξης (support vectors), αποτελεί το βασικό συστατικό της μεθοδολογίας SVM [57]. Όταν το dataset δεν είναι υπερβολικά μεγάλο, η ικανότητα του SVM να παρέχει υψηλή ακρίβεια ταξινόμησης με μικρότερη κατανάλωση υπολογιστικής ισχύος από άλλα πολύπλοκα μοντέλα είναι ένα από τα κύρια πλεονεκτήματα του. Λόγω της αποτελεσματικότητας του, το SVM είναι μια επιθυμητή επιλογή για εφαρμογές ασφαλείας του IoT, όπου η ακριβής και έγκαιρη ανίχνευση των απειλών είναι απαραίτητη. Παρά τα πλεονεκτήματα του, το SVM παρουσιάζει ορισμένες δυσκολίες βελτιστοποίησης λόγω της εξάρτησης του από την κατάλληλη επιλογή του πυρήνα και των παραμέτρων, καθώς και της υπολογιστικής του απαίτησης για μεγάλα datasets [10], [58].
- **Ensemble Learning (EL):** Ένας ανερχόμενος αλγόριθμος μάθησης είναι το EL, το οποίο είναι μια συλλογή αλγορίθμων που συνδυάζει τα πλεονεκτήματα πολλών μοντέλων για να βελτιώσει την συνολική απόδοση [57]. Οι δημοφιλέστεροι αλγόριθμοι EL είναι οι εξής:
    1. **Gradient Boosting Algorithm (GBA):** Χρησιμοποιώντας DT ως βασικό αλγόριθμο εκπαίδευσης, ο GBA επικεντρώνεται στην βελτίωση των προβλέψεων με την διαδοχική διόρθωση σφαλμάτων από προηγούμενα μοντέλα. Οι δυνατότητες του κύριου αλγορίθμου GBA επεκτείνονται από τις βασικές παραλλαγές του, τον XGBoost και τον LightGBM. Με την αυξημένη αποδοτικότητα και επεκτασιμότητα του, ο XGBoost βελτιώνει την ταχύτητα και την απόδοση, καθιστώντας τον μια εφικτή επιλογή για εφαρμογές ασφαλείας σε πραγματικό χρόνο [60], [70]. Ο LightGBM, βελτιώνει αυτή την στρατηγική μεγιστοποιώντας την ταχύτητα επεξεργασίας και την χρήση των πόρων του συστήματος, γεγονός που την καθιστά ιδιαίτερα χρήσιμη για μεγάλα datasets [71]. Και οι δύο παραλλαγές του αλγορίθμου είναι φτιαγμένες για να αντιμετωπίσουν τις υπολογιστικές δυσκολίες που συνοδεύονται από τον GBA, εξασφαλίζοντας εξαιρετική ακρίβεια χωρίς να απαιτούν μεγάλη επεξεργαστική ισχύ [63].
    2. **AdaBoost:** Ο στόχος του AdaBoost είναι η δημιουργία ενός ισχυρού προγνωστικού μοντέλου συνδυάζοντας έναν αριθμό αδύναμων ταξινομητών. Μέσω της επαναληπτικής τροποποίησης των βαρών των λανθασμένων ταξινομημένων παραδειγμάτων, ο AdaBoost τονίζει τα πιο δύσκολα χαρακτηριστικά του dataset σε μεταγενέστερα μοντέλα [60], [63].



Σχήμα 4.3: *Διαδοχική εκπαίδευση AdaBoost με ενημερώσεις των βαρών* [60].

- **k-Means:** Ο αλγόριθμος k-Means είναι ένας απλός αλλά αποτελεσματικός αλγόριθμος μάθησης χωρίς επίβλεψη, ο οποίος θεωρείται ιδιαίτερα σημαντικός για τις ικανότητες του στην ομαδοποίηση. Είναι ιδιαίτερα κατάλληλος για εφαρμογές ασφαλείας του IoT, όπου δεν υπάρχουν labeled δεδομένα. Αναδεικνύοντας τις ακραίες τιμές (outliers), διευκολύνει τον εντοπισμό ανωμαλιών και πιθανών κινδύνων με την ομαδοποίηση των δεδομένων σύμφωνα με προκαθορισμένα κριτήρια. Παρόλο που θεωρείται λιγότερο αποτελεσματικός αλγόριθμος σε σύγκριση με αλγόριθμους που χρησιμοποιούν επιβλεπόμενη μάθηση, το χαμηλό υπολογιστικό κόστος και η ευκολία υλοποίησης του, το καθιστούν μία καλή επιλογή για την ανάλυση των δεδομένων που παράγονται από τα συστήματα IoT [10], [57].

Πίνακας 4.1: Σύνοψη αλγορίθμων ML

| **Αλγόριθμος** | **Τρόπος Μάθησης** | **Πλεονεκτήματα** | **Μειονεκτήματα** |
|---|---|---|---|
| DT | Supervised | Απλός | Αποθηκευτικός χώρος |
| RF | Supervised | Συσχέτιση χαρακτηριστικών | Περιορισμός σε εφαρμογές πραγματικού χρόνου |
| KNN | Supervised | Εύκολη χρήση | Χρονοβόρος σε μεγάλα datasets |
| NB | Supervised | Απλός | Μη αποτελεσματικός σε μεγάλα datasets |
| SVM | Supervised | Υψηλή ακρίβεια με μικρή κατανάλωση ισχύος | Εξαρτάται από την επιλογή του πυρήνα και των παραμέτρων |
| XGBoost | Supervised | Ταχύτατος, Αποδοτικός Κατάλληλος για εφαρμογές σε πραγματικό χρόνο | - |

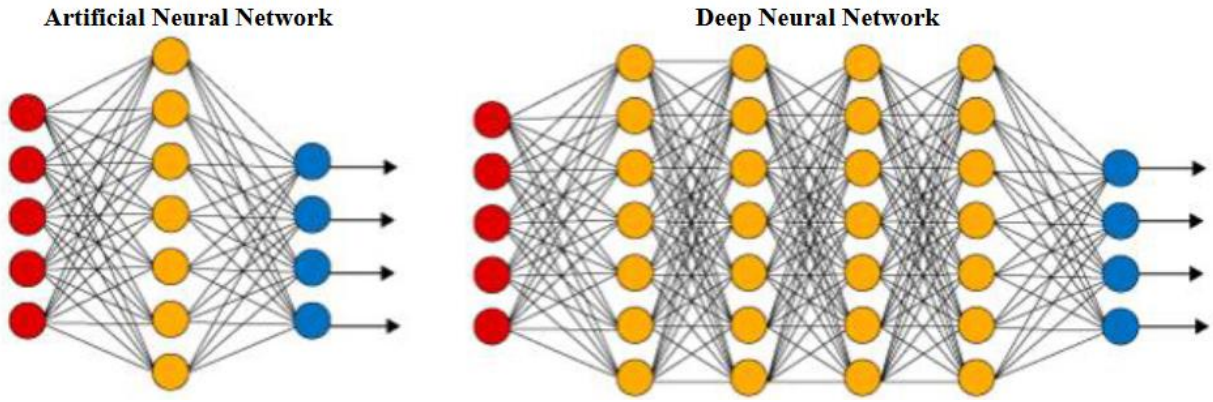
| | | | |
|---|---|---|---|
| LightGBM | Supervised | Μεγιστοποιεί την ταχύτητα επεξεργασίας<br>Μεγιστοποιεί τους πόρους του συστήματος<br>Ιδανικός για μεγάλα datasets | - |
| AdaBoost | Supervised | Τονίζει τα δύσκολα χαρακτηριστικά σε ένα dataset | - |
| k-Means | Unsupervised | Χαμηλό υπολογιστικό κόστος<br>Εύκολο στην υλοποίηση | Λιγότερο αποτελεσματικός συγκριτικά με άλλους αλγορίθμους |

## 4.5 Αλγόριθμοι Βαθιάς Μάθησης

Η αιχμή της τεχνολογίας στο ML αντιπροσωπεύεται από αλγορίθμους DL, οι οποίοι επιτρέπουν την καλύτερη κατανόηση μεγάλων και πολύπλοκων datasets. Το παρόν υποκεφάλαιο εξετάζει συγκεκριμένους αλγορίθμους DL που έχουν διαδραματίσει σημαντικό ρόλο στην επανάσταση των πρωτοκόλλων ασφαλείας του IoT.

- **Artificial Neural Networks (ANN):** Το DL είναι μια αναπαράσταση του ανθρώπινου εγκεφάλου, όπως αναφέρθηκε στην αρχή του κεφαλαίου. Επεκτείνοντας αυτή την ιδέα, τα ANN παρέχουν την θεμελιώδη δομή και λειτουργικότητα που απαιτούνται για την προσομοίωση της δομής και των λειτουργιών του εγκεφάλου [72]. Ένα επίπεδο εισόδου, ένα ή δύο κρυφά επίπεδα και ένα επίπεδο εξόδου είναι τα τρία διασυνδεδεμένα επίπεδα νευρώνων που συνθέτουν ένα ANN. Κάθε νευρώνας σε αυτά τα επίπεδα συνδέεται μέσω βαρών που προσαρμόζονται κατά την διάρκεια της διαδικασίας της μάθησης για την καλύτερη μοντελοποίηση των μοτίβων [57], [73].

  Με την προσθήκη περισσότερων κρυφών επιπέδων, τα Deep Neural Networks (DNN) βελτιώνουν τις δυνατότητες των συνηθισμένων ANN. Τα DNNs μπορούν να χειριστούν πιο περίπλοκους μετασχηματισμούς δεδομένων και να βελτιώσουν τις δυνατότητες της αναπαράστασης και της ταξινόμησης, χάρη σε αυτή την βαθύτερη αρχιτεκτονική [57], [74]. Τα πολλαπλά κρυφά επίπεδα των DNNs καθιστούν δυνατή την περαιτέρω επεξεργασία των χαρακτηριστικών, πράγμα απαραίτητο για την ασφάλεια του IoT που απαιτείται βαθιά κατανόηση και ερμηνεία.




Σχήμα 4.4: *ANN vs DNN* [73].

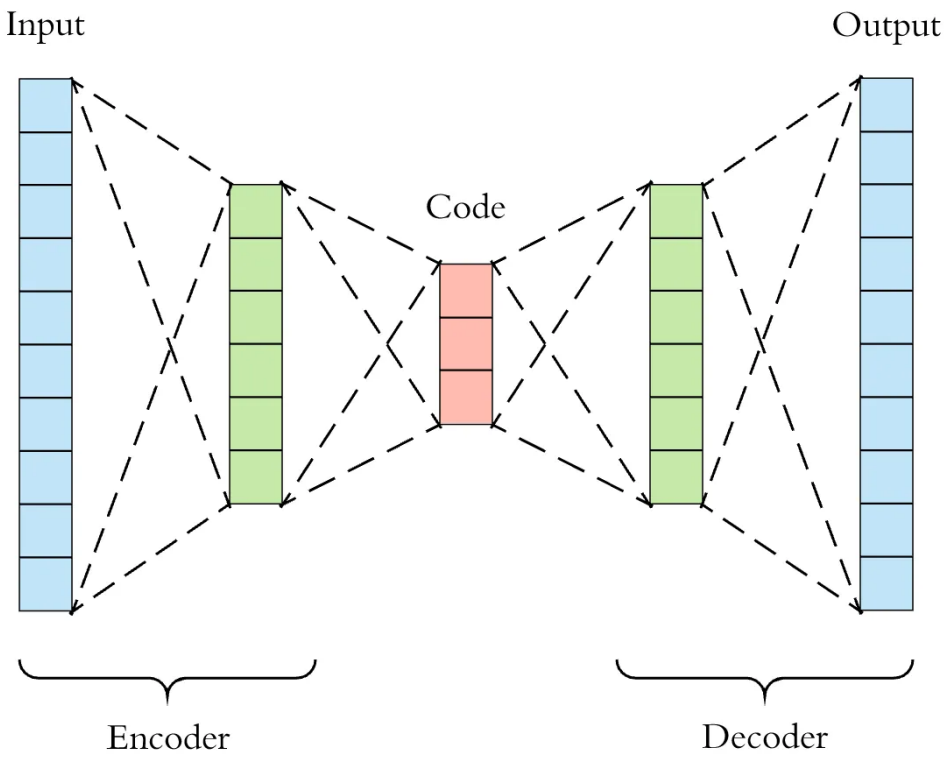
- **Recurrent Neural Networks (RNN):** Οι συσκευές IoT παράγουν πολλά διαδοχικά δεδομένα, τα οποία τα RNNs μπορούν να τα επεξεργαστούν με μεγάλη επιτυχία. Λόγω αυτού του χαρακτηριστικού, τα RNNs είναι ιδιαίτερα κατάλληλα για την ασφάλεια του IoT, όπου ο εντοπισμός ανωμαλιών και άλλων πιθανών απειλών απαιτεί την ανάλυση δεδομένων χρονοσειρών από τις συσκευές. Λόγω της ιδιαίτερης ικανότητας τους να επεξεργάζονται και να διατηρούν πληροφορίες από προηγούμενες εισόδους, τα RNNs είναι σε θέση να προβλέπουν καλύτερα τις μελλοντικές ευπάθειες, επειδή μπορούν να κατανοήσουν την χρονική δυναμική στις ακολουθίες των δεδομένων. Επίσης μπορούν διαχειρίζονται πιο εύκολα τα καινούργια δεδομένα εισόδου που έρχονται [57], [58].
- **Long Short-Term Memory (LSTM):** Αξιοποιώντας τις δυνατότητες των RNNs, τα LSTMs παρέχουν μια βελτιωμένη λύση ελαχιστοποιώντας ορισμένες από τις προκλήσεις των RNNs [72]. Τα LSTM είναι ειδικά σχεδιασμένα για να θυμούνται πληροφορίες για μεγάλα χρονικά διαστήματα, ξεπερνώντας τους παραδοσιακούς τεχνητούς νευρώνες όσον αφορά την διατήρηση των δεδομένων. Για την πλήρη αξιοποίηση των LSTM, ωστόσο, απαιτείται μεγαλύτερος όγκος δεδομένων και μεγαλύτερη επεξεργαστική ισχύς, και λόγω της πολυπλοκότητας της αρχιτεκτονικής των LSTM, η εκπαίδευση διαρκεί σημαντικά περισσότερο χρόνο [57], [58].

  Στην έρευνα [75], παρουσιάστηκε το μοντέλο LSTM+, το οποίο αναπτύσει περαιτέρω την τεχνολογία LSTM και παρέχει σημαντικές βελτιώσεις σε σχέση με την προηγούμενη έκδοση. Εκτός από την μείωση του σφάλματος παλινδρόμησης, το μοντέλο LSTM+ είναι ικανό να ανιχνεύει δεδομένα που συλλέγονται από τις IoT συσκευές σε πραγματικό χρόνο. Έχει την ικανότητα να χειρίζεται αποτελεσματικά τα ανώμαλα δεδομένα, εξασφαλίζοντας ότι η λειτουργικότητα του δικτύου παραμένει εξαιρετικά σταθερή και ανθεκτική. Αυτό το χαρακτηριστικό είναι ιδιαίτερα χρήσιμο για την ασφάλεια του IoT, επειδή βελτιώνει την ικανότητα του συστήματος να διαχειρίζεται και να αντιδρά στα μεγάλα και δυναμικά περιβάλλοντα.

- **Convolutional Neural Networks (CNN):** Τα δίκτυα CNN έχουν χρησιμοποιηθεί ευρέως στην επεξεργασία της εικόνας και γλώσσας σε υπολογιστές. Αυτά τα μοντέλα είναι ικανά να αξιολογούν χαρακτηριστικά μέσω πράξεων συνέλιξης, γεγονός που τους επιτρέπει να επεξεργάζονται απευθείας ακατέργαστες εικόνες χωρίς την ανάγκη προ-επεξεργασίας [76]. Μέσω αυτής της διαδικασίας, τα CNNs μπορούν να εξάγουν αποτελεσματικά και αυτόματα σημαντικά χαρακτηριστικά. Λόγω των εξελιγμένων μηχανισμών, τα CNNs είναι γνωστά για την επίτευξη υψηλότερης ακρίβειας σε δύσκολες διαδικασίες. Αλλά για να επιτευχθούν τόσο

αυτά τα υψηλά επίπεδα ακρίβειας, η ικανότητα αυτή έχει ως κόστος την απαίτηση σημαντικής επεξεργαστικής ισχύος [58], [64].

- **Autoencoders (AE):** Οι AE διαθέτουν την αξιοσημείωτη ικανότητα να μαθαίνουν και να ταξινομούν την έξοδο αυτόματα, παρακάμπτοντας την ανάγκη για labeled δεδομένα. Λόγω αυτού, είναι πολύ κατάλληλοι για εφαρμογές μάθησης χωρίς επίβλεψη, όπως η ανίχνευση ανωμαλιών και η μείωση των διαστάσεων [58]. Ο κωδικοποιητής και ο αποκωδικοποιητής είναι δύο κρίσιμες φάσεις που είναι απαραίτητες για την λειτουργία των AE. Προκειμένου να δημιουργηθεί μια έξοδος που είναι όσο το δυνατόν πιο κοντά στην αρχική είσοδο, το στάδιο του κωδικοποιητή συμπιέζει τα δεδομένα εισόδου σε μια συμπαγή αναπαράσταση. Στην συνέχεια, ο αποκωδικοποιητής ανακατασκευάζει τα δεδομένα από αυτή την συμπαγή αναπαράσταση. Εκτός από ότι επιτρέπει την αποτελεσματική αναπαράσταση των δεδομένων, αυτή η διαδικασία δύο σταδίων έχει αποδειχθεί ότι είναι αποδοτική από πλευράς μνήμης και υπολογιστικής απόδοσης κατά τον χειρισμό αισθητηριακών εισόδων όπως ηχητικά κύματα, εικόνες και βίντεο. Παρά τα πλεονεκτήματα τους, είναι σημαντικό να αναφερθεί ότι οι AE μπορούν να απαιτούν σημαντικό χρόνο επεξεργασίας λόγω της πολυπλοκότητας της διαδικασίας εκπαίδευσης τους και της απαίτησης προσαρμογής της αρχιτεκτονικής και των παραμέτρων τους [57], [64].




Σχήμα 4.5: *Αναπαράσταση AE* [77].

- **Restricted Boltzmann Machines (RBM):** Τα RBMs είναι βαθιά παραγωγικά μοντέλα που έχουν σχεδιαστεί κυρίως για εφαρμογές μάθησης χωρίς επίβλεψη. Το χαρακτηριστικό τους ως διακριτικά μοντέλα είναι η ικανότητα τους να κατηγοριοποιούν δείγματα δεδομένων σύμφωνα με τις αναπαραστάσεις που έχουν μάθει για τα δεδομένα εισόδου. Το ορατό επίπεδο, το οποίο δέχεται τα δεδομένα εισόδου, και το κρυφό επίπεδο, το οποίο προσπαθεί να εντοπίσει και να απεικονίσει τα χαρακτηριστικά των δεδομένων, είναι τα δύο βασικά επίπεδα που αποτελούν την βάση των RBM [57], [64].

- **Deep Belief Networks (DBN):** Τα DBN είναι εξελιγμένα μοντέλα DL που αποτελούνται από πολλά RBMs και προορίζονται για την εκμάθηση αναπαραστάσεων δεδομένων σε ιεραρχική μορφή. Τα DBNs αποδίδουν καλά τόσο σε εφαρμογές μάθησης με επίβλεψη όσο και σε εφαρμογές μάθησης χωρίς επίβλεψη. Εκπαιδεύονται με την χρήση στοιβαγμένων RBMs με μη επιβλεπόμενο τρόπο για την εύρεση σύνθετων μοτίβων στα δεδομένα και στην συνέχεια βελτιώνονται με την χρήση επιβλεπόμενων τεχνικών, όπως η ταξινόμηση [60]. Λόγω της βαθιάς αρχιτεκτονικής τους, τα DBNs έχουν το πλεονέκτημα ότι μπορούν να καταγράψουν αφηρημένα μοτίβα δεδομένων, αλλά παρουσιάζουν επίσης δυσκολίες όσον αφορά τις υπολογιστικές απαιτήσεις και την πολυπλοκότητα της εκπαίδευσης [64].

## 4.6 Μετρικές αξιολόγησης

Η κατανόηση και η ακριβής μέτρηση της αποτελεσματικότητας των διαφόρων αμυντικών μηχανισμών είναι εξαιρετικά σημαντική στον τομέα της ασφάλειας, ιδίως στην ανάπτυξη και την αξιολόγηση των IDS (Intrusion Detection System). Οι βασικές μετρικές, όπως το accuracy, το precision, το recall και το F1-score, έχουν βασικό ρόλο σε αυτή την αξιολόγηση, παρέχοντας πληροφορίες σχετικά με την αξιοπιστία και την αποτελεσματικότητα των λύσεων ασφαλείας. Παρακάτω παρουσιάζονται αυτές οι μετρικές [58], [78]:

- **Accuracy:** Μία από τις πιο βασικές μετρήσεις είναι το accuracy. Είναι το ποσοστό των παρατηρήσεων που προβλέφθηκαν με ακρίβεια. Η ερώτηση "από όλες τις ταξινομήσεις, πόσες τα ταξινόμησε σωστά το σύστημα;", απαντάται από το accuracy.
- **Precision:** Το precision μετράει πόσο ακριβείς είναι οι θετικές προβλέψεις που έκανε το μοντέλο. Ουσιαστικά αξιολογεί το ποσοστό των θετικών προβλέψεων που έγιναν από το μοντέλο και ήταν πράγματι σωστές.
- **Recall:** Το recall μετρά την ικανότητα ενός μοντέλου να εντοπίζει όλες τις σχετικές περιπτώσεις σε ένα dataset. Για παράδειγμα, ένα dataset περιλαμβάνει 10 περιπτώσεις κακόβουλης κυκλοφορίας. Εάν το μοντέλο αναγνωρίσει σωστά και τις 10 κακόβουλες περιπτώσεις, τότε το recall είναι 100%, υποδεικνύοντας ότι το μοντέλο κατέγραψε επιτυχώς όλη την κακόβουλη κυκλοφορία που υπάρχει στο dataset.
- **F1-score:** Το F1-score είναι μια σημαντική μετρική που συνδυάζει το precision και το recall σε ένα ενιαίο μέτρο. Καταγράφει τόσο την ακρίβεια των θετικών προβλέψεων όσο και την ικανότητα του μοντέλου να εντοπίζει όλες τις σχετικές περιπτώσεις.

## 4.7 Επίλογος

Αυτό το κεφάλαιο έχει θέσει με επιτυχία μια σταθερή βάση σχετικά με το ML και το DL, που κυμαίνεται από τις θεμελιώδεις αρχές έως τους πολύπλοκους αλγορίθμους. Αυτή η λεπτομερείς εξέταση όχι μόνο δίνει έμφαση στις θεωρητικές πτυχές αυτών των ισχυρών πεδίων, αλλά θέτει επίσης τις βάσεις για την συζήτηση των πρακτικών εφαρμογών τους στα επόμενα κεφάλαια. Επίσης, η έμφαση στους διαφορετικούς αλγορίθμους και η εισαγωγή των σημαντικών μετρικών αξιολόγησης προετοιμάζει τον αναγνώστη για την ενδελεχή κατανόηση και αξιολόγηση της αποτελεσματικότητας αυτών των μοντέλων. Αυτή η θεμελιώδης κατανόηση είναι απαραίτητη για την αποτελεσματική εφαρμογή αυτών των τεχνολογιών και την διασφάλιση της βέλτιστης απόδοσης τους σε πραγματικές συνθήκες.

# 5. Βασικές Αρχές Κυβερνοασφάλειας

## 5.1 Εισαγωγή

Η σημασία της κυβερνοασφάλειας σε έναν κόσμο όπου το IoT κατακτά τη εξουσία, δεν μπορεί να μην επισημανθεί. Ο αριθμός των διασυνδεδεμένων συσκευών αυξάνεται εκθετικά, καλύπτοντας διάφορους κλάδους. Αυτό αυξάνει τις πιθανές επιθέσεις από κακόβουλους χρήστες. Το ρίσκο είναι υψηλότερο από ποτέ, με τις συνδεδεμένες ιατρικές συσκευές να μεταδίδουν ιδιωτικά δεδομένα των ασθενών και τις υποδομές έξυπνων πόλεων να διαχειρίζονται ζωτικά συστήματα. Ως αποτέλεσμα, η διατήρηση της ακεραιότητας και της ασφάλειας του IoT έχει καταστεί ύψιστη προτεραιότητα τόσο για τις επιχειρήσεις όσο και για τους ιδιώτες.

Στο κεφάλαιο αυτό παρουσιάζονται οι βασικές αρχές της ασφάλειας στον κυβερνοχώρο, παρέχοντας μια σταθερή βάση για την ενίσχυση της κατανόησης της ασφάλειας του IoT. Η καθιέρωση ενός κοινού λεξιλογίου είναι απαραίτητη καθώς διερευνώνται οι πολυπλοκότητες της διασφάλισης διασυνδεδεμένων συστημάτων. Με την εξοικείωση με τους βασικούς όρους της κυβερνοασφάλειας, διευκολύνεται η βαθύτερη κατανόηση της φύσης των απειλών στον κυβερνοχώρο και η ανάπτυξη αποτελεσματικών στρατηγικών άμυνας.

## 5.2 Περιουσιακά στοιχεία (Assets)

Στον τομέα της κυβερνοασφάλειας, τα περιουσιακά στοιχεία είναι τα πολύτιμα μέρη του ψηφιακού συστήματος ενός οργανισμού που πρέπει να προστατεύονται από διάφορους τύπους επιθέσεων και αδυναμιών. Τα εν λόγω περιουσιακά στοιχεία καλύπτουν ένα ευρύ φάσμα προϊόντων και υπηρεσιών, ξεπερνώντας τα συνηθισμένα στοιχεία και συμπεριλαμβάνοντας υποδομές, λογισμικό, υλικά, δεδομένα και πνευματική ιδιοκτησία. Ο ορισμός αυτός διευρύνεται για να συμπεριλάβει τις συνδεδεμένες συσκευές και τους αισθητήρες, οι οποίοι αποτελούν βασικά στοιχεία στο τεράστιο και διασυνδεδεμένο δίκτυο του IoT. Κάθε περιουσιακό στοιχείο είναι ουσιώδες για το ανταγωνιστικό πλεονέκτημα και την λειτουργική ακεραιότητα ενός οργανισμού, είτε πρόκειται για ένα δίκτυο συσκευών IoT, είτε για μία απλή βάση δεδομένων που περιέχει ευαίσθητα δεδομένα, είτε για ένα κομμάτι λογισμικού. Εξαιτίας αυτού, η ασφάλεια αυτών των περιουσιακών στοιχείων είναι πολύ σημαντική για την διατήρηση της εμπιστοσύνης και της ιδιωτικότητας των χρηστών που βασίζονται σε αυτά τα συστήματα, καθώς και για την προστασία των πόρων του οργανισμού [79].

## 5.3 Ευπάθειες (Vulnerabilities)

Οι ευπάθειες είναι αδυναμίες σε ένα σύστημα, δίκτυο ή λογισμικό, οι οποίες μπορούν να χρησιμοποιηθούν από κακόβουλους χρήστες για να παραβιάσουν την ασφάλεια και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Αυτές οι ευπάθειες μπορούν να λάβουν πολλές διαφορετικές μορφές, όπως ξεπερασμένο λογισμικό, λάθη κωδικοποίησης και λανθασμένες ρυθμίσεις. Ιδιαίτερα στον αναπτυσσόμενο τομέα του IoT, η κατανόηση των ευπαθειών αποκτά πρόσθετη σημασία λόγω της μοναδικής και πολύπλοκης φύσης των δικτύων και των συσκευών. Τα περιβάλλοντα IoT, που χαρακτηρίζονται από την εκτεταμένη συνδεσιμότητα και την ενσωμάτωση ποικίλων συσκευών, εισάγουν πληθώρα προκλήσεων ασφαλείας [79].

Είναι απαραίτητο να γίνει λεπτομερής ανάλυση των ευπαθειών στα δίκτυα και τις συσκευές του IoT, προκειμένου να αναπτυχθούν ολοκληρωμένες στρατηγικές ασφάλειας που να ανταποκρίνονται

στα μοναδικά χαρακτηριστικά του IoT. Αυτού του είδους η ανάλυση, η οποία θα καλυφθεί σε επόμενο κεφάλαιο, στοχεύει στην επεξήγηση των πολύπλοκων προκλήσεων ασφαλείας που υπάρχουν.

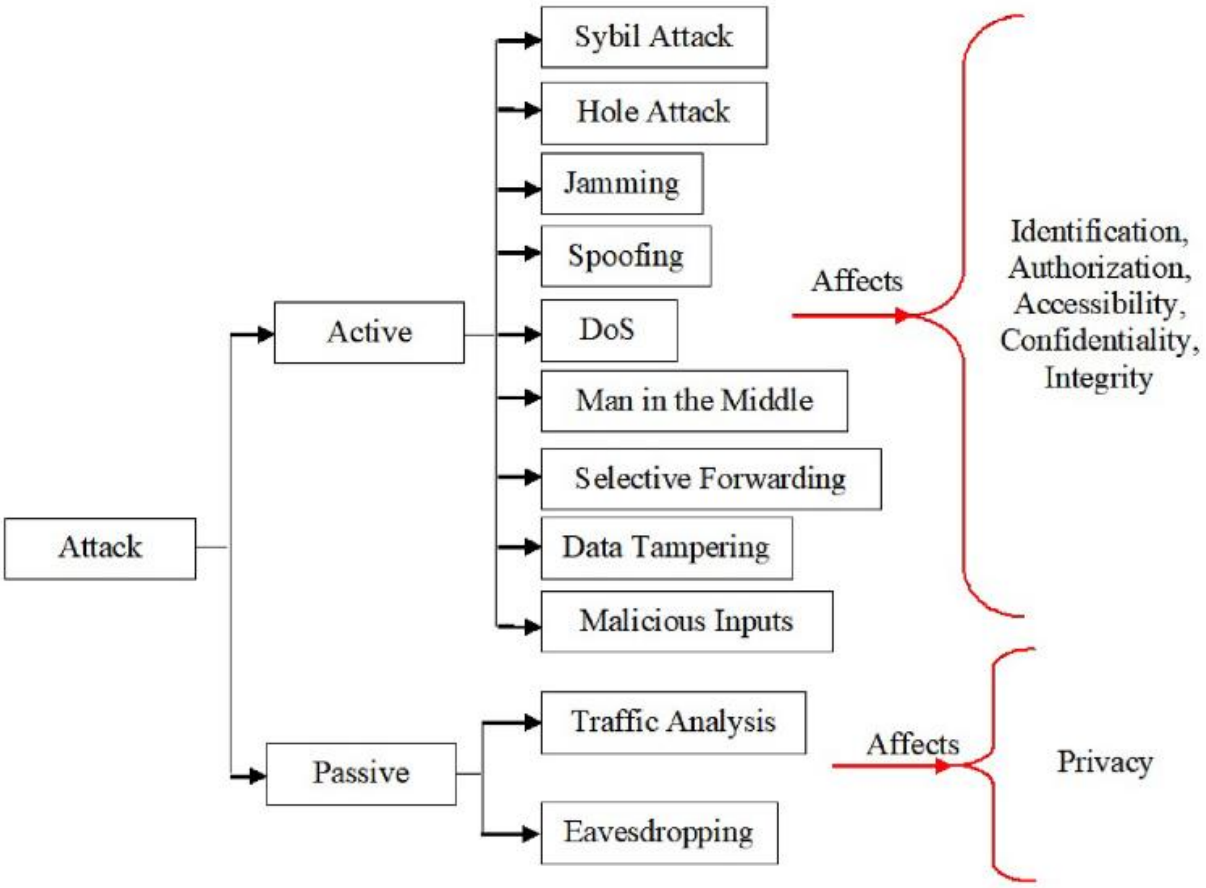
## 5.4 Απειλές (Threats)

Οι απειλές αναφέρονται σε οποιεσδήποτε πιθανές ενέργειες που θα μπορούσαν να εκμεταλλευτούν τις ευπάθειες των περιουσιακών στοιχείων ενός οργανισμού για να προκαλέσουν ζημιά. Αυτές οι απειλές κατηγοριοποιούνται σε δύο βασικές κατηγορίες: τις ανθρώπινες απειλές, οι οποίες περιλαμβάνουν ενέργειες κακόβουλων χρηστών, και τις φυσικές καταστροφές, που περιλαμβάνουν γεγονότα όπως πλημμύρες, σεισμούς ή πυρκαγιές που μπορούν να οδηγήσουν σε ζημιές στις υποδομές. Οι διαφορές μεταξύ αυτών των κατηγοριών αναδεικνύουν την ποικιλία των απειλών που πρέπει να ξεπεράσουν οι οργανισμοί για να προστατευτούν [79].

## 5.5 Επιθέσεις (Attacks)

Οι επιθέσεις περιλαμβάνουν ένα σύνολο σκόπιμων και κακόβουλων ενεργειών που πραγματοποιούνται κατά των ψηφιακών περιουσιακών στοιχείων ή της υποδομής ενός οργανισμού. Οι παθητικές (passive) και οι ενεργητικές (active) επιθέσεις είναι οι δύο κύριες κατηγορίες επιθέσεων που στοχεύουν τα συστήματα IoT, καθεμία από τις οποίες θέτει ξεχωριστές προκλήσεις και κινδύνους για την ασφάλεια.

Οι παθητικές επιθέσεις είναι κρυφές προσπάθειες υποκλοπής και απόκτησης ιδιωτικών δεδομένων χωρίς την επίγνωση του χρήστη. Αυτές οι επιθέσεις είναι αφανείς, καθώς εκμεταλλεύονται τις ευπάθειες του δικτύου για την υποκλοπή (eavesdropping) των επικοινωνιών και την ανάλυση της κυκλοφορίας (traffic analysis). Μέσω της χρήσης των συσκευών IoT, οι επιτιθέμενοι είναι σε θέση να συλλέγουν και να εκμεταλλεύονται κρυφά ιδιωτικές πληροφορίες, θέτοντας σε κίνδυνο την ιδιωτικότητα του δικτύου. Οι ενεργές επιθέσεις από την άλλη πλευρά, περιλαμβάνουν πιο εμφανή χειραγώγηση της λειτουργίας του δικτύου με στόχο την παρεμβολή στις υπηρεσίες και την διακινδύνευση της ακεραιότητας των δεδομένων. Οι επιτιθέμενοι χρησιμοποιούν μεθόδους όπως πλημμύρες (flooding), παρεμβολές (jamming) και άρνηση παροχής υπηρεσιών (Denial of Service, DoS) για να παρεμποδίσουν την επικοινωνία και να επιδεινώσουν την αποδοτικότητα του δικτύου [7], [10].




Σχήμα 5.1: *Διαφορετικά είδη ενεργητικών και παθητικών επιθέσεων, συμπεριλαμβανομένων των επιπτώσεών τους* [10].

## 5.6 Μοντέλα Κυβερνοασφάλειας

Η ανάγκη διασφάλισης της εμπιστευτικότητας (confidentiality), της ακεραιότητας (integrity) και της διαθεσιμότητας (availability) των δεδομένων και των συστημάτων βρίσκεται στο επίκεντρο της κυβερνοασφάλειας. Αυτοί οι τρεις βασικοί πυλώνες, οι οποίοι μαζί αποτελούν την τριάδα CIA (Confidentiality, Integrity, Availability), αποτελούν την βάση των αρχών της κυβερνοασφάλειας και καθοδηγούν τις προσπάθειες μας για την προστασία ευαίσθητων δεδομένων και την διασφάλιση της συνεχιζόμενης λειτουργίας βασικών υπηρεσιών. Το μοντέλο ενισχύεται από το AAA (Authentication, Authorization, Accounting), το οποίο παρέχει ισχυρούς μηχανισμούς ελέγχου πρόσβασης μέσω της ενσωμάτωσης της αυθεντικοποίησης (authentication), της εξουσιοδότησης (authorization) και της καταγραφής (accounting). Οι οργανισμοί μπορούν να ελέγχουν την πρόσβαση σε πόρους, να παρακολουθούν τις λειτουργίες του συστήματος και να επιβεβαιώνουν τις ταυτότητες των χρηστών μέσω της χρήσης εφαρμογών παρακολούθησης, ελέγχου ταυτότητας και εξουσιοδότησης. Εξηγώντας τους ρόλους ασφαλείας που είναι ενσωματωμένοι στο πλαίσιο AAA και αναλύοντας την ουσία κάθε αρχής της τριάδας CIA, οι ορισμοί έχουν ως εξής [10], [79], [80], [81]:

- **Εμπιστευτικότητα:** Ασχολείται με την προστασία των ιδιωτικών πληροφοριών από παράνομη πρόσβαση ή αποκάλυψη. Περιλαμβάνει μέτρα που εγγυώνται ότι οι πληροφορίες είναι προσβάσιμες μόνο σε όσους επιτρέπεται, προστατεύοντας την ιδιωτικότητα των δεδομένων και αποτρέποντας την μη εξουσιοδοτημένη αποκάλυψη. Για τους σκοπούς της προστασίας

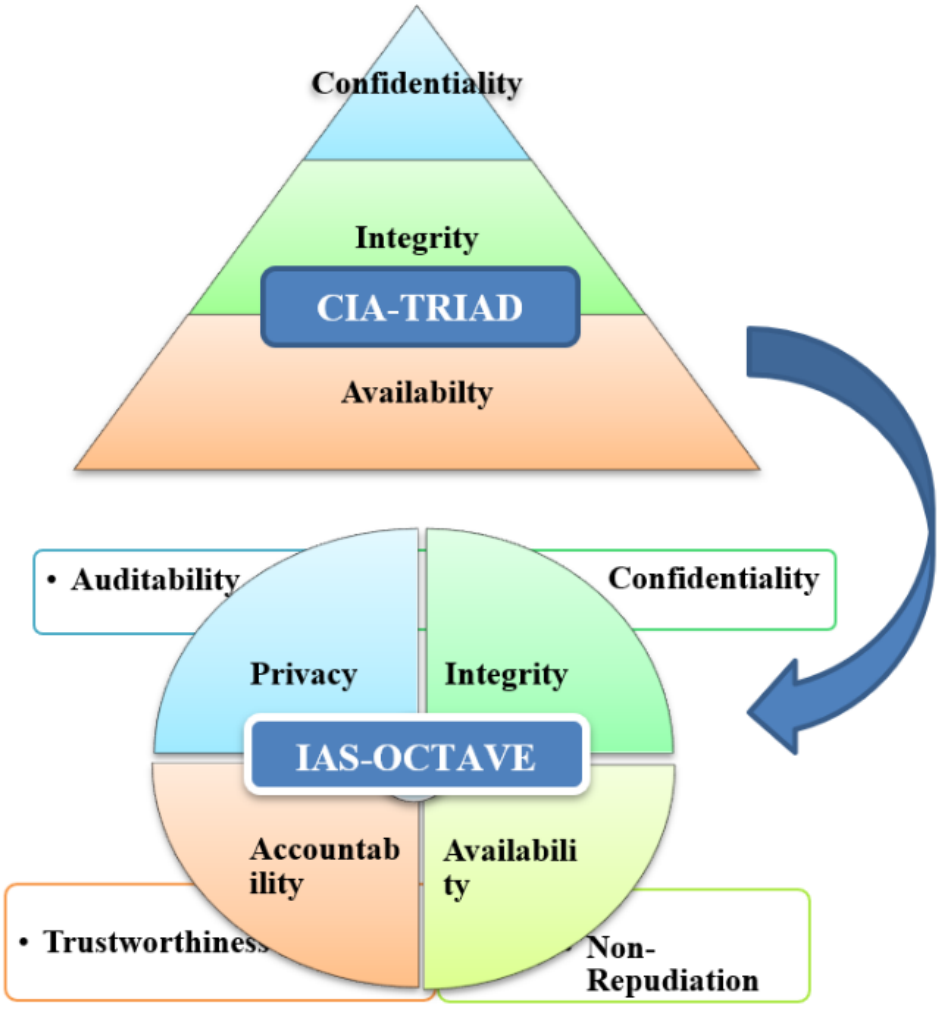
ευαίσθητων δεδομένων που μεταφέρονται μεταξύ συνδεδεμένων συσκευών στο IoT, όπως ιδιωτικές πληροφορίες υγείας σε ιατρικά συστήματα, η εμπιστευτικότητα είναι κρίσιμη.

- **Ακεραιότητα:** Αφορά την διατήρηση της αυθεντικότητας και της ορθότητας των δεδομένων καθόλη την διάρκεια της μεταφοράς προς τον τελικό προορισμό. Προκειμένου να διατηρηθεί η ακεραιότητα των δεδομένων και να διασφαλιστεί ότι παραμένουν ανέπαφα και μη αλλοιωμένα, είναι απαραίτητο να τεθούν σε εφαρμογή μηχανισμοί που μπορούν να εντοπίζουν και να σταματούν μη εξουσιοδοτημένες τροποποιήσεις. Η ακεραιότητα είναι εξαιρετικά σημαντική σε περιβάλλοντα IoT για να διασφαλιστεί η εγκυρότητα και η αξιοπιστία των δεδομένων που παράγονται από τους αισθητήρες και να σταματήσει η χειραγώγηση ή η αλλοίωση που θα μπορούσε να οδηγήσει σε εσφαλμένες αποφάσεις ή ενέργειες που βασίζονται σε ανακριβείς πληροφορίες.
- **Διαθεσιμότητα:** Προκειμένου να διασφαλιστεί ότι τα δεδομένα και οι υπηρεσίες είναι διαθέσιμα και χρησιμοποιήσιμα όταν χρειάζεται, πρέπει να εξασφαλίζεται η διαθεσιμότητα. Περιλαμβάνει την λήψη μέτρων για την αποφυγή διακοπών λειτουργίας που θα μπορούσαν να θέσουν σε κίνδυνο την διαθεσιμότητα κρίσιμων συστημάτων ή πόρων. Η διαθεσιμότητα έχει κρίσιμο ρόλο στο IoT, καθώς εγγυάται την συνεχή λειτουργία των συνδεδεμένων συσκευών και υπηρεσιών.
- **Αυθεντικοποίηση:** Έχει να κάνει με την επαλήθευση της ταυτότητας των χρηστών ή των συσκευών που ζητούν πρόσβαση σε ένα σύστημα. Οι οργανισμοί μπορούν να επιβεβαιώσουν την νομιμότητα των ατόμων ή των συσκευών που προσπαθούν να αλληλεπιδράσουν με τα συστήματα του IoT χρησιμοποιώντας μία ποικιλία μηχανισμών ελέγχου ταυτότητας, όπως κωδικούς πρόσβαση, βιομετρικά στοιχεία και έλεγχο ταυτότητας πολλαπλών παραγόντων.
- **Εξουσιοδότηση:** Η εξουσιοδότηση του συστήματος ελέγχει τα δικαιώματα και τα προνόμια που χορηγούνται στις επαληθευμένες οντότητες. Οι μηχανισμοί εξουσιοδότησης ελέγχουν τι μπορεί να γίνει και σε ποιους πόρους μπορεί να έχει πρόσβαση ένας χρήστης ή μία συσκευή αφού έχει πιστοποιηθεί. Οι οργανισμοί μπορούν να μειώσουν τον κίνδυνο μη εξουσιοδοτημένης δραστηριότητας ή παραβίασης των δεδομένων σε περιβάλλοντα IoT περιορίζοντας το εύρος της πρόσβασης που χορηγείται σε οντότητες μέσω του ορισμού πολιτικών ελέγχου πρόσβασης.
- **Καταγραφή:** Προκειμένου να τηρείται ένα πλήρες αρχείο των ενεργειών των χρηστών και της χρήσης των πόρων, καταγράφονται οι δραστηριότητες που γίνονται στα συστήματα. Μέσω της καταγραφής των συμβάντων, οι οργανισμοί μπορούν να εντοπίζουν και να διερευνούν περιστατικά ασφαλείας και να εντοπίζουν πιθανές ανωμαλίες ή μη εξουσιοδοτημένες κινήσεις.

Οι ερευνητές στον τομέα της κυβερνοασφάλειας διερευνούν εναλλακτικά πρότυπα ασφάλειας για να συμπληρώσουν τις παραδοσιακές προσεγγίσεις στην προσπάθεια τους να ενισχύσουν τα πλαίσια ασφάλειας στον κυβερνοχώρο. Οι ερευνητές [82], [83], [84] έχουν παρουσιάσει το νέο μοντέλο ασφαλείας IAS (Information Assurance and Security) Octave το οποίο υπερβαίνει τις παραδοσιακές τριάδες CIA και AAA. Οι ερευνητές υποστηρίζουν ότι η τριάδα CIA μπορεί να μην είναι σε θέση να ανταποκριθεί στις νέες προκλήσεις που προκύπτουν από τα διασυνδεδεμένα τοπία ασφάλειας. Παρόλο που το μοντέλο IAS Octave και η τριάδα CIA μοιράζονται θεμελιώδεις έννοιες για την προστασία των συστημάτων, οι στρατηγικές τους διαφέρουν. Όσον αφορά την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα, και τα δύο μοντέλα είναι συμβατά στο ότι τονίζουν πόσο σημαντικά είναι η προστασία της εμπιστευτικότητας των δεδομένων, η εγγύηση της ακεραιότητας των δεδομένων και η διατήρηση της διαθεσιμότητας του συστήματος. Ωστόσο, το μοντέλο IAS Octave προσθέτει την έννοια της λογοδοσίας (accountability), η οποία συμβαδίζει με την ιδέα της απόδοσης ευθυνών σε χρήστες για τις ενέργειες τους στο πλαίσιο της ασφάλειας, όπως ακριβώς κάνει και η καταγραφή στο μοντέλο της

τριάδας AAA. Επιπλέον, παρόλο που η εξουσιοδότηση και η αυθεντικοποίηση αποτελούν σημαντικά στοιχεία για την ανάπτυξη εμπιστοσύνης στο μοντέλο του AAA, το μοντέλο IAS Octave συνδυάζει αυτά τα χαρακτηριστικά σε μία ενιαία, πιο ολοκληρωμένη κατηγορία αξιοπιστίας (trustworthiness). Το μοντέλο IAS Octave επεκτείνει τις τριάδες CIA και AAA με την ενσωμάτωση βασικών στοιχείων όπως της μη άρνησης (non-repudiation), της ιδιωτικότητας (privacy) και της ελεγξιμότητας (auditability).

- **Μη άρνηση:** Περιγράφει την ικανότητα του συστήματος να επιβεβαιώνει ή να αρνείται την εκτέλεση μιας ενέργειας.
- **Ιδιωτικότητα:** Διασφαλίζεται η τήρηση των πολιτικών απορρήτου σε όλο το σύστημα και παρέχεται στους χρήστες η δυνατότητα ελέγχου των προσωπικών τους δεδομένων.
- **Ελεγξιμότητα:** Περιλαμβάνει την ικανότητα συνεχούς και ολοκληρωμένης παρακολούθησης όλων των δραστηριοτήτων του συστήματος.




Σχήμα 5.2: *IAS Octave* [85]

## 5.7 Επίλογος

Το κεφάλαιο τονίζει την αξία της προστασίας των περιουσιακών στοιχείων, ενώ παράλληλα προσφέρει μια κρίσιμη ανασκόπηση της κυβερνοασφάλειας στο πλαίσιο του IoT. Καλύπτει θεμελιώδεις έννοιες όπως τα περιουσιακά στοιχεία, οι ευπάθειες και οι απειλές, καθώς και τις διαφορές μεταξύ παθητικών και ενεργητικών επιθέσεων, παρέχοντας τα θεμέλια για την κατανόηση των δυσκολιών της κυβερνοασφάλειας. Επίσης παρουσιάζονται σημαντικά μοντέλα κυβερνοασφάλειας που βοηθούν τους

οργανισμούς να ενισχύσουν τα μέτρα ασφαλείας τους, όπως το IAS Octave, το AAA και το CIA. Συνοψίζοντας, το κεφάλαιο αυτό δίνει έμφαση στην κρίσιμη ισορροπία μεταξύ της προστασίας των περιουσιακών στοιχείων και του μετριασμού των απειλών, παρέχοντας μια θεμελιώδη προοπτική για τις στρατηγικές κυβερνοασφάλειας που απαιτούνται για την πλοήγηση στο περιβάλλον του IoT.

# 6. Ασφάλεια του IoT σε χαμηλά επίπεδα

## 6.1 Εισαγωγή

Το παρόν κεφάλαιο στρέφει την προσοχή του σε μια διεξοδική εξέταση του περιβάλλοντος ασφαλείας που υποστηρίζει το IoT. Το κεφάλαιο ξεκινά με την ταξινόμηση και τον εντοπισμό των ευπαθειών που υπάρχουν στα συστήματα IoT.

Στην συνέχεια, παρουσιάζονται οι διάφορες επιθέσεις που στοχεύουν τα συστήματα IoT. Αυτό το υποκεφάλαιο χωρίζεται περαιτέρω για την λεπτομερή ανάλυση των επιθέσεων ανάλογα με τα επίπεδα αρχιτεκτονικής του IoT που στοχεύουν. Αρχικά εξετάζονται οι επιθέσεις που βασίζονται στο επίπεδο αντίληψης, οι οποίες θέτουν σε κίνδυνο την ακεραιότητα και την εμπιστευτικότητα των δεδομένων που συλλέγονται από τις συσκευές IoT, θέτοντας σε κίνδυνο άμεσα τους αισθητήρες. Η ανάλυση μετατοπίζεται στις επιθέσεις που βασίζονται στο επίπεδο δικτύου, δείχνοντας πως οι επιτιθέμενοι εκμεταλλεύονται τα πρωτόκολλα επικοινωνίας για να θέσουν σε κίνδυνο τα συστήματα του IoT, να κλέψουν δεδομένα ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση.

Μια ανασκόπηση γνωστών επιθέσεων IoT ολοκληρώνει το κεφάλαιο, παρέχοντας παραδείγματα από τον πραγματικό κόσμο που δείχνουν πως οι ευπάθειες και οι τεχνικές επίθεσης μπορούν να χρησιμοποιηθούν στην πράξη.

## 6.2 Ευπάθειες στο IoT

Το IoT αποτελείται από ένα ευρύ φάσμα δικτυωμένων συστημάτων, αισθητήρων και συσκευών που βοηθούν στην επεξεργασία, την μετάδοση και την συλλογή των δεδομένων. Όμως αυτή η συνδεσιμότητα φέρνει μαζί της και ένα πλήθος ευπαθειών που ενέχουν σοβαρές απειλές για την ασφάλεια. Οι ερευνητές στα [52], [85], [86], εξέτασαν και παρουσίασαν τις παρακάτω ευπάθειες:

- **Φυσική Ασφάλεια:** Πολλές συσκευές IoT είναι επιρρεπείς σε χειραγώγηση ή αλλοίωση, επειδή δεν διαθέτουν επαρκή μέτρα ασφαλείας, όπως η προστασία θυρών USB. Επιπλέον, οι επιτιθέμενοι μπορούν να επωφεληθούν από τις φυσικές θύρες που αφήνονται ανοιχτές για συντήρηση ή διαμόρφωση των ρυθμίσεων. Αυτές οι ευπάθειες επιδεινώνονται με την χρήση προεπιλεγμένων διαπιστευτηρίων και την απλότητα των κωδικών πρόσβασης, γεγονός που θέτει σε κίνδυνο την εμπιστευτικότητα και την ακεραιότητα των δεδομένων IoT.
- **Περιττές Ανοιχτές Θύρες Δικτύου:** Οι ανοιχτές θύρες δικτύου, λειτουργούν ως σημεία εισόδου για μη εξουσιοδοτημένη πρόσβαση, καθιστώντας δυνατή την εκμετάλλευση των αδύναμων υπηρεσιών δικτύου από τους επιτιθέμενους. Οι ανοιχτές θύρες δημιουργούν μια σημαντική ευπάθεια, επιτρέποντας στους επιτιθέμενους να δημιουργήσουν συνδέσεις με σκοπό να εκμεταλλευτούν ένα ευρύ φάσμα ευπαθειών. Αυτή η προσβασιμότητα μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση και πιθανές μετατροπές των δεδομένων, θέτοντας σε κίνδυνο την συνολική ασφάλεια και ακεραιότητα του δικτύου IoT.
- **Ανεπαρκής Συλλογή Ενέργειας:** Οι συσκευές IoT είναι ευάλωτες σε επιθέσεις εξάντλησης πόρων, καθώς συχνά δεν διαθέτουν μηχανισμούς συλλογής ενέργειας. Αυτές οι επιθέσεις εκμεταλλεύονται τους περιορισμένους ενεργειακούς πόρους των συσκευών, αδειάζοντας τις μπαταρίες για να εμποδίσουν την λειτουργία τους.
- **Ανεπαρκής Έλεγχος Ταυτότητας:** Οι αδύναμες διαδικασίες ελέγχου ταυτότητας αποτελούν σοβαρό κίνδυνο για την ασφάλεια, καθώς δίνουν στους κακόβουλους χρήστες την δυνατότητα πρόσβασης σε δίκτυα και συσκευές χωρίς εξουσιοδότηση. Επειδή πολλές συσκευές IoT

χρησιμοποιούν προεπιλεγμένα ή απλά διαπιστευτήρια, είναι ευάλωτες σε επιθέσεις brute-force. Επιπλέον, ορισμένες συσκευές ενδέχεται να μην διαθέτουν έλεγχο ταυτότητας πολλαπλών παραγόντων (Multi Factor Authentication, MFA), γεγονός που θα μπορούσε να αποδυναμώσει περαιτέρω την ασφάλεια των συστημάτων ελέγχου ταυτότητας.

- **Ακατάλληλη Κρυπτογράφηση:** Η κακή διαχείριση των κλειδιών ή η χρήση ελλιπών κρυπτογραφικών αλγορίθμων μπορεί να θέσει σε κίνδυνο την ασφάλεια του IoT. Οι επιτιθέμενοι μπορούν να θέσουν σε κίνδυνο την εμπιστευτικότητα και την ακεραιότητα των επικοινωνιών χρησιμοποιώντας αδυναμίες στις υλοποιήσεις κρυπτογράφησης για να κλέψουν, να κρυφακούσουν ή να αλλοιώσουν τα ευαίσθητα δεδομένα.
- **Ακατάλληλοι Μηχανισμοί Ελέγχου:** Η ανίχνευση και η διερεύνηση περιστατικών ασφαλείας μπορεί να είναι δύσκολη όταν δεν υπάρχουν επαρκείς μηχανισμοί ελέγχου. Αυτό καθιστά πιο δύσκολο τον εντοπισμό και τον μετριασμό των πιθανών απειλών. Πολλές συσκευές IoT ενδέχεται να μην έχουν πλήρεις δυνατότητες καταγραφής ή να μην καταγράφουν σημαντικά συμβάντα ασφαλείας, γεγονός που θα περιόριζε το τι μπορεί να διαπιστωθεί σχετικά με τις λειτουργίες του συστήματος και τις αλληλεπιδράσεις των χρηστών.
- **Ανεπαρκής Μηχανισμοί Ενημερώσεων:** Η παραμέληση της διαχείρισης των ενημερώσεων, η οποία επιδεινώνεται από την έλλειψη αυτοματοποιημένων συστημάτων για την εφαρμογή διορθώσεων ασφαλείας και ενημερώσεων του λογισμικού. Λόγω αυτής της παράλειψης, οι συσκευές IoT εκτίθενται σε γνωστά κενά ασφαλείας, γεγονός που αποτελεί ευπάθεια που μπορούν να εκμεταλλευτούν οι κακόβουλοι χρήστες.

## 6.3 Επιθέσεις στο IoT

Το IoT γίνεται στόχος από κακόβουλους χρήστες που έχουν ως στόχο να εκμεταλλευτούν τις ευπάθειες που παρουσιάσαμε. Αυτό το υποκεφάλαιο διερευνά το σύνθετο πεδίο των επιθέσεων στο IoT και προσφέρει μια λεπτομερή παρουσίαση όλων των κινδύνων που αντιμετωπίζουν αυτά τα δίκτυα. Είναι σημαντικό να συνειδητοποιήσουμε ότι αυτές οι επιθέσεις είναι πραγματικές απειλές με πραγματικές επιπτώσεις στην λειτουργικότητα, την ασφάλεια και την ιδιωτικότητα και δεν είναι απλώς θεωρητικές ανησυχίες.

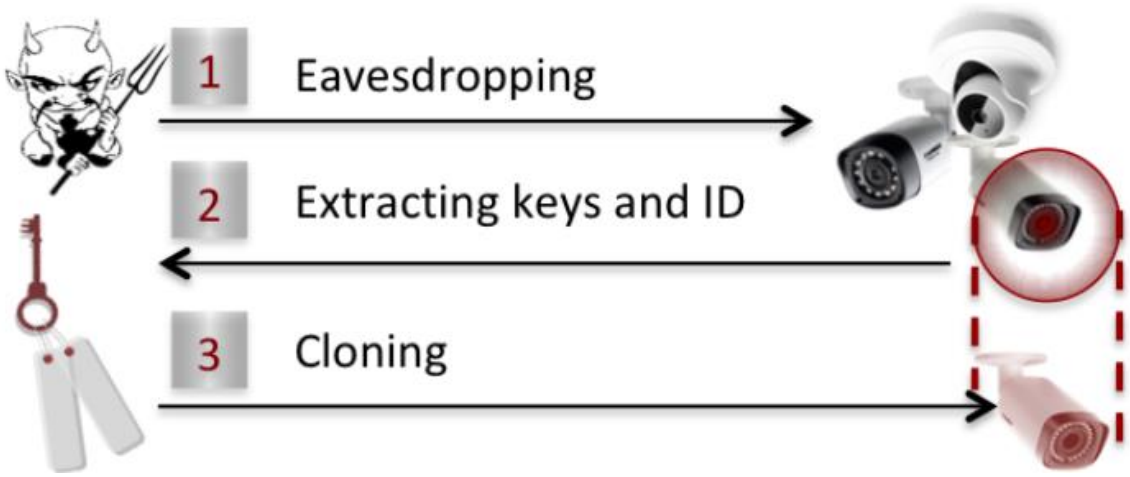
### 6.3.1 Επίπεδο Αντίληψης

Το επίπεδο αντίληψης, το οποίο διασυνδέεται απευθείας με τον φυσικό κόσμο για την συλλογή των δεδομένων, λειτουργεί ως η πρώτη γραμμή στην αρχιτεκτονική των συστημάτων IoT. Το παρόν υποκεφάλαιο μετατοπίζεται στην επικέντρωση στις συγκεκριμένες απειλές που στοχεύουν σε αυτό το κρίσιμο επίπεδο. Οι επιθέσεις του επιπέδου αντίληψης εκμεταλλεύονται τις ευπάθειες των αισθητήρων και των συσκευών συλλογής δεδομένων προκειμένου να αλλοιώσουν ή να υποκλέψουν τα μη επεξεργασμένα δεδομένα που είναι απαραίτητα για τις λειτουργίες του IoT. Η ανάλυση που ακολουθεί, αναλύει αυτές τις επιθέσεις και τονίζει το πόσο κρίσιμο είναι να υπάρχουν ισχυρά μέτρα ασφαλείας για την προστασία των βασικών στοιχείων των συστημάτων IoT.

- **Επίθεση Πλευρικού Καναλιού (Side-channel Attack):** Η διαρροή πληροφοριών από την φυσική υλοποίηση μιας συσκευής, όπως η κατανάλωση ενέργειας, οι ηλεκτρομαγνητικές εκπομπές ή οι διακυμάνσεις του χρονισμού, αξιοποιείται από επιθέσεις πλευρικού καναλιού. Οι επιτιθέμενοι μπορούν να αντλήσουν ευαίσθητες πληροφορίες, όπως κρυπτογραφικά κλειδιά ή δεδομένα, εξετάζοντας αυτά τα πλευρικά κανάλια. Για τον προσδιορισμό των μυστικών κλειδιών, οι επιθέσεις ανάλυσης ισχύος για παράδειγμα, παρακολουθούν πόση ισχύ χρησιμοποιεί μια συσκευή κατά την εκτέλεση κρυπτογραφικών λειτουργιών [85]. Με παρόμοιο

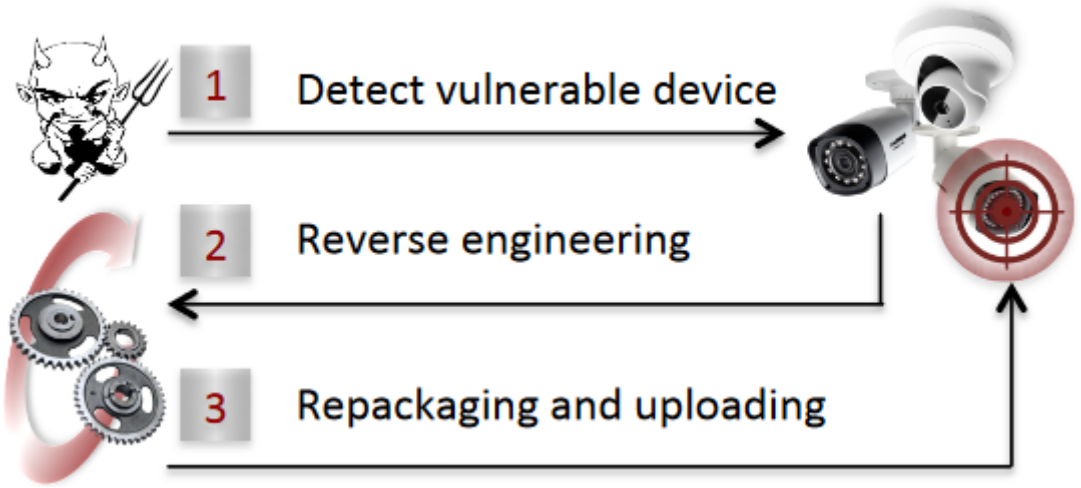
τρόπο, η ηλεκτρομαγνητική ανάλυση προσπαθεί να αποκρυπτογραφήσει τα κρυπτογραφημένα δεδομένα καταγράφοντας τα σήματα που εκπέμπονται. Τα συστήματα RFID είναι επίσης ευάλωτα σε επιθέσεις πλευρικού καναλιού, ιδίως σε εκείνες που στοχεύουν τα ηλεκτρομαγνητικά σήματα που εκπέμπονται κατά την επικοινωνία μεταξύ των RFID tags και των RFID readers [52].

- **Επίθεση Εξάντλησης Μπαταρίας (Battery Draining Attack):** Η επίθεση που είναι γνωστή ως "εξάντληση της μπαταρίας" έχει ως σκοπό την εξάντληση του ενεργειακού αποθέματος της συσκευής, εμποδίζοντας την να λειτουργήσει κανονικά ή ακόμη και να την θέσουν ολοκληρωτικά εκτός λειτουργίας. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τις ευπάθειες της συσκευής, επιταχύνοντας την εξάντληση των πόρων της μπαταρίας. Αυτές οι επιθέσεις μπορεί να είναι ιδιαίτερα επιβλαβείς σε περιπτώσεις όπου οι συσκευές IoT τοποθετούνται σε σημεία με δύσκολη πρόσβαση και λίγες πηγές ενέργειας ή όταν δεν είναι πρακτικό να αντικαθίστανται συχνά οι μπαταρίες [86], [87].
- **Επίθεση Παρεμβολής (Jamming Attack):** Η επίθεση παρεμβολής είναι ένας τύπος απειλής, όπου οι κακόβουλοι χρήστες διαταράσσουν σκόπιμα την ασύρματη επικοινωνία τροφοδοτώντας το φάσμα ραδιοσυχνοτήτων με θόρυβο ή σήματα παρεμβολής. Η επίθεση παρεμβολής μπορεί να επηρεάσει την ικανότητα μιας συσκευής IoT να στέλνει ή να λαμβάνει δεδομένα στοχεύοντας στα πρωτόκολλα ασύρματης επικοινωνίας που χρησιμοποιεί η συσκευή. Μπορεί να υπάρξουν σοβαρές επιπτώσεις από αυτή την επίθεση, όπως η απώλεια δεδομένων, η μη διαθεσιμότητα των συστημάτων και η εξάντληση των πόρων [10], [88].
- **Επίθεση Υποκλοπής (Eavesdropping Attack):** Η μη εξουσιοδοτημένη επικοινωνία μεταξύ συσκευών IoT μπορεί να κλαπεί σε επίθεση υποκλοπής, η οποία θα μπορούσε να θέσει σε κίνδυνο τις ευαίσθητες πληροφορίες. Οι επιτιθέμενοι υποκλέπτουν τα πακέτα που αποστέλλονται και λαμβάνονται μεταξύ των συσκευών χωρίς την γνώση ή την συγκατάθεση τους, παρακολουθώντας παθητικά τις ασύρματες μεταδόσεις. Ανάλογα με τον τύπο της εφαρμογής, αυτά τα υποκλαπέντα δεδομένα μπορεί να περιλαμβάνουν ευαίσθητες πληροφορίες ή διαπιστευτήρια της σύνδεσης [39], [87]. Η ασφάλεια και η ιδιωτικότητα των συστημάτων IoT τίθενται σοβαρά σε κίνδυνο από τις επιθέσεις υποκλοπής, ιδίως σε περιβάλλοντα όπου η ασύρματη επικοινωνία είναι κοινή. Για παράδειγμα, οι επιτιθέμενοι μπορούν να υποκλέψουν τα δεδομένα που ανταλλάσσονται μεταξύ συσκευών με δυνατότητα NFC, χρησιμοποιώντας κεραίες που είναι πιο ισχυρές από τις κινητές συσκευές [89].
- **Επίθεση Κατάληψης Κόμβου (Node Capture Attack):** Τα συστήματα IoT είναι ευάλωτα σε επίθεση κατάληψης κόμβου, ιδίως στους κόμβους πύλης (gateway), όπου συγκεντρώνονται σημαντικές λειτουργίες του δικτύου. Οι επιτιθέμενοι παίρνουν τον φυσικό έλεγχο των κομβών πύλης εκμεταλλευόμενοι τις ευπάθειες, γεγονός που τους επιτρέπει την πρόσβαση σε ιδιωτικά δεδομένα, όπως πρωτόκολλα επικοινωνίας και κλειδιά κρυπτογράφησης [88]. Η ακεραιότητα και η εμπιστευτικότητα των δεδομένων που μεταδίδονται στο δίκτυο απειλούνται από αυτή την επίθεση, η οποία μπορεί να καταστήσει δυνατή την υποκλοπή και την τροποποίηση των επικοινωνιών μεταξύ των κόμβων από τους επιτιθέμενους. Επιπλέον, οι παραβιασμένοι κόμβοι πύλης μπορεί να χρησιμοποιηθούν ως σημεία εισόδου για πρόσθετη εκμετάλλευση, δίνοντας στους κακόβουλους χρήστες πρόσβαση για να διεισδύσουν και να θέσουν σε κίνδυνο το περιβάλλον του IoT στο σύνολο του [3]. Όπως φαίνεται στο Σχήμα 6.1, η επίθεση πραγματοποιείται με τον επιτιθέμενο να υποκλέπτει τα ευαίσθητα δεδομένα της πραγματικής συσκευής και με βάση αυτά τα δεδομένα, κλωνοποιεί έναν καινούργιο κακόβουλο κόμβο.




Σχήμα 6.1: *Φάσεις επίθεσης κατάληψης κόμβου* [86]

- **Επίθεση Εισαγωγής Ψεύτικων Κόμβων και Κακόβουλων Δεδομένων (Fake Node and Malicious Data Injection Attack):** Αυτή η επίθεση περιλαμβάνει την εισαγωγή κακόβουλων πακέτων δεδομένων στην ροή επικοινωνίας και την προσθήκη μη εξουσιοδοτημένων ή πλαστών συσκευών σε ένα δίκτυο IoT. Μέσω της χρήσης παραπλανητικών συσκευών που μιμούνται αυθεντικούς κόμβους, οι επιτιθέμενοι είναι σε θέση να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση και ενδεχομένως να προκαλέσουν βλάβη στις λειτουργίες του συστήματος. Οι επιτιθέμενοι μπορούν να αλλάξουν την συμπεριφορά του συστήματος, να θέσουν σε κίνδυνο την ακεραιότητα των δεδομένων και να εξαπατήσουν τους χρήστες ή τις συνδεδεμένες συσκευές εισάγοντας κακόβουλα πακέτα [39]. Επιπλέον, είναι δυνατόν να εισαχθεί κακόβουλος κώδικας στις συσκευές, υποβαθμίζοντας την λειτουργικότητα τους. Η εισαγωγή ψευδών δεδομένων μπορούν να ξεγελάσουν τις συσκευές διαδίδοντας λανθασμένα αποτελέσματα, τροποποιώντας το λογισμικό ή χειραγωγώντας τις ενδείξεις των αισθητήρων [87].




Σχήμα 6.2: *Φάσεις τροποποίησης του λογισμικού* [86]

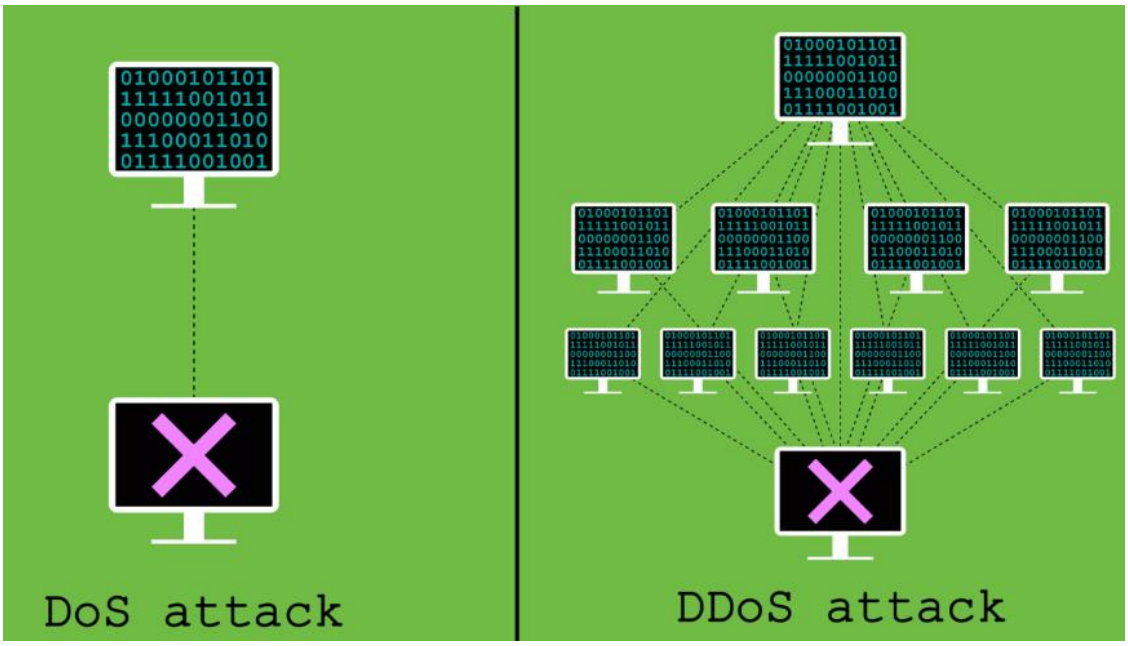
- **Επίθεση Αναπαραγωγής (Replay Attack):** Στην επίθεση αναπαραγωγής, έγκυρες μεταδόσεις δεδομένων μεταξύ των συσκευών υποκλέπτονται και επαναμεταδίδονται με κακόβουλο τρόπο σε μεταγενέστερο χρόνο. Οι επιτιθέμενοι ξανά στέλνουν τα πακέτα που έχουν αποσταλεί προηγουμένως στον προοριζόμενο παραλήπτη, με σκοπό να αποκτήσουν μη εξουσιοδοτημένη

πρόσβαση ή να πραγματοποιήσουν μη εξουσιοδοτημένες λειτουργίες [39]. Η επίθεση αναπαραγωγής μπορεί να οδηγήσει σε διάφορους κινδύνους ασφαλείας, όπως παράνομη πρόσβαση σε έξυπνες συσκευές, χειραγώγηση των δεδομένων από αισθητήρες ή διακοπή των υπηρεσιών. Σε ένα περιβάλλον έξυπνου σπιτιού για παράδειγμα, θα ήταν δυνατό για έναν επιτιθέμενο να καταγράψει και να αναπαράγει μία εντολή για το ξεκλείδωμα μιας πόρτας, επιτρέποντας του να εισέλθει στο κτίριο χωρίς εξουσιοδότηση. Επίσης αυτή η επίθεση έχει την δυνατότητα να χειραγωγήσει τις ενδείξεις αισθητήρων, οδηγώντας σε δυσμενή αποτελέσματα.

### 6.3.2 Επίπεδο Δικτύου

Τα δεδομένα μεταβαίνουν από το επίπεδο αντίληψης στο επίπεδο δικτύου, το οποίο είναι ένα κρίσιμο σημείο στην αρχιτεκτονική του IoT, όπου η ασφάλεια των δεδομένων αποκτά ιδιαίτερη σημασία. Η ανάλυση επικεντρώνεται στις συγκεκριμένες επιθέσεις που στοχεύουν αυτό το επίπεδο, καθεμία από τις οποίες χρησιμοποιεί μια διαφορετική στρατηγική για να εκμεταλλευτεί τις αδυναμίες του.

- **Επίθεση DoS/DDoS:** Κατακλύζοντας την συσκευή με υπερβολική ποσότητα μη εξουσιοδοτημένης κυκλοφορίας, οι επιθέσεις DoS και DDoS αποσκοπούν στην κακόβουλη παρεμπόδιση της διαθεσιμότητας των υπηρεσιών IoT. Συνήθως, μία μοναδική πηγή χρησιμοποιείται σε μία επίθεση DoS για να γεμίσει τον στόχο με κίνηση και να εμποδίσει την πρόσβαση εξουσιοδοτημένων χρηστών σε αυτόν. Μπορούν επίσης να έχουν μακροπρόθεσμες επιπτώσεις, επειδή αναγκάζουν τις συσκευές IoT να λειτουργούν συνεχώς, γεγονός που μειώνει την διάρκεια ζωής της μπαταρίας. Η επίθεση DDoS από την άλλη πλευρά, χρησιμοποιεί έναν μεγάλο αριθμό πηγών που συνήθως είναι παραβιασμένες συσκευές οι οποίες συντονίζονται για να πραγματοποιήσουν μία συγχρονισμένη επίθεση στον στόχο [10], [86].

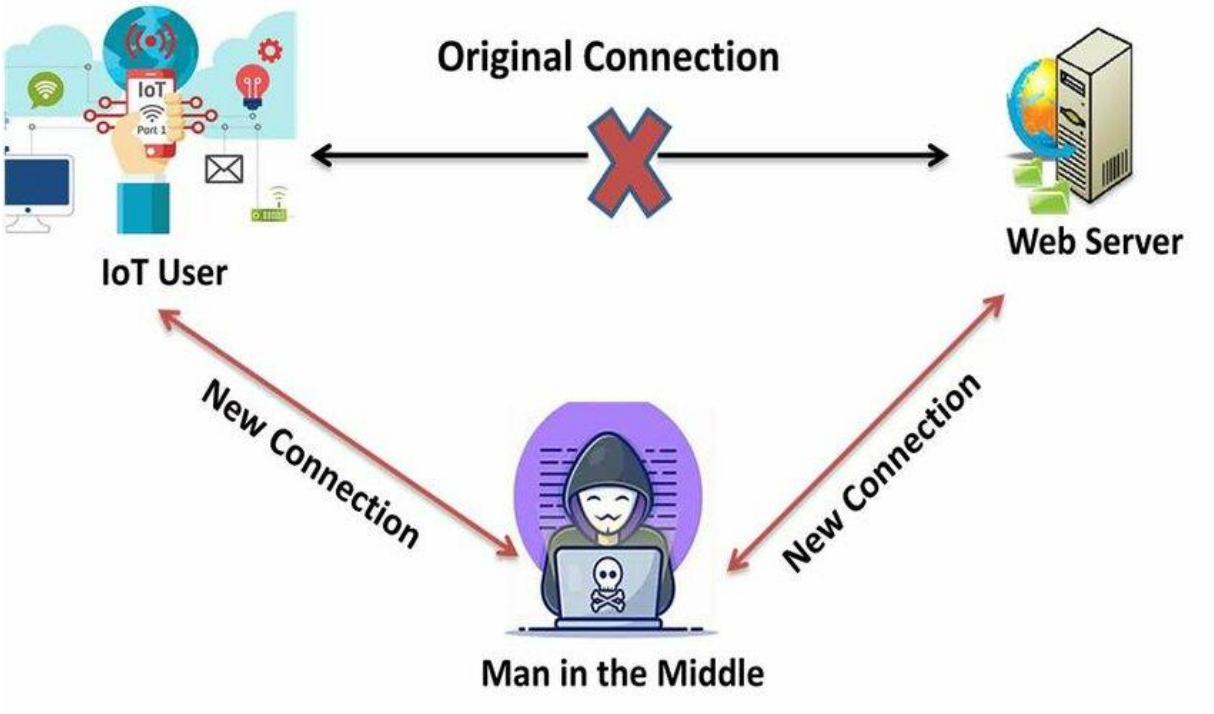



Σχήμα 6.3: *Απεικόνιση επιθέσεων DoS και DDoS* [90]

- **Επίθεση Man-in-the-Middle (MitM):** Στην επίθεση MitM, ο επιτιθέμενος τοποθετείται με τρόπο που του επιτρέπει να υποκλέψει κρυφά και ενδεχομένως να αλλάξει τα δεδομένα που μεταδίδονται μεταξύ δύο συσκευών IoT. Χωρίς την γνώση και την συγκατάθεση των συσκευών, αυτή η μη εξουσιοδοτημένη πρόσβαση επιτρέπει στον επιτιθέμενο να εισάγει

κακόβουλα δεδομένα ή να τροποποιήσει την επικοινωνία σε πραγματικό χρόνο [39]. Οι ερευνητές στο [78], έχουν περιγράψει τις πιο διαδεδομένες παραλλαγές επιθέσεων MitM, καθεμία από τις οποίες παρουσιάζει τις τακτικές που χρησιμοποιεί ο επιτιθέμενος για να βλάψει την ασφάλεια του IoT.

- **ARP Spoofing:** Το ARP spoofing συμβαίνει όταν ένας επιτιθέμενος στέλνει πλαστά μηνύματα ARP σε ένα δίκτυο. Συνδέοντας την διεύθυνση IP μιας αξιόπιστης συσκευής στο δίκτυο με την διεύθυνση MAC (Media Access Control) του επιτιθέμενου, αυτό το τέχνασμα τροποποιεί την επικοινωνία ARP. Με αυτόν τον τρόπο, ο επιτιθέμενος μπορεί να κατευθύνει την κυκλοφορία που προοριζόταν για την εν λόγω εξουσιοδοτημένη συσκευή στην δική του συσκευή.
- **DNS (Domain Name System) Spoofing:** Το DNS spoofing συνεπάγεται στην τροποποίηση των απαντήσεων DNS προκειμένου να ανακατευθήνει την κυκλοφορία από αξιόπιστους servers σε κακόβουλους. Ο επιτιθέμενος έχει την δυνατότητα να τροποποιεί τις εγγραφές DNS και να εξαπατά τις συσκευές ώστε να επικοινωνούν με ψεύτικους ιστότοπους, εκμεταλλεύοντας τις αδυναμίες του πρωτοκόλλου DNS.
- **Session Hijacking:** Το Session Hijacking είναι μια ιδιαίτερα ύπουλη απειλή, κατά την οποία ο επιτιθέμενος προσπαθεί να κλέψει μια τρέχουσα επικοινωνία μεταξύ δύο συσκευών. Ο επιτιθέμενος εισέρχεται στην συνομιλία απαρατήρητος και κλέβει το αναγνωριστικό της συνεδρίας, το οποίο χρησιμεύει ως μοναδική ταυτοποίηση για κάθε ανταλλαγή. Χρησιμοποιώντας αυτή την τακτική, μπορεί να προσποιηθεί ότι είναι η πραγματική συσκευή και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα.




Σχήμα 6.4: *Επίθεση MitM* [91]

- **Επίθεση Δρομολόγησης (Routing Attack):** Οι επιθέσεις δρομολόγησης, οι οποίες στοχεύουν στους μηχανισμούς που είναι υπεύθυνοι για την καθοδήγηση της κυκλοφορίας των δεδομένων μεταξύ των κόμβων, αποτελούν σοβαρές απειλές για την αποτελεσματικότητα των δικτύων IoT. Η ικανότητα του δικτύου να παραδίδει τα δεδομένα με ασφάλεια τίθεται σε κίνδυνο από αυτές

τις επιθέσεις, οι οποίες εκμεταλλεύονται τις ευπάθειες στα πρωτόκολλα και στους αλγορίθμους δρομολόγησης. Οι επιτιθέμενοι μπορούν να παρεμποδίσουν την επικοινωνία, να αναδρομολογήσουν την κυκλοφορία ή ακόμη και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, αλλοιώνοντας τα μονοπάτια δρομολόγησης [87]. Παρακάτω εξετάζονται οι διάφοροι τύποι επιθέσεων δρομολόγησης που είναι συνηθισμένοι σε περιβάλλοντα του IoT.

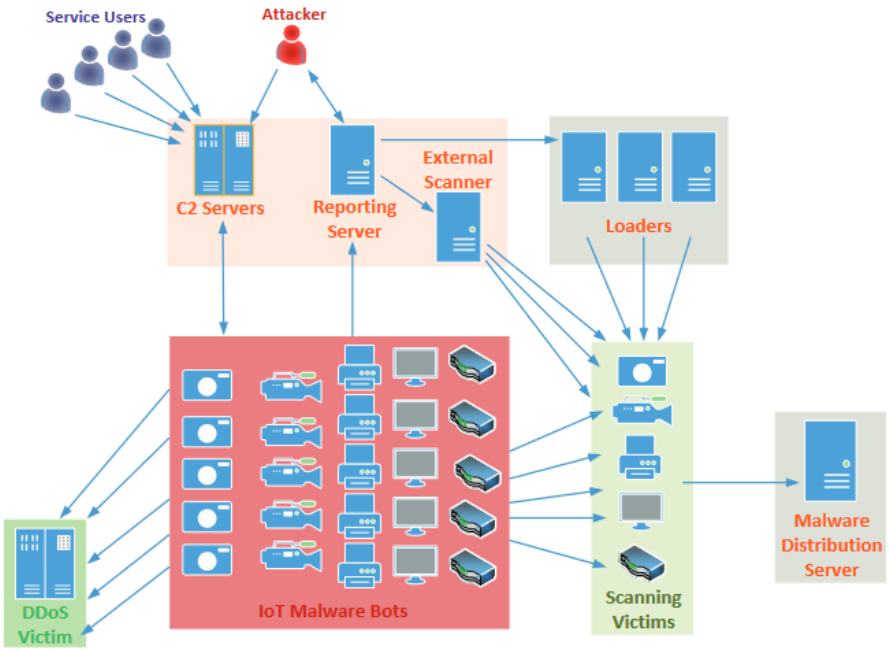
- **Επίθεση Μαύρης Τρύπας (Blackhole Attack):** Ένας παραβιασμένος κόμβος δικτύου, επίσης γνωστός ως κόμβος μαύρης τρύπας, μπορεί να απορρίπτει όλα τα πακέτα δεδομένων που διέρχονται από αυτόν [7]. Υποκλέπτοντας τα πακέτα των νόμιμων κόμβων και εμποδίζοντας τα να φτάσουν στον προορισμό τους, η επίθεση αυτή έχει ως στόχο να παρεμποδίσει την ικανότητα επικοινωνίας των νόμιμων κόμβων. Αφού προσελκύσει την κυκλοφορία, είτε τα χειραγωγεί είτε τα απορρίπτει. Προβάλλοντας τον εαυτό του ως έχοντας την ταχύτερη και καλύτερη διαδρομή προς τον προορισμό, ο κόμβος blackhole συνήθως προσελκύει την κυκλοφορία στον εαυτό του, με σκοπό να τα χειραγωγήσει ή να τα απορρίψει [82].
- **Επίθεση Καταβόθρας (Sinkhole Attack):** Η επίθεση καταβόθρας είναι μια εξελιγμένη απειλή, στην οποία εμφανίζεται όταν ένας επιτιθέμενος τροποποιεί τις πληροφορίες δρομολόγησης για να κατευθύνει την κυκλοφορία σε ένα κακόβουλο κόμβο. Προκειμένου να ξεγελάσει τους νόμιμους κόμβους ώστε να ανακατευθύνουν τα πακέτα μέσω αυτού, αυτός ο κακόβουλος κόμβος διαφημίζει πλασματικές διαδρομές δρομολόγησης. Ο επιτιθέμενος ελπίζει να προσελκύσει ένα σημαντικό ποσό κίνησης στο δίκτυο εξαπατώντας τις συσκευές, κάνοντας τες να πιστέψουν ότι υπάρχουν καλύτερες διαδρομές. Αυτό θα του δώσει την δυνατότητα να υποκλέψει και να τροποποιήσει τα πακέτα δεδομένων που θα ακολουθήσουν αυτές τις διαδρομές [83], [86].
- **Επίθεση Σκουληκότρυπας (Wormhole Attack):** Σε μία επίθεση σκουληκότρυπας, κακόβουλοι κόμβοι συνεργάζονται για να δημιουργήσουν μία εικονική σήραγγα που τους επιτρέπει να προωθούν τα πακέτα με υψηλές ταχύτητες μεταξύ τους [78].
- **Επίθεση Επιλεκτικής Προώθησης (Selective Forwarding Attack):** Η επιλεκτική προώθηση, που μερικές φορές αναφέρεται ως "επίθεση γκρίζας τρύπας (grayhole attack)", είναι επίθεση κατά την οποία ένας κακόβουλος κόμβος επιλέγει ποια πακέτα θα προωθήσει ή θα απορρίψει με βάση την προέλευση ή το περιεχόμενο τους [78]. Η επιλεκτική προώθηση περιλαμβάνει έναν κόμβο που επιλέγει στρατηγικά ποια εισερχόμενα πακέτα θα προωθήσει και ποια θα απορρίψει, σε αντίθεση με τις επιθέσεις blackhole ή sinkhole, όπου οι κόμβοι είτε απορρίπτουν είτε ανακατευθύνουν όλα τα εισερχόμενα πακέτα [7].
- **Επίθεση Sybil:** Ένας κακόβουλος κόμβος θέτει σε κίνδυνο το δίκτυο σε μία επίθεση Sybil χρησιμοποιώντας πολλές ψεύτικες ταυτότητες στον ίδιο φυσικό κόμβο. Αυτός ο κόμβος παριστάνεται ως αξιόπιστος, δίνοντας στον επιτιθέμενο την δυνατότητα να τροποποιήσει τους κανόνες δρομολόγησης [83].
- **Εκμετάλλευση RPL:** Το πρωτόκολλο RPL το οποίο έχει αναλυθεί στο κεφάλαιο 3, είναι ευάλωτο σε διάφορες επιθέσεις λόγω των ευπαθειών του [92]. Οι επιθέσεις που στοχεύουν στη δομή του DODAG, ένα κρίσιμο μέρος του RPL, είναι μεταξύ αυτών των ευπαθειών. Ο βαθμός (rank) DODAG είναι ο στόχος ενός τύπου επίθεσης, κατά την οποία ο επιτιθέμενος χειρίζεται την θέση του στο ιεραρχικό δέντρο για να προσελκύσει μεγάλο αριθμό κόμβων-παιδιών και να κατευθύνει την κυκλοφορία μέσω αυτού. Ένα διαφορετικό είδος επίθεσης είναι όταν δημοσιεύεται ένας υψηλότερος

αριθμός έκδοσης για το δέντρο DODAG, οδηγώντας τους κόμβους να δημιουργήσουν μία νέα δομή DODAG με βάση τα λανθασμένα δεδομένα. Τέλος, οι επιτιθέμενοι μπορούν επίσης να χρησιμοποιούν πλασματικές διευθύνσεις IP στα μηνύματα DIS (DODAG Information Solicitation), γεγονός που αναγκάζει τους κόμβους να παράγουν μηνύματα DIO (DODAG Information Object), με αποτέλεσμα να επιβαρυνθεί το δίκτυο [7].

- **Εκμετάλλευση 6LoWPAN:** Λόγω της έλλειψης ισχυρών μέτρων ασφαλείας, το πρωτόκολλο 6LoWPAN είναι ευάλωτο σε επιθέσεις. Η έλλειψη ελέγχου ταυτότητας εισάγει μία σοβαρή ευπάθεια που εκμεταλλεύεται από την επίθεση κατακερματισμού (fragmentation attack). Στέλνοντας κατακερματισμένα πακέτα με πλαστογραφημένες κεφαλίδες και ελέγχοντας την διαδικασία επανασυναρμολόγησης, ο επιτιθέμενος μπορεί να εκμεταλλευτεί αυτή την ευπάθεια για να παρεμποδίσει την επικοινωνία [7], [93].

## 6.4 Ιστορικά γνωστές επιθέσεις στο IoT

Οι συνέπειες των ευπαθειών του IoT σε αυτή την συνδεδεμένη εποχή υπερβαίνουν κατά πολύ τις παραβιάσεις των δεδομένων και ενέχουν πραγματικούς κινδύνους για τον πραγματικό κόσμο, που κυμαίνονται από την απειλή της ασφάλειας των ευφυών συστημάτων μεταφορών έως την διακοπή ζωτικών υπηρεσιών όπως η παροχή ηλεκτρικής ενέργειας και νερού. Τα προηγούμενα περιστατικά επιθέσεων στο IoT δεν χρησιμεύουν μόνο ως προειδοποιητικές ιστορίες, αλλά παρέχουν επίσης ισχυρή απόδειξη των πραγματικών συνεπειών που προκύπτουν όταν παραμελείται η ασφάλεια του IoT. Ένα παράδειγμα του τρόπου με τον οποίο οι κακόβουλοι εκμεταλλεύονται τις ευπάθειες σε μεγάλη κλίμακα είναι τα botnets, τα οποία είναι δίκτυα μολυσμένων συσκευών υπό τον έλεγχο επιτιθέμενων που πραγματοποιούν συντονισμένες επιθέσεις. Αυτές οι καταγεγραμμένες επιθέσεις αποκαλύπτουν τις πολύπλοκες στρατηγικές και τις ποικίλες προσεγγίσεις που χρησιμοποιούν οι επιτιθέμενοι, έτσι ώστε να κατανοηθούν οι στρατηγικές και να δημιουργηθούν ασφαλέστεροι μηχανισμοί.




Σχήμα 6.5: *Γενική δομή ενός IoT botnet* [94]

Παρακάτω παρουσιάζονται οι γνωστές επιθέσεις, ταξινομημένες με βάση τον αριθμό των παραβιασμένων συσκευών που χρησιμοποιήθηκαν για να έρθει εις πέρας η κάθε επίθεση:

- **Yandex:** Το μέγεθος και η πολυπλοκότητα της επίθεσης DDoS της Yandex, η οποία σημειώθηκε στις 5 Σεπτεμβρίου 2021 και συνδέεται με το botnet Meris, την καθιστούν την μεγαλύτερη επίθεση στην ιστορία. Χρησιμοποιώντας την μέθοδο HTTP (Hypertext Transfer Protocol) pipelining, το botnet μπόρεσε να χρησιμοποιήσει περίπου 250.000 παραβιασμένες συσκευές IoT για να κατακλύσει τους servers της Yandex με 21.8 εκατομμύρια αιτήματα ανά δευτερόλεπτο. Με την χρήση αυτής της τεχνικής, οι επιτιθέμενοι κατάφεραν να πλημμυρίσουν τους servers με ένα τεράστιο όγκο κίνησης, κάνοντας πολλαπλά αιτήματα χωρίς να χρειάζεται να περιμένουν απάντηση [95].
- **OVH:** Στις 22 Σεπτεμβρίου 2016, η OVH, μια γνωστή γαλλική εταιρεία cloud, έγινε στόχος πολλαπλών DDoS επιθέσεων. Οι επιτιθέμενοι πραγματοποίησαν την δεύτερη μεγαλύτερη επίθεση DDoS που έχει καταγραφεί, χρησιμοποιώντας ένα botnet που αποτελούνταν από περίπου 145.607 παραβιασμένες συσκευές IoT, όπως κάμερες IP και DVR. Δύο κύρια κακόβουλα λογισμικά που ήταν υπεύθυνα για τις μολυσμένες συσκευές ήταν το Bashlite και το Mirai. Η κίνηση που δημιουργήθηκε από την επίθεση, κυμάνθηκε από 1.1 Tbps έως 1.5 Tbps και η κάθε συσκευή έστειλε όγκο κίνησης από 1 Mbps έως 30 Mbps. Τα πακέτα που συνδυάστηκαν ήταν TCP/ACK, TCP/Ack+PSH και TCP/SYN [94].
- **Dyn:** Ένα σημαντικό γεγονός συνέβη το 2016, όταν μια επίθεση DDoS είχε ως στόχο την Dyn, μία εταιρεία που προσφέρει υπηρεσίες DNS. Η επίθεση αυτή ήταν αξιοσημείωτη τόσο για το εύρος της όσο και για τον τρόπο λειτουργίας της. Περίπου 100.000 συσκευές IoT με δυνατότητα σύνδεση στο διαδίκτυο, όπως εκτυπωτές, κάμερες IP και οθόνες παρακολούθησης βρεφών, μολύνθηκαν από τους επιτιθέμενους. Χρησιμοποιώντας την θύρα δικτύου 53, η οποία χρησιμοποιείται για την κυκλοφορία DNS, οι συσκευές αυτές χρησιμοποιήθηκαν για να την πλημμυρίσουν με πακέτα TCP και UDP. Στόχος αυτής της πλημμύρας ήταν να υπερφορτωθούν οι servers της Dyn, ώστε η υπηρεσία DNS να μην λειτουργεί σωστά. Επίσης η επίθεση σχεδιάστηκε για να παράγει αναδρομική (recursive) κυκλοφορία DNS, έτσι ώστε να αναγκάσει τους DNS servers να ξανά προσπαθήσουν αυτόματα να επιλύσουν τα ερωτήματα DNS εάν οι αρχικές προσπάθειες πρόσβασης αποτύγχαναν [94], [96].
- **KrebsOnSecurity.com:** Στα τέλη Σεπτεμβρίου του 2016, μία πολύ μεγάλη επίθεση DDoS έριξε τον ιστότοπο KrebsOnSecurity.com του δημοσιογράφου για θέματα κυβερνοασφάλειας Brian Krebs. Αυτή η επίθεση ήταν ξεχωριστή, καθώς εκτός από το τεράστιο μέγεθος της, πραγματοποιήθηκε με την χρήση μιας συγκεκριμένης μεθοδολογίας. Με την βοήθεια 24.000 συσκευών IoT που είχαν μολυνθεί με το κακόβουλο λογισμικό Bashlite και Mirai, εκτελέστηκε η επίθεση, με αποτέλεσμα ο μέγιστος όγκος της επίθεσης να είναι εντυπωσιακός, 623 Gbps. Οι ψηφιακές συσκευές εγγραφής βίντεο (DVR) και οι κάμερες IP που ήταν συνδεδεμένες στο διαδίκτυο ήταν οι κύριες κακόβουλες συσκευές αυτής της κυβερνοεπίθεσης. Αυτές οι συσκευές παραβιάστηκαν, μολύνθηκαν και στην συνέχεια χρησιμοποιήθηκαν για την δημιουργία ενός botnet, το οποίο χρησιμοποιήθηκε για την έναρξη της επίθεσης DDoS. Χρησιμοποιώντας έγκυρες συνδέσεις μεταξύ των παραβιασμένων συσκευών και του στόχου, η κίνηση αποτελούταν κυρίως από κίνηση GRE, SYN flooding, αιτήσεις GET και αιτήσεις POST [94].
- **Liberia:** Με στόχο το υποθαλάσσιο καλώδιο διαδικτύου της Λιβερίας στις αρχές Νοεμβρίου 2016, σημειώθηκε μια DDoS επίθεση, η οποία πιστεύεται ότι εκτελέστηκε μέσω του Mirai botnet. Ανησυχίες εκφράστηκαν σχετικά με την ικανότητα αυτής της επίθεσης να καταστρέψει

την συνδεσιμότητα του δικτύου της χώρας, καθώς ένας ερευνητής ισχυρίστηκε ότι η επίθεση είχε μέγεθος 500 Gbps [94].

- **Lappeenranta, Φινλανδία:** Η φινλανδική πόλη Lappeenranta δέχθηκε επίθεση τον χειμώνα του 2016, η οποία είχε ως στόχο τα συστήματα ζεστού νερού και θέρμανσης. Στην επίθεση εκτιμάται ότι χρησιμοποιήθηκε το Mirai botnet [94].
- **Πυρηνικό πρόγραμμα του Ιράν:** Μία από τις πιο προηγμένες επιθέσεις, το σκουλήκι Stuxnet στόχευσε το πυρηνικό πρόγραμμα του Ιράν τον Ιούνιο του 2010. Σχεδιάστηκε για να επιτεθεί σε προγραμματιζόμενους λογικούς ελεγκτές (Programmable Logic Controller, PLC), οι οποίοι χρησιμοποιούνται σε υποδομές και βιομηχανικά συστήματα. Τα PLC αυτοματοποιούσαν τις λειτουργίες των μηχανών και ήταν απαραίτητα για την διαχείριση των φυγοκεντρωτών ουρανίου στο πυρηνικό πρόγραμμα του Ιράν [97].

## 6.5 Σύνολα Δεδομένων

Στον τομέα της ασφάλειας στον κυβερνοχώρο, τα datasets είναι απαραίτητα, ιδίως όταν πρόκειται για την εκπαίδευση μοντέλων ML και DL που έχουν σχεδιαστεί ειδικά για την ασφάλεια του IoT. Παρακάτω, εξετάζονται διάφορα σημαντικά datasets που είναι χρήσιμα για την δημιουργία και την βελτίωση των αλγορίθμων που προορίζονται για τον εντοπισμό, την πρόβλεψη και την αντίδραση σε απειλές. Κάθε dataset προσφέρει πληθώρα πληροφοριών που βοηθούν στην προσομοίωση πραγματικών καταστάσεων, ανεξάρτητα από το αν επικεντρώνεται στην κυκλοφορία του δικτύου, στην συμπεριφορά των botnet ή σε άλλα συγκεκριμένα περιστατικά ασφαλείας.

- **UNSW-NB15:** Το dataset UNSW-NB15 αποτελεί πολύτιμο υλικό για την έρευνα στον τομέα της ανίχνευσης κακόβουλων σε δίκτυα. Περιέχει 2.540.044 εγγραφές, συμπεριλαμβανομένων 2.218.761 περιπτώσεων κανονικής κυκλοφορίας και 321.283 περιπτώσεων κακόβουλης κυκλοφορίας. Αυτό το σύνολο δεδομένων αντιπροσωπεύει εννέα μεγάλες οικογένειες επιθέσεων, παρέχοντας ένα εκτεταμένο και ρεαλιστικό περιβάλλον δοκιμών για τα IDS. Περιλαμβάνει ένα ολοκληρωμένο σύνολο 49 χαρακτηριστικών που καταγράφουν τόσο τα βασικά στατιστικά στοιχεία όσο και πιο σύνθετα χαρακτηριστικά, τα οποία είναι κρίσιμα για την ανάλυση και την κατανόηση της συμπεριφοράς του δικτύου [98].
- **BoT-IoT:** Το dataset BoT-IoT είναι ένα βασικό εργαλείο προσαρμοσμένο για την ανάλυση της ασφάλειας του IoT. Με πάνω από 73 εκατομμύρια εγγραφές, 9.543 κανονικές και 73.360.900 περιπτώσεις κακόβουλης κίνησης, προσομοιώνει ολοκληρωμένα περιβάλλοντα IoT. Με 45 μοναδικά χαρακτηριστικά ανά εγγραφή, αυτό το dataset είναι ειδικά φτιαγμένο για να μιμείται τα ζητήματα ασφαλείας του IoT στον πραγματικό κόσμο, περιλαμβάνοντας επιθέσεις όπως DDoS, DoS και botnet. Είναι ιδανικό για την δημιουργία και την δοκιμή προηγμένων λύσεων ασφαλείας, όπως μοντέλα μηχανικής και βαθιάς μάθησης, τα οποία εξαρτώνται από μεγάλα και ποικίλα datasets προκειμένου να εντοπίζουν και να αντιμετωπίζουν με ακρίβεια τις πιθανές απειλές [99].
- **NSL-KDD:** Το dataset NSL-KDD είναι μια βελτιωμένη έκδοση του dataset KDD'99, ειδικά σχεδιασμένο για να βελτιώσει την εκπαίδευση και την δοκιμή των IDS. Περιέχει 125.973 εγγραφές εκπαίδευσης και 22.554 εγγραφές δοκιμής, επιτρέποντας την αποτελεσματική αξιολόγηση των μοντέλων χωρίς να απαιτούνται υπερβολικοί υπολογιστικοί πόροι. Το dataset περιέχει 41 χαρακτηριστικά που αντιπροσωπεύουν ένα ευρύ φάσμα δεδομένων. Είναι σημαντικό ότι το NSL-KDD περιλαμβάνει ένα ισορροπημένο μείγμα κανονικής κυκλοφορίας και στοχευμένων επιθέσεων στον κυβερνοχώρο, όπως DoS, R2L (Remote to Local Attack), Probe και U2R (User to Root Attack), παρέχοντας ένα ρεαλιστικό σενάριο για τα IDS [100].

- **N-BaIoT:** Το dataset N-BaIoT έχει σχεδιαστεί ειδικά για την βελτίωση των συστημάτων ασφαλείας IoT έναντι επιθέσεων botnet. Αυτό το πλούσιο σε πόρους dataset περιέχει δεδομένα από ένα ευρύ φάσμα συσκευών IoT, όπως κάμερες ασφαλείας, θερμοστάτες και οθόνες παρακολούθησης βρέφων, οι οποίες έχουν μολυνθεί με διάφορα κακόβουλα λογισμικά, συμπεριλαμβανομένων γνωστών όπως το Mirai και το Bashlite. Διαθέτει μια μεγάλη συλλογή από 115 διαφορετικά χαρακτηριστικά, καταγράφοντας ένα ευρύ φάσμα δεδομένων που παρέχουν πληροφορίες σχετικά με την συμπεριφορά των μολυσμένων συσκευών. Το dataset περιέχει μεγάλο όγκο δεδομένων, συμπεριλαμβανομένων 6.506.674 κακόβουλα και 555.932 μη κακόβουλα δεδομένα [101].
- **IoT-23:** Το dataset IoT-23 περιέχει μια λεπτομερή συλλογή δεδομένων κίνησης δικτύου που έχει σχεδιαστεί ειδικά για την ανάλυση των απειλών ασφαλείας του IoT. Κατηγοριοποιεί είκοσι κακόβουλες και τρεις μη κακόβουλες συσκευές, παρέχοντας μια λεπτομερή κατανόηση των προκλήσεων ασφαλείας. Περιλαμβάνει μεγάλο όγκο δεδομένων που συλλέχθηκαν από το 2018 έως το 2020, με 30.858.735 μη κακόβουλα δεδομένα και 294.449.255 κακόβουλα δεδομένα, αποδεικνύοντας την επικράτηση των απειλών στον κυβερνοχώρο σε περιβάλλοντα IoT. Το κάθε δεδομένο συνοδεύεται με 6 χαρακτηριστικά [102].
- **Edge-IIoT:** Το dataset Edge-IIoT είναι ειδικά σχεδιασμένο για την διερεύνηση των ζητημάτων κυβερνοασφάλειας σε περιβάλλοντα που αφορούν το βιομηχανικό IoT. Περιλαμβάνει πληροφορίες που συλλέχθηκαν από 15 διαφορετικές συσκευές, παράγοντας ένα dataset με 61 χαρακτηριστικά και συνολικά 20.952.648 δεδομένα, που περιλαμβάνουν 9.728.708 κακόβουλα και 11.223.940 κανονικά δεδομένα. Το dataset περιλαμβάνει ένα ευρύ φάσμα τύπων δεδομένων, από λειτουργικές καταστάσεις έως μετρήσεις αισθητήρων, και παρέχει μια ολοκληρωμένη προσομοίωση των αλληλεπιδράσεων στον πραγματικό κόσμο μεταξύ των συσκευών IIoT (Industrial Internet of Things). Επίσης, περιλαμβάνει 14 διαφορετικά είδη επιθέσεων, συμπεριλαμβανομένων μολύνσεων από κακόβουλο λογισμικό και DDoS [103].
- **ToN-IoT:** Το dataset ToN-IoT προορίζεται να διευκολύνει την λεπτομερή έρευνα σχετικά με την ασφάλεια των δικτύων IIoT, περιλαμβάνοντας δεδομένα τόσο για τυπικές λειτουργίες όσο και για πιθανές απειλές ασφαλείας. Περιέχει ένα σύνολο εννέα διαφορετικών τύπων επιθέσεων, παρέχοντας ένα ευρύ φάσμα κακόβουλων σεναρίων για έρευνα. Το dataset περιέχει ένα ικανοποιητικό όγκο δεδομένων, με 300.000 δεδομένα που έχουν ταξινομηθεί ως κακόβουλα και 161.043 ως μη κακόβουλα δεδομένα. Με 44 χαρακτηριστικά, το ToN-IoT παρέχει μια λεπτομερή εικόνα της συμπεριφοράς του δικτύου και της συσκευής, επιτρέποντας την ανάπτυξη εξελιγμένων μοντέλων ML και DL, ικανών να διακρίνουν μεταξύ κανονικών και ανώμαλων δραστηριοτήτων [63].
- **CTU-13:** Το dataset CTU-13 είναι ένας από τους λίγους διαθέσιμους στο κοινό πόρους που προσφέρει μια λεπτομερή εξέταση διαφόρων δειγμάτων botnet σε 13 διαφορετικά σενάρια. Είναι ειδικά σχεδιασμένο για την εις βάθος ανάλυση της συμπεριφοράς των botnet μέσα στην κυκλοφορία του δικτύου. Συγκεκριμένα, με 1.535.374 δεδομένα ταξινομημένα ως κακόβουλα και 3.181.797 δεδομένα ταξινομημένα ως μη κακόβουλα, το dataset περιέχει μια μεγάλη ποικιλία δεδομένων, επιτρέποντας την αξιόπιστη εκπαίδευση των IDS. Επιπλέον, το dataset περιλαμβάνει μόλις 6 χαρακτηριστικά που είναι απαραίτητα για την ανίχνευση της κίνησης που δημιουργείται από botnet, επιτρέποντας μια πιο αποτελεσματική και στοχευμένη ανάλυση [104].
- **DIDarknet:** Τα datasets CXVPN2016 [105] και ISCXTor2017 [106] συνδυάστηκαν για την δημιουργία του DIDarknet, μιας μεγάλης συλλογής που σχεδιάστηκε κυρίως για την ανάλυση της κυκλοφορίας του darknet σε συνδυασμό με την μη κακόβουλη δραστηριότητα του δικτύου.

Υπάρχουν συνολικά 158.659 δεδομένα, εκ των οποίων 24.311 έχουν ταξινομηθεί ως δεδομένα darknet και 134.348 μη κακόβουλα δεδομένα. Με 44 ολοκληρωμένα χαρακτηριστικά ανά εγγραφή, αυτό το dataset βοηθά σημαντικά στην δημιουργία μοντέλων για την αντιμετώπιση της κίνησης από darknet επιθέσεις [107].

- **IoT-Botnet 2020:** Το IoT-Botnet 2020 είναι μια ολοκληρωμένη συλλογή απειλών στον κυβερνοχώρο ειδικά για περιβάλλοντα IoT, όπως DDoS, DoS, σαρώσεις δικτύου και κλοπή πληροφοριών. Διαθέτει συνολικά 1.940.389 δεδομένα, με 97.197 μη κακόβουλα και 1.843.192 κακόβουλα δεδομένα. Επίσης προσφέρει μία λεπτομερή ανάλυση με 85 χαρακτηριστικά ανά εγγραφή [108].
- **CICIDS2017:** Ένας βασικός πόρος για την έρευνα στον τομέα της κυβερνοασφάλειας είναι το dataset CICIDS2017, το οποίο είναι ιδιαίτερα χρήσιμο για τον σχεδιασμό και την αξιολόγηση των IDS. Διαθέτει 2.830.540 δεδομένα που κατανέμονται σε 83 χαρακτηριστικά, με 2.359.087 μη κακόβουλα και 471.453 κακόβουλα δεδομένα. Αυτό το dataset προσομοιώνει την πραγματική κίνηση δικτύου σε έναν μεσαίου μεγέθους οργανισμό, καταγράφοντας τις δραστηριότητες μιας εβδομάδας με 15 διαφορετικούς τύπους επιθέσεων, όπως DDoS, botnets και σαρώσεις θυρών δικτύου [109].

Πίνακας 6.1: Σύνοψη των datasets.

| **Dataset** | **Αριθμός Χαρακτηριστικών** | **Δεδομένα** | **Μη κακόβουλα Δεδομένα** | **Κακόβουλα Δεδομένα** |
|---|---|---|---|---|
| UNSW-NB15 | 49 | 2.540.044 | 2.218.761 | 321.283 |
| BoT-IoT | 45 | 73.370.493 | 9.543 | 73.360.900 |
| NSL-KDD | 41 | 148.527 | 22.554 | 125.973 |
| N-BaIoT | 115 | 7.062.606 | 555.932 | 6.506.674 |
| IoT-23 | 6 | 60.307.990 | 30.858.735 | 294.449.255 |
| Edge-IIoT | 61 | 20.952.648 | 11.223.940 | 9.728.708 |
| ToN-IoT | 44 | 461.043 | 161.043 | 300.000 |
| CTU-13 | 6 | 4.717.171 | 3.181.797 | 1.535.374 |
| DIDarknet | 44 | 158.659 | 134.348 | 24.311 |
| IoT-Botnet 2020 | 85 | 1.940.389 | 97.197 | 1.843.192 |
| CICIDS2017 | 83 | 2.830.540 | 2.359.087 | 471.453 |

## 6.6 Επίλογος

Η εξέταση της ασφάλειας στα συστήματα του IoT έφερε στο φως τα σημαντικά εμπόδια και την επείγουσα ανάγκη για ισχυρά μέτρα ασφαλείας. Το κεφάλαιο ξεκινά με μια ανάλυση των ευπαθειών και προχωρά σε μια αναλυτική διερεύνηση των διαφόρων ειδών επιθέσεων που απευθύνονται ειδικά στα επίπεδα αντίληψης και δικτύου του IoT. Το κεφάλαιο ολοκληρώνεται με μία επισκόπηση των datasets που είναι απαραίτητα για την εκπαίδευση και την δοκιμή των λύσεων ασφαλείας του IoT. Κύριος σκοπός του κεφαλαίου είναι να υπογραμμίσει την σημασία της συνεχούς επαγρύπνησης και της εξέλιξης των πρωτοκόλλων ασφαλείας για την προστασία των διασυνδεδεμένων τεχνολογιών που είναι απαραίτητες για την σύγχρονη ζωή.

# 7. Τρόποι αντιμετώπισης βασισμένοι στην Μηχανική Μάθηση

## 7.1 Εισαγωγή

Βασιζόμενο άμεσα στις θεωρητικές βάσεις που καθορίστηκαν στο Κεφάλαιο 4, το παρόν κεφάλαιο εξετάζει τις πραγματικές χρήσεις των αλγορίθμων ML και DL για την βελτίωση της ασφάλειας του IoT. Εδώ, η εστίαση μετατοπίζεται από την αφηρημένη κατανόηση των διαφόρων αλγορίθμων σε συγκεκριμένες, πραγματικές εφαρμογές που έχουν χρησιμοποιηθεί με επιτυχία για την αντιμετώπιση των διαφόρων απειλών στον κυβερνοχώρο. Οι αλγόριθμοι που συζητήθηκαν προηγουμένως, οι οποίοι περιλαμβάνουν πιο εξελιγμένα DNN και DT, παρουσιάζονται τώρα στην πράξη, αποδεικνύοντας την προσαρμοστικότητα και την αποτελεσματικότητα τους στην ασφάλεια των περιβαλλόντων του IoT.

## 7.2 Έρευνες σχετικά με την χρήση ML στην ασφάλεια IoT

Είναι σημαντικό να προσεγγιστούν οι μελέτες με οργανωμένο τρόπο, καθώς ξεκινά η ανάλυση των εφαρμογών ML και DL στην ασφάλεια του IoT. Η ανάλυση παρουσιάζει τις έρευνες με χρονολογική σειρά, από τα παλαιότερα προς τα νεότερα, προκειμένου να δοθεί μια σαφής προοπτική για την εξέλιξη και την βελτίωση των τεχνικών ML και DL με την πάροδο του χρόνου. Κάθε έρευνα που πραγματοποιήθηκε αποτελεί μια στάση στην πορεία των τεχνολογιών, δείχνοντας πώς κάθε νέα εξέλιξη βασίστηκε στην προηγούμενη για την αντιμετώπιση όλο και πιο πολύπλοκων ζητημάτων ασφάλειας.

Ο Alrashdi κ.ά. [110], διερευνούν την χρήση του ML στον τομέα της ασφάλειας έξυπνων πόλεων χρησιμοποιώντας το dataset UNSW-NB15 και τον αλγόριθμο RF. Η εστίαση τους στην ανίχνευση ανωμαλιών παράγει εντυπωσιακά αποτελέσματα, με accuracy 99.34% και σχεδόν τέλειες βαθμολογίες σε precision, recall και F1-score με ποσοστό 98%, αποδεικνύοντας την αποτελεσματικότητα του RF στον εντοπισμό ακανόνιστων μοτίβων μέσα σε ροές αστικών δεδομένων. Στον τομέα των οπτικών δικτύων, ο Bensalem και η ομάδα του [111], χρησιμοποιούν ένα ANN για την καταπολέμηση των επιθέσεων jamming, ενώ εργάζονται με ένα ιδιωτικό dataset. Η έρευνα τους επιτυγχάνει υψηλό accuracy 99.5%, δείχνοντας τις δυνατότητες του ANN στην προστασία κρίσιμων δικτυακών υποδομών. Ο Hasan και οι συνεργάτες του [112], δοκιμάζουν διάφορα μοντέλα ML και DL, όπως DT, RF και ANNs, στο dataset DS2OS για την αντιμετώπιση διαφόρων τύπων επιθέσεων. Όλα τα μοντέλα επιτυγχάνουν υψηλό accuracy 99.4%, αλλά το μοντέλο RF προτιμάται επειδή υπερτερεί έναντι άλλων κρίσιμων μετρικών όπως το precision, το recall και το F1-score, τα οποία είναι όλα στο 99%. Ο Jan κ.ά. [113], δημιούργησαν ένα καινοτόμο ελαφρύ σύστημα IDS χρησιμοποιώντας τον αλγόριθμο SVM, ειδικά για να ξεπεράσουν τις αδυναμίες που έχουν τα συστήματα IoT, οι οποίες συζητήθηκαν στο κεφάλαιο 6. Η ομάδα διεξήγαγε ενδελεχή έρευνα χρησιμοποιώντας δύο ξεχωριστά πειράματα για να επικυρώσει την αποτελεσματικότητα του μοντέλου τους υπό διαφορετικές συνθήκες. Στο πρώτο πείραμα, χρησιμοποιώντας ένα ιδιωτικό dataset, το IDS είχε ικανοποιητικές επιδόσεις, επιτυγχάνοντας accuracy 91%. Βασιζόμενοι σε αυτό, διεξήχθη ένα δεύτερο πείραμα με το dataset CICIDS2017 και το σύστημα βελτίωσε σημαντικά το accuracy του, φτάνοντας το 98.35%.

Χρησιμοποιώντας ένα DNN βελτιστοποιημένο με διαφορετικούς αλγορίθμους EL, η ομάδα του Liao [74], δημιουργεί ένα σύστημα ελέγχου ταυτότητας για το φυσικό επίπεδο βασισμένο σε DL που προστατεύει από επιθέσεις πλαστογράφησης. Η μελέτη τους όχι μόνο εξετάζει την αποτελεσματικότητα αυτών των αλγορίθμων, αλλά προσφέρει επίσης μια σύγκριση των τεχνικών ελέγχου ταυτότητας με βάση το RMS (Root Mean Square) και το Adam (Adaptive Moment Estimation) με βάση τις

διαφορετικές απαιτήσεις. Σύμφωνα με την έρευνα τους, η Adam-based μέθοδος αυθεντικοποίησης έχει την ταχύτερη ταχύτητα σύγκλισης και ένα 97.75% ποσοστό accuracy, αλλά έχει ένα υψηλότερο υπολογιστικό κόστος. Σε αντίθεση, η RMS-based προσέγγιση έχει ένα πιο αργό ποσοστό σύγκλισης αλλά παράγει μια ελαφρώς χαμηλότερο accuracy 96.50%. Αυτό οφείλεται στην σημαντικά χαμηλότερη επιβάρυνση υπολογισμού της. Εξαιτίας της προσαρμοστικότητας, οι χρήστες μπορούν να επιλέξουν την καλύτερη τεχνική αυθεντικοποίησης για τις ανάγκες τους βασισμένη τους υπολογιστικούς πόρους που διαθέτουν.

Προκειμένου να εντοπίσουν και να κατηγοριοποιήσουν σοβαρές απειλές δικτύου, όπως blackhole, DDoS, sinkholes και wormholes, οι Thamilarasu και Chawla [114], αναπτύσσουν ένα IDS χρησιμοποιώντας DNN. Με μέσο ποσοστό precision 95%, recall 97% και F1-score 96%, το σύστημα τους αποδίδει σε ικανοποιητικό βαθμό. Οι Wang κ.ά. [115], αναλύουν δεδομένα από μονάδες μετρήσεις φασμάτων (Phasor Measurement Unit, PMU) για να προτείνουν ένα προηγμένο μοντέλο για την ανίχνευση επιθέσεων δικτύου σε διαταραχές των smart grids χρησιμοποιώντας RF ενισχυμένο με AdaBoost. Με accuracy 93.91%, precision 93.8%, recall 93.6% και F1-score 93.5%, η μέθοδος τους ανιχνεύει με επιτυχία 37 διαφορετικές κυβερνοεπιθέσεις. Συνδυάζοντας γενετικούς αλγορίθμους με DBN, ο Zhang και η ομάδα του [116], υλοποιούν ένα ευρηματικό IDS, το οποίο αξιολογείται στο dataset NSL-KDD. Με εντυπωσιακό μέσο accuracy 98.8%, precision 97.3%, recall 97.6% και F1-score 97.4%, αντιμετωπίζουν ένα ευρύ φάσμα επιθέσεων, συμπεριλαμβανομένων των DoS, R2L, U2R και Probe.

Οι Abu Al-Haija και Zein-Sabatto [117], χρησιμοποιούν ένα CNN στο dataset NSL-KDD για να αναπτύξουν αυτόνομα συστήματα ανίχνευσης και ταξινόμησης DL για κυβερνοεπιθέσεις. Το σύστημα τους υπερέχει στον εντοπισμό επιθέσεων DoS, R2L, U2R και Probe με accuracy 99.3%, precision 99.04%, recall 99.33% και F1-score 99.18%. Το LightGBM χρησιμοποιείται από τον Al-kasassbeh κ.ά [71], για την καταπολέμηση εξελιγμένων επιθέσεων botnet με βάση το dataset N-BaIoT. Επιτυγχάνουν το απόλυτο σε όλες τις μετρικές, 100% accuracy, precision, recall και F1-score, αποδεικνύοντας την αξιοσημείωτη ικανότητα του LightGBM να χειρίζεται προηγμένες επιθέσεις στο IoT. Για MANET δίκτυα, ο Amouri κ.ά [118], παρουσιάζουν ένα IDS δύο σταδίων που στοχεύει σε επιθέσεις DDoS και blackhole. Με βάση ένα ιδιωτικό dataset και ένα αλγόριθμο RF, το σύστημα τους παρουσιάζει μεταβλητή απόδοση υπό διάφορες συνθήκες. Επιτυγχάνει accuracy 98% σε σενάρια υψηλής ισχύος/ταχύτητας των κόμβων και accuracy 90% σε συνθήκες χαμηλής ισχύος/ταχύτητας των κόμβων, αποδεικνύοντας την προσαρμοστικότητα του σε ένα εύρος επιχειρησιακών περιβαλλόντων.

Ο Arjoune και οι συνεργάτες [119], του χρησιμοποιούν τον αλγόριθμο RF σε ένα ιδιωτικό dataset για να βελτιώσουν την ασφάλεια του δικτύου έναντι επιθέσεων jamming. Με accuracy 97.5%, το σύστημα τους είναι σε θέση να ανιχνεύει με επιτυχία τέτοιου είδους επιθέσεις. Ο Bagaa κ.ά [120], χρησιμοποιούν το one-class SVM για την υλοποίηση ενός συστήματος IDS σε έξυπνα κτίρια. Για την δοκιμή χρησιμοποιείται το dataset NSL-KDD. Με υψηλό accuracy 99.71%, η μέθοδος τους δείχνει πως το one-class SVM μπορεί να χρησιμοποιηθεί για την προστασία εξελιγμένων συστημάτων διαχείρισης κτιρίων. Ο Chen κ.ά. [121], χρησιμοποιούν το DT σε ένα ιδιωτικό dataset για να δημιουργήσουν ένα αξιόπιστο IDS σχεδιασμένο ειδικά για επιθέσεις DDoS. Τα αξιοσημείωτο accuracy 99.98%, το precision και το recall λίγο πάνω από 97% και η αντίστοιχη βαθμολογία F1-score αναδεικνύουν πόσο καλά τα DTs μπορούν να διακρίνουν μεταξύ μη κακόβουλης και κακόβουλης κυκλοφορίας.

Ο Hoang κ.ά [122], διερευνούν την χρήση των αλγορίθμων k-means και one-class SVM στην ανίχνευση επιθέσεων eavesdropping σε συστήματα που υποστηρίζονται από UAV. Όταν η ισχύς του υποκλοπέα είναι μεταξύ 0 και 10 dB, το one-class SVM αποδίδει καλά με accuracy περίπου 90%. Σε υψηλότερα επίπεδα ισχύος, μεταξύ 12 και 20 dB, ο k-means γίνεται πιο πλεονεκτικός, επιτυγχάνοντας

accuracy 99%. Ο Kasturi και οι συνάδελφοι του , χρησιμοποιούν το GB σε ένα ιδιωτικό dataset για να δημιουργήσουν ένα μηχανισμό για την κατηγοριοποίηση διαφόρων ειδών επιθέσεων jamming. Με accuracy 94.2%, το σύστημα τους καθιστά τα ασύρματα δίκτυα πιο ανθεκτικά, επιτρέποντας πιο εξελιγμένη ανίχνευση των απειλών.

Η επίθεση που στοχεύει στην τροποποίηση του κυκλώματος των συσκευών IoT, γνωστό ως hardware trojan, αντιμετωπίζεται από τον Khalid κ.ά [123]. Χρησιμοποιώντας ένα DNN σε ένα ιδιωτικό dataset, επιτυγχάνουν accuracy 96.25%, αποδεικνύοντας πόσο χρήσιμα είναι τα DNN για τον εντοπισμό τέτοιων τροποποιήσεων που μπορεί να θέσουν σε κίνδυνο την ακεραιότητα της συσκευής. Ο Peng κ.ά [124], προτείνουν ένα δημιουργικό τρόπο για την δημιουργία "δακτυλικών αποτυπωμάτων" ραδιοσυχνοτήτων που μπορούν να χρησιμοποιηθούν για την μοναδική αναγνώριση διαφόρων συσκευών με την χρήση ενός CNN. Η προσέγγιση τους, η οποία δοκιμάστηκε σε ένα ιδιωτικό dataset, επιτυγχάνει accuracy 99.1% ανοίγοντας την πόρτα για περισσότερα μέτρα ασφαλείας με βάση την αυθεντικοποίηση των συσκευών. Χρησιμοποιώντας τον αλγόριθμο RF που έχει δοκιμαστεί στα datasets UNSW-NB15 και CICIDS2017, ο Rashid κ.ά [125], αναπτύσσουν ένα IDS για την ενίσχυση των υποδομών στις έξυπνες πόλεις. Η μέθοδος τους διαχειρίζεται διάφορες απειλές δικτύου και βελτιώνει την ασφάλεια με ικανοποιητικά ποσοστά accuracy 95.45% και εξίσου ίσες βαθμολογίες precision, recall και F1-score.

Στον τομέα της υγειονομικής περίθαλψης, ο Roldan κ.ά [68], παρουσιάζουν ένα σύγχρονο μοντέλο LR που προορίζεται για τον εντοπισμό διαφόρων ειδών επιθέσεων σε πραγματικό χρόνο, συμπεριλαμβανομένων των port scans, DoS, TCP και UDP. Αυτό το μοντέλο είναι μοναδικό, καθώς διατηρεί την ακεραιότητα των ιατρικών συστημάτων, εγγυάται την προστασία των ευαίσθητων δεδομένων και λαμβάνει την μέγιστη βαθμολογία σε όλες τις μετρικές απόδοσης. Με έμφαση στην ασφάλεια δικτύων, ο Saharkhizan κ.ά [126], χρησιμοποιούν ένα μοντέλο LSTM για να αντιμετωπίσουν με επιτυχία επιθέσεις DoS και MitM, αποδεικνύοντας την ικανότητα του μοντέλου σε ένα ιδιωτικό dataset. Η έρευνα τους δείχνει πόσο καλά το LSTM μπορεί να αποκωδικοποιήσει και να μετριάσει σύνθετες απειλές στον κυβερνοχώρο σε περιβάλλοντα IoT, με accuracy 99.62%, precision 99.41%, recall 98.88% και F1-score 99.14%.

Στην ανάλυση τους για την ανίχνευση επιθέσεων botnet σε έξυπνες πόλεις, ο Shafiq κ.ά [127], συγκρίνουν τους αλγορίθμους C4.5, RF και NB χρησιμοποιώντας δεδομένα από το dataset BoT-IoT. Παρά το γεγονός ότι οι μετρικές αξιολόγησης ήταν ίδιες, με τιμές accuracy 99.79%, precision 100%, recall 100%, F1-score 100%, επιλέχθηκε ο NB λόγω της πολύ μικρότερης περιόδου εκπαίδευσης. Ο Zhang κ.ά [128], διερευνούν νέες προσεγγίσεις για την ανίχνευση επιθέσεων δικτύου συνδυάζοντας SVM και DBN για τον μετριασμό των επιθέσεων DoS στο dataset CICIDS2017. Αυτή η υβριδική προσέγγιση συνδυάζει το DL με τον υπολογισμό της ροής των δεδομένων για να παράγει accuracy 92.56% καθώς και υψηλά ποσοστά precision 97.7%, recall 97.6% και F1-score 97.6%. Ο Gad κ.ά [63], υλοποιούν ένα σύστημα IDS για VANET χρησιμοποιώντας το XGBoost. Η μέθοδος τους βελτιώνει αποτελεσματικά την ασφάλεια στις επικοινωνίες μεταξύ των οχημάτων και πετυχαίνει υψηλά ποσοστά μετρικής, 97.8% accuracy, precision, recall και F1-score, όταν εφαρμόζεται στο dataset ToN-IoT. Χρησιμοποιώντας AE σε συνδυασμό με SVM και εφαρμόζοντας στο dataset NSL-KDD, ο Lv κ.ά [129], δημιούργησαν ένα IDS που πετυχαίνει accuracy 97.83%.

Ο Sarker [130], παρέχει μια διεξοδική εξέταση της ανίχνευσης ανωμαλιών και πολλαπλών επιθέσεων με την χρήση του RF σε διάφορα datasets. Το σύστημα επιτυγχάνει 99% σε όλες τις μετρικές για τις ανωμαλίες και τις πολλαπλές επιθέσεις στο NSL-KDD. Στο dataset UNSW-NB15, οι επιδόσεις ποικίλλουν, με την ανίχνευση ανωμαλιών να σημειώνει σε όλες τις μετρικές 95% και την ανίχνευση

πολλαπλών επιθέσεων να σημειώνει χαμηλότερες επιδόσεις 82-83%. Χρησιμοποιώντας το AdaBoost σε ένα ιδιωτικό dataset που αποτελείται από 130.223 δεδομένα επιθέσεων DoS και 130.284 δεδομένα κανονικής κυκλοφορίας, ο Rachmadi κ.ά [131], επικεντρώνονται στην ανίχνευση επιθέσεων DoS. Το μοντέλο αποδίδει με 95.84% accuracy, 98.29% precision, 93.28% recall και 95.72% F1-score. Με την χρήση πολυδιάστατων CNN (CNN1D, CNN2D, CNN3D) στα datasets BoT-IoT και IoT-23, οι Ullah και Mahmoud [132], δημιουργούν ένα ιδιαίτερο IDS. Ωθούν τα όρια του DL στην ασφάλεια του IoT με την ευφυή προσέγγιση τους, η οποία αποδίδει εξαιρετικές μετρήσεις με 99.90% accuracy, 99.75% precision, 99.85% recall και 99.79% F1-score.

Ο Yang κ.ά [133], χρησιμοποιούν one-class SVM για να δημιουργήσουν ένα σύστημα ανίχνευσης που προορίζεται ειδικά για συσκευές IoT με περιορισμένους πόρους. Η προσέγγιση τους επικεντρώνεται στην μείωση των απαιτήσεων μνήμης και του χρόνου υπολογισμού για να ταιριάζει σε εφαρμογές του πραγματικού κόσμου και έχει εφαρμοστεί σε διάφορα datasets, συμπεριλαμβανομένων των CICIDS2017, CTU-13 και ιδιωτικών καταναλωτικών datasets IoT. Ωστόσο, δεν δίνονται συγκεκριμένες μετρήσεις επιδόσεων.

Ο Popoola κ.ά [134], χρησιμοποιούν στοιβαγμένα (stacked) RNNs για τον εντοπισμό botnets σε έξυπνα σπίτια, τα οποία αποτελούν ένα βήμα μπροστά από τα τυπικά RNNs λόγω του ότι μπορούν να διαχειρίζονται προβλήματα που υπερπροσαρμογής. Η προσέγγιση τους, όταν εφαρμόζεται στο dataset BoT-IoT, επιτυγχάνει τις απόλυτες βαθμολογίες σε όλες τις μετρικές. Σε παρόμοιο πλαίσιο, ο Pokhrel κ.ά [67], εντοπίζουν botnets με ακρίβεια 99.6% χρησιμοποιώντας τον αλγόριθμο KNN στο ίδιο dataset. Ενώ ο SRNN παρέχει άψογα ποσοστά στις μετρικές, ο απλούστερος αλγόριθμος KNN διατηρεί υψηλά ποσοστά accuracy, καθιστώντας τον ελκυστική επιλογή για περιπτώσεις όπου η υπολογιστική οικονομία και η ταχύτητα είναι σημαντικές.

Χρησιμοποιώντας το dataset DIDarknet, ο Abu Al-Haija κ.ά [135], παρουσιάζουν έναν εξελιγμένο μηχανισμό ταξινόμησης που συνδυάζει EL αλγορίθμους και ένα DT. Η μέθοδος τους, η οποία επιτυγχάνει αξιοσημείωτο accuracy ταξινόμησης 99.5%, είναι ειδικά σχεδιασμένη για τον εντοπισμό και την ταξινόμηση σύνθετων απειλών, όπως επιθέσεις darknet και blackhole. Οι Lahasan και Samma [136], δημιουργούν ένα ελαφρύ AE ειδικά για την ασφάλεια του IoT χρησιμοποιώντας μια νέα προσέγγιση που εξοικονομεί πόρους. Το dataset N-BaIoT χρησιμοποιείται για την δοκιμή αυτού του μοντέλου, το οποίο έχει λίγα κρυφά στρώματα και μικρό μέγεθος εισόδου. Επιτυγχάνουν εκπληκτικό accuracy 99% χρησιμοποιώντας μόνο 30 χαρακτηριστικά και τροφοδοτώντας δεδομένα σε 2 κρυμμένους νευρώνες. Οι βαθμολογίες precision, recall και F1-score είναι όλες πολυ υψηλές με τιμή 99%. Ο Liu κ.ά [75], χρησιμοποιούν το LSTM+ για να επεξεργαστούν ένα ιδιωτικό dataset θερμοκρασίας με έμφαση στην αξιοπιστία των δεδομένων σε συστήματα IoT. Στόχος του μοντέλου τους είναι ο εντοπισμός και η διόρθωση ανώμαλων δεδομένων, που αποτελεί βασικό στοιχείο της διατήρησης της ακεραιότητας των δεδομένων σε εφαρμογές IoT. Η εφαρμογή του LSTM+ υποδηλώνει μια εξελιγμένη μέθοδο για την εγγύηση της ακρίβειας και της αξιοπιστίας των δεδομένων, παρόλο που δεν δίνονται συγκεκριμένες μετρήσεις.

Ο Salman κ.ά [137], δημιούργησαν ένα ισχυρό σύστημα που χρησιμοποιεί έναν αλγόριθμο RF για να εγγυηθεί την ασφάλεια του IoT, δίνοντας έμφαση στην ανίχνευση κακόβουλης κυκλοφορίας και στην αναγνώριση των συσκευών. Με βάση τα τυποποιημένα μοτίβα κίνησης, το σύστημα αυτό δημιουργεί μοναδικά "δακτυλικά αποτυπώματα" για κάθε συσκευή IoT, επιτρέποντας του να αναγνωρίζει τον συγκεκριμένο τύπο κίνησης που παράγει η κάθε συσκευή. Σαρώνει συνεχώς την κυκλοφορία για αλλαγές που ενδέχεται να υποδηλώνουν παραβίαση της συσκευής ή πιθανές παραβιάσεις της ασφάλειας, αποκλίνοντας από αυτά τα αναμενόμενα μοτίβα. Το μοντέλο επιτυγχάνει

accuracy 94.5% για τον προσδιορισμό του τύπου της συσκευής, με precision 81.59%, recall 81.51% και F1-score 81.4%. Έχει επίσης ικανοποιητικές επιδόσεις στην ανίχνευση της ανώμαλης κυκλοφορίας με accuracy 97%, precision 85.81%, recall 86.28% και F1-score 86%.

Ο Douiba κ.ά [138], ενισχύουν τις δυνατότητες του IDS σε πολλαπλά datasets, συμπεριλαμβανομένων των Edge-IIoT, BoT-IoT, NSL-KDD και IoT-23, αξιοποιώντας ένα DT σε συνδυασμό EL. Το μοντέλο υπερέχει στην ανίχνευση ανωμαλιών, με μέσο accuracy, precision, recall και F1-score 99.99%.

Πίνακας 7.1: Σύνοψη των ερευνών

| **Άρθρο** | **Χρονολογία** | **Αλγόριθμος** | **Dataset** | **Accuracy** | **Precision** | **Recall** | **F1-score** |
|---|---|---|---|---|---|---|---|
| [110] | 2019 | RF | UNSW-NB15 | 99.34% | 98% | 98% | 98% |
| [111] | 2019 | ANN | Ιδιωτικό | 99.5% | - | - | - |
| [112] | 2019 | RF | DS2OS | 99.4% | 99% | 99% | 99% |
| [113] | 2019 | SVM | Ιδιωτικό<br>CICIDS2017 | 91%<br>98.35% | - | - | - |
| [74] | 2019 | DNN | Ιδιωτικό | 96.50% | - | - | - |
| [114] | 2019 | DNN | Ιδιωτικό | - | 95% | 97% | 96% |
| [115] | 2019 | RF+Adaboost | Ιδιωτικό | 93.91% | 93.8% | 93.6% | 93.5% |
| [116] | 2019 | DBN | NSL-KDD | 98.8% | 97.3% | 97.6% | 97.4% |
| [117] | 2020 | CNN | NSL-KDD | 99.3% | 99.04% | 99.33% | 99.18% |
| [71] | 2020 | LightGBM | N-BaIoT | 100% | 100% | 100% | 100% |
| [118] | 2020 | RF | Ιδιωτικό | a) 98%<br>b) 90% | - | - | - |
| [119] | 2020 | RF | Ιδιωτικό | 97.5% | - | - | - |
| [120] | 2020 | OCSVM | NSL-KDD | 99.71% | - | - | - |
| [121] | 2020 | DT | Ιδιωτικό | 99.98% | 97% | 97% | 97% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| [122] | 2020 | k-means<br>OCSVM | Ιδιωτικό | 90%<br>99% | | | |
| [123] | 2020 | DNN | Ιδιωτικό | 96.23% | - | - | - |
| [124] | 2020 | CNN | Ιδιωτικό | 99.1% | - | - | - |
| [125] | 2020 | RF | UNSW-NB15<br>CICIDS2017 | 95.45% | 95.45% | 95.45% | 95.45% |
| [68] | 2020 | LR | Ιδιωτικό | 100% | 100% | 100% | 100% |
| [126] | 2020 | LSTM | Ιδιωτικό | 99.62% | 99.41% | 98.88% | 99.14% |
| [127] | 2020 | NB | BoT-IoT | 99.79 | 100% | 100% | 100% |
| [128] | 2020 | SVM+DBN | CICIDS2017 | 92.56% | 97.7% | 97.6% | 97.6% |
| [63] | 2021 | XGBoost | ToN-IoT | 97.8% | 97.8% | 97.8% | 97.8% |
| [129] | 2021 | AE | NSL-KDD | 97.83% | - | - | - |
| [130] | 2021 | RF | NSL-KDD<br>UNSW-NB15 | 99%<br>a) 95%<br>b) 83% | 99%<br>95%<br>83% | 99%<br>95%<br>83% | 99%<br>95%<br>83% |
| [131] | 2021 | AdaBoost | Ιδιωτικό | 95.84% | 98.29% | 93.28% | 95.72% |
| [132] | 2021 | CNN | BoT-IoT<br>IoT-23 | 99.90% | 99.75% | 99.85% | 99.79% |
| [133] | 2021 | OCSVM | CICIDS2017<br>CTU-13<br>Ιδιωτικό | - | - | - | - |
| [134] | 2021 | SRNN | BoT-IoT | 100% | 100% | 100% | 100% |
| [67] | 2021 | KNN | BoT-IoT | 99.6% | - | - | - |
| [135] | 2022 | DT+EL | DIDarknet | 99.5% | - | - | - |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| [136] | 2022 | AE | N-BaIoT | 99% | 99% | 99% | 99% |
| [75] | 2022 | LSTM+ | Ιδιωτικό | - | - | - | - |
| [137] | 2022 | RF | Ιδιωτικό | a) 94.5%<br>b) 97% | 81.59%<br>85.81% | 81.5%<br>86.28% | 81.4%<br>86% |
| [138] | 2023 | DT+EL | Edge-IIoT<br>BoT-IoT<br>NSL-KDD<br>IoT-23 | 99.99% | 99.99% | 99.99% | 99.99% |

## 7.3 Επίλογος

Αυτό το κεφάλαιο σχετικά με την ασφάλεια του IoT που βασίζεται στο ML ολοκληρώνεται με ένα σύνολο εξελιγμένων λύσεων μηχανικής μάθησης που αναπτύσσονται σε διάφορα περιβάλλοντα IoT. Η εφαρμογή εξελιγμένων αλγορίθμων έχει αποδειχθεί ιδιαίτερα αποτελεσματική στην αποτροπή ενός ολοένα και πιο σύνθετου εύρους απειλών στον κυβερνοχώρο, από τα έξυπνα σπίτια και τα συστήματα υγειονομικής περίθαλψης έως τις έξυπνες πόλεις και τα δίκτυα αυτοκινήτων. Κατά την διάρκεια της ανάλυσης, διάφορα μοντέλα ML, από RF και SVM μέχρι τα πιο σύνθετα DNN και SRNN, τροποποιήθηκαν για να ικανοποιήσουν συγκεκριμένες απαιτήσεις. Η μετατόπιση από απλούστερες αλγοριθμικές εφαρμογές σε πιο σύνθετα σύνολα και υβριδικά μοντέλα αντικατοπτρίζει την μεταβαλλόμενη φύση των απειλών στον κυβερνοχώρο, η οποία απαιτεί πιο δυναμικούς και ανθεκτικούς αμυντικούς μηχανισμούς.

# 8. Συμπεράσματα και Μελλοντικές Κατευθύνσεις

Η διπλωματική έδειξε ότι ακόμη και με την χρήση των τεχνολογιών DL και ML, η απόλυτη ασφάλεια εξακολουθεί να είναι δύσκολο να επιτευχθεί. Οι κακόβουλοι χρήστες παραμένουν συνέχεια ένα βήμα μπροστά από τα πιο εξελιγμένα συστήματα ασφαλείας εξελίσσοντας συνεχώς τις στρατηγικές τους. Αν και τα μοντέλα ασφάλειας που εξετάστηκαν στην έρευνα έχουν επιδείξει ενθαρρυντικά αποτελέσματα όσον αφορά την ανίχνευση επιθέσεων, υπάρχει έλλειψη πραγματικών δεδομένων που να τεκμηριώνουν την ικανότητα των μοντέλων να αποτρέπουν με επιτυχία επιθέσεις στον πραγματικό κόσμο στον κυβερνοχώρο.

Η έρευνα παρείχε επίσης μια σύγκριση των απαιτήσεων των datasets και των απαιτήσεων των πόρων μεταξύ των ML και DL. Προκειμένου να εκπαιδευτούν τα μοντέλα DL έτσι ώστε να παρέχουν υψηλό accuracy, απαιτούνται μεγάλα datasets. Ωστόσο, οι περιορισμένοι πόροι των συσκευών IoT, περιορίζουν την εφαρμογή αυτών των μοντέλων. Επιπλέον, τα μοντέλα ML αντιμετωπίζουν δυσκολίες σε περιβάλλοντα IoT παρά το γεγονός ότι είναι συνήθως λιγότερο απαιτητικά σε πόρους από τα μοντέλα DL. Ακόμη και τα μοντέλα ML πρέπει να προσαρμόζονται προσεκτικά και να ενημερώνονται λόγω της πολυπλοκότητας και της ποικιλομορφίας των συστημάτων του IoT.

Μελλοντικά, οι τεχνολογίες federated learning και blockchain μπορούν να εξεταστούν για την βελτίωση της ασφάλειας του IoT. Αυτές οι τεχνολογίες είναι ακόμη πιο περίπλοκες από το ML και DL, με αποτέλεσμα να απαιτούνται ακόμη περισσότεροι πόροι που δεν μπορούν να παρέχουν οι συσκευές IoT.

# ΒΙΒΛΙΟΓΡΑΦΙΑ


[1] "Arpa-Arpanet-Internet.pdf." Accessed: Dec. 20, 2023. [Online]. Available: https://www.jbcoco.com/Arpa-Arpanet-Internet.pdf

[2] J. F. Kurose and K. W. Ross, *Computer networking: a top-down approach*, Seventh edition. Boston: Pearson, 2017.

[3] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, vol. 108, pp. 909–920, Jul. 2020, doi: 10.1016/j.future.2018.04.027.

[4] Accessed: Dec. 09, 2023. [Online]. Available: https://www.cs.cmu.edu/~coke/history_long.txt

[5] B. b. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 21, p. e4946, 2020, doi: 10.1002/cpe.4946.

[6] C. C. Sobin, "A Survey on Architecture, Protocols and Challenges in IoT," *Wirel. Pers. Commun.*, vol. 112, no. 3, pp. 1383–1429, Jun. 2020, doi: 10.1007/s11277-020-07108-5.

[7] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 1, pp. 616–644, 2020, doi: 10.1109/COMST.2019.2953364.

[8] "IoT connected devices by technology 2030," Statista. Accessed: Dec. 10, 2023. [Online]. Available: https://www.statista.com/statistics/1194688/iot-connected-devices-communications-technology/

[9] "Internet of Things - Worldwide | Statista Market Forecast," Statista. Accessed: Dec. 10, 2023. [Online]. Available: https://www.statista.com/outlook/tmo/internet-of-things/worldwide

[10] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *J. Netw. Comput. Appl.*, vol. 161, p. 102630, Jul. 2020, doi: 10.1016/j.jnca.2020.102630.

[11] D. Law, D. Dove, J. D'Ambrosia, M. Hajduczenia, M. Laubach, and S. Carlson, "Evolution of ethernet standards in the IEEE 802.3 working group," *IEEE Commun. Mag.*, vol. 51, no. 8, pp. 88–96, Aug. 2013, doi: 10.1109/MCOM.2013.6576344.

[12] S. Vitturi, C. Zunino, and T. Sauter, "Industrial Communication Systems and Their Future Challenges: Next-Generation Ethernet, IIoT, and 5G," *Proc. IEEE*, vol. 107, no. 6, pp. 944–961, Jun. 2019, doi: 10.1109/JPROC.2019.2913443.

[13] M. D. F. F. Domingues and A. Radwan, "Optical Fiber Sensors in IoT," in *Optical Fiber Sensors for IoT and Smart Devices*, in SpringerBriefs in Electrical and Computer Engineering. , Cham: Springer International Publishing, 2017, pp. 73–86. doi: 10.1007/978-3-319-47349-9_5.

[14] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, "Smart Choice for the Smart Grid: Narrowband Internet of Things (NB-IoT)," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1505–1515, Jun. 2018, doi: 10.1109/JIOT.2017.2781251.

[15] C. Chauvenet, G. Etheve, M. Sedjai, and M. Sharma, "G3-PLC based IoT sensor networks for SmartGrid," in *2017 IEEE International Symposium on Power Line Communications and its Applications (ISPLC)*, Madrid, Spain: IEEE, 2017, pp. 1–6. doi: 10.1109/ISPLC.2017.7897113.

[16] "Full Text PDF." Accessed: Nov. 16, 2023. [Online]. Available: https://media.proquest.com/media/hms/PFT/1/AzzPR?cit%3Aauth=Mansour%2C+Mohammad%3BGamal%2C+Amal%3BAhmed%2C+Ahmed+I%3BSaid%2C+Lobna+A%3BElbaz%2C+Abdelmoniem%3BHerencsar%2C+Norbert%3BSoltan%2C+Ahmed&cit%3Atitle=Internet+of+Things%3A+A+Comprehensive+Overview+on+Protocols%2C+...&cit%3Apub=Energies&cit%3Avol=16&cit%3Aiss=8&cit%3Apg=3465&cit%3Adate=2023&ic=true&cit%3Aprod=ProQuest+Preview+Content&_a=ChgyMDIzMTExNjA4NTUxMTU4NDo2OTMyMzkSBzEzODMzMjMaCk9ORV9TRUFSQ0giDTg3LjIwMi4xNDkuOTUqBzIwMzI0MDIyCjI4MDY1MjAwMzM6DURvY3VtZW50SW1hZ2VCATBSBk9ubGluZVoCRlRiA1BGVGoKMjAyMy8wMS8wMXIKMjAyMy8xMi8zMXoAggEgUC0xMDAwMDg0LTIwMTM5NS1TVEFGRi1udWxsLW51bGySAQZPbmxpbmXKAW9Nb3ppbGxhLzUuMCAoV2luZG93cyBOVCAxMC4wOyBXaW42NDsgeDY0KSBBcHBsZVdlYktpdC81MzcuMzYgKEtIVE1MLCBsaWtlIEdlY2tvKSBDaHJvbWUvMTE5LjAuMC

4wIFNhZmFyaS81MzcuMzbSARJTY2hvbGFybHkgSm91cm5hbHOaAgdQcmVQYWlkqgIrT1M6RU1TLU1lZGlhTGlua3NTZXJ2aWNlLWdldE1lZGlhVXJsRm9ySXRlbcoCD0FydGljbGV8RmVhdHVyZdICAVnyAgD6AgFZggMDV2ViigMcQ0lEOjIwMjMxMTE2MDg1NTExNTg0OjI0ODYwOQ%3D%3D&_s=MafpElA1%2FsuKDDkFJ%2Bljvp407vs%3D
[17] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless Body Area Networks: A Survey," *IEEE Commun. Surv. Tutor.*, vol. 16, no. 3, pp. 1658–1686, 2014, doi: 10.1109/SURV.2013.121313.00064.
[18] R. Nazir, A. A. laghari, K. Kumar, S. David, and M. Ali, "Survey on Wireless Network Security," *Arch. Comput. Methods Eng.*, vol. 29, no. 3, pp. 1591–1610, May 2022, doi: 10.1007/s11831-021-09631-5.
[19] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.
[20] D.-J. Deng, S.-Y. Lien, J. Lee, and K.-C. Chen, "On Quality-of-Service Provisioning in IEEE 802.11ax WLANs," *IEEE Access*, vol. 4, pp. 6086–6104, 2016, doi: 10.1109/ACCESS.2016.2602281.
[21] Z. Abichar, Yanlin Peng, and J. M. Chang, "WiMax: The Emergence of Wireless Broadband," *IT Prof.*, vol. 8, no. 4, pp. 44–48, Jul. 2006, doi: 10.1109/MITP.2006.99.
[22] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.
[23] D. Tan and Y. Liu, "The development and trend of wireless body area networks in the smart clothing field," in *Proceedings of the 4th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering 2015*, Xi'an, China: Atlantis Press, 2015. doi: 10.2991/icmmcce-15.2015.229.
[24] P. Chitra and T. Ranganayaki, "A Study on Manet: Applications, Challenges and Issues," *Int. J. Eng. Res.*, vol. 8, no. 03, 2020.
[25] S. Mohamed Hatim, S. Jamel Elias, N. Awang, and M. Y. Darus, "VANETs and Internet of Things (IoT): A Discussion," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 1, p. 218, Oct. 2018, doi: 10.11591/ijeecs.v12.i1.pp218-224.
[26] İ. Bekmezci, O. K. Sahingoz, and Ş. Temel, "Flying Ad-Hoc Networks (FANETs): A survey," *Ad Hoc Netw.*, vol. 11, no. 3, pp. 1254–1270, May 2013, doi: 10.1016/j.adhoc.2012.12.004.
[27] R. Al-Zaidi, J. Woods, M. Al-Khalidi, and H. Hu, "An IOT-enabled System for Marine Data Aquisition and Cartography," *Trans. Netw. Commun.*, Feb. 2017, doi: 10.14738/tnc.51.2796.
[28] M. A. Al-Absi, A. A. Al-Absi, M. Sain, and H. Lee, "Moving Ad Hoc Networks—A Comparative Study," *Sustainability*, vol. 13, no. 11, p. 6187, May 2021, doi: 10.3390/su13116187.
[29] J. Wei, J. Han, and S. Cao, "Satellite IoT Edge Intelligent Computing: A Research on Architecture," *Electronics*, vol. 8, no. 11, p. 1247, Oct. 2019, doi: 10.3390/electronics8111247.
[30] T. H. Moges, D. S. Lakew, N. P. Nguyen, N.-N. Dao, and S. Cho, "Cellular Internet of Things: Use cases, technologies, and future work," *Internet Things*, vol. 24, p. 100910, Dec. 2023, doi: 10.1016/j.iot.2023.100910.
[31] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of wireless sensor networks towards the Internet of Things: A survey".
[32] J. Espina, T. Falck, A. Panousopoulou, L. Schmitt, O. Mülhens, and G.-Z. Yang, "Network Topologies, Communication Protocols, and Standards," in *Body Sensor Networks*, G.-Z. Yang, Ed., London: Springer London, 2014, pp. 189–236. doi: 10.1007/978-1-4471-6374-9_5.
[33] "Wireless connectivity for the Internet of Things, one size does not fit all," 2014.
[34] Z. Mahmood, Ed., *Connected Environments for the Internet of Things: Challenges and Solutions*. in Computer Communications and Networks. Cham: Springer International Publishing, 2017. doi: 10.1007/978-3-319-70102-8.
[35] M. Azman, J. G. Panicker, and R. Kashyap, "Wireless Daisy Chain and Tree Topology Networks for Smart Cities," in *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India: IEEE, Feb. 2019, pp. 1–6. doi: 10.1109/ICECCT.2019.8869252.
[36] R. Jiang, "A review of Network Topology," in *Proceedings of the 2015 4th International*

*Conference on Computer, Mechatronics, Control and Electronic Engineering*, Guangzhou, China: Atlantis Press, 2015. doi: 10.2991/iccmcee-15.2015.222.
[37] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," *J. Comput. Commun.*, vol. 03, no. 05, pp. 164–173, 2015, doi: 10.4236/jcc.2015.35021.
[38] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, pp. 1–25, 2017, doi: 10.1155/2017/9324035.
[39] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey," *Sensors*, vol. 18, no. 9, p. 2796, Aug. 2018, doi: 10.3390/s18092796.
[40] R. W. Anwar, A. Zainal, T. Abdullah, and S. Iqbal, "Security Threats and Challenges to IoT and its Applications: A Review," in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, Paris, France: IEEE, Apr. 2020, pp. 301–305. doi: 10.1109/FMEC49853.2020.9144832.
[41] "IoT Security Best Practice Guidelines".
[42] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," *Internet Res.*, vol. 26, no. 2, pp. 337–359, Jan. 2016, doi: 10.1108/IntR-07-2014-0173.
[43] D. Navani, S. Jain, and M. S. Nehra, "The Internet of Things (IoT): A Study of Architectural Elements," in *2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, Jaipur, India: IEEE, Dec. 2017, pp. 473–478. doi: 10.1109/SITIS.2017.83.
[44] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *2012 10th International Conference on Frontiers of Information Technology*, Islamabad, Pakistan: IEEE, Dec. 2012, pp. 257–260. doi: 10.1109/FIT.2012.53.
[45] M. Zhang, F. Sun, and X. Cheng, "Architecture of Internet of Things and Its Key Technology Integration Based-On RFID," in *2012 Fifth International Symposium on Computational Intelligence and Design*, Hangzhou, China: IEEE, Oct. 2012, pp. 294–297. doi: 10.1109/ISCID.2012.81.
[46] M. U.Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A Review on Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 113, no. 1, pp. 1–7, Mar. 2015, doi: 10.5120/19787-1571.
[48] B. Fennani, H. Hamam, and A. O. Dahmane, "RFID overview," in *ICM 2011 Proceeding*, Hammamet, Tunisia: IEEE, Dec. 2011, pp. 1–5. doi: 10.1109/ICM.2011.6177411.
[49] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in *2017 8th International Conference on Information Technology (ICIT)*, Amman, Jordan: IEEE, May 2017, pp. 685–690. doi: 10.1109/ICITECH.2017.8079928.
[50] S. Cheruvu, A. Kumar, N. Smith, and D. M. Wheeler, *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment*. Berkeley, CA: Apress, 2020. doi: 10.1007/978-1-4842-2896-8.
[51] this link will open in a new tab Link to external site, this link will open in a new tab Link to external site, this link will open in a new tab Link to external site, this link will open in a new tab Link to external site, this link will open in a new tab Link to external site, and this link will open in a new tab Link to external site, "Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions," p. 3465, 2023, doi: 10.3390/en16083465.
[52] A. E. Omolara *et al.*, "The internet of things security: A survey encompassing unexplored areas and new insights," *Comput. Secur.*, vol. 112, p. 102494, Jan. 2022, doi: 10.1016/j.cose.2021.102494.
[53] G. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X. Costa, and B. Walke, "The IEEE 802.11 universe," *IEEE Commun. Mag.*, vol. 48, no. 1, pp. 62–70, Jan. 2010, doi: 10.1109/MCOM.2010.5394032.
[54] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, Jul. 2018, doi: 10.1016/j.jksuci.2016.10.003.
[55] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–29, Nov. 2019, doi: 10.1145/3292674.
[56] I. Mat, M. R. Mohd Kassim, A. N. Harun, and I. M. Yusoff, "Smart Agriculture Using Internet of

Things," in *2018 IEEE Conference on Open Systems (ICOS)*, Langkawi, Malaysia: IEEE, Nov. 2018, pp. 54–59. doi: 10.1109/ICOS.2018.8632817.
[57] C. Gupta, I. Johri, K. Srinivasan, Y.-C. Hu, S. M. Qaisar, and K.-Y. Huang, "A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks," *Sensors*, vol. 22, no. 5, p. 2017, Mar. 2022, doi: 10.3390/s22052017.
[58] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," *Internet Things*, vol. 14, p. 100365, Jun. 2021, doi: 10.1016/j.iot.2021.100365.
[59] S. Singh, "Cousins of Artificial Intelligence," Medium. Accessed: Apr. 02, 2024. [Online]. Available: https://towardsdatascience.com/cousins-of-artificial-intelligence-dda4edc27b55
[60] "Aurelien-Geron-Hands-On-Machine-Learning-with-Scikit-Learn-Keras-and-Tensorflow_-Concepts-Tools-and-Techniques-to-Build-Intelligent-Systems-OReilly-Media-2019.pdf." Accessed: Mar. 20, 2024. [Online]. Available: https://powerunit-ju.com/wp-content/uploads/2021/04/Aurelien-Geron-Hands-On-Machine-Learning-with-Scikit-Learn-Keras-and-Tensorflow_-Concepts-Tools-and-Techniques-to-Build-Intelligent-Systems-OReilly-Media-2019.pdf
[61] T. M. Ghazal *et al.*, "IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare—A Review," *Future Internet*, vol. 13, no. 8, Art. no. 8, Aug. 2021, doi: 10.3390/fi13080218.
[62] R. Rafique, S. M. R. Islam, and J. U. Kazi, "Machine learning in the prediction of cancer therapy," *Comput. Struct. Biotechnol. J.*, vol. 19, pp. 4003–4017, 2021, doi: 10.1016/j.csbj.2021.07.003.
[63] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset," *IEEE Access*, vol. 9, pp. 142206–142217, 2021, doi: 10.1109/ACCESS.2021.3120626.
[64] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.
[65] J. Alsamiri and K. Alsubhi, "Internet of Things Cyber Attacks Detection using Machine Learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, 2019, doi: 10.14569/IJACSA.2019.0101280.
[66] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1686–1721, 2020, doi: 10.1109/COMST.2020.2986444.
[67] S. Pokhrel, R. Abbas, and B. Aryal, "IoT Security: Botnet detection in IoT using Machine learning." arXiv, Apr. 05, 2021. Accessed: Mar. 03, 2024. [Online]. Available: http://arxiv.org/abs/2104.02231
[68] J. Roldán, J. Boubeta-Puig, J. Luis Martínez, and G. Ortiz, "Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks," *Expert Syst. Appl.*, vol. 149, p. 113251, Jul. 2020, doi: 10.1016/j.eswa.2020.113251.
[69] G. James, D. Witten, T. Hastie, R. Tibshirani, and J. Taylor, "Linear Regression," in *An Introduction to Statistical Learning*, in Springer Texts in Statistics. , Cham: Springer International Publishing, 2023, pp. 69–134. doi: 10.1007/978-3-031-38747-0_3.
[70] X. Wang and X. Lu, "A Host-Based Anomaly Detection Framework Using XGBoost and LSTM for IoT Devices," *Wirel. Commun. Mob. Comput.*, vol. 2020, p. e8838571, Oct. 2020, doi: 10.1155/2020/8838571.
[71] M. Al-kasassbeh, M. A. Abbadi, and A. M. Al-Bustanji, "LightGBM Algorithm for Malware Detection," in *Intelligent Computing*, K. Arai, S. Kapoor, and R. Bhatia, Eds., in Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, 2020, pp. 391–403. doi: 10.1007/978-3-030-52243-8_28.
[72] M. Z. Alom *et al.*, "A State-of-the-Art Survey on Deep Learning Theory and Architectures," *Electronics*, vol. 8, no. 3, Art. no. 3, Mar. 2019, doi: 10.3390/electronics8030292.
[73] B. Mostafa, N. El-Attar, S. Abd-Elhafeez, and W. Awad, "Machine and Deep Learning Approaches in Genome: Review Article," *Alfarama J. Basic Appl. Sci.*, Aug. 2020, doi: 10.21608/ajbas.2020.34160.1023.
[74] R.-F. Liao *et al.*, "Security Enhancement for Mobile Edge Computing Through Physical Layer Authentication," *IEEE Access*, vol. 7, pp. 116390–116401, 2019, doi:

10.1109/ACCESS.2019.2934122.
[75] J. Liu, J. Bai, H. Li, and B. Sun, “Improved LSTM-Based Abnormal Stream Data Detection and Correction System for Internet of Things,” *IEEE Trans. Ind. Inform.*, vol. 18, no. 2, pp. 1282–1290, Feb. 2022, doi: 10.1109/TII.2021.3079504.
[76] M. Roopak, G. Yun Tian, and J. Chambers, “Deep Learning Models for Cyber Security in IoT Networks,” in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA: IEEE, Jan. 2019, pp. 0452–0457. doi: 10.1109/CCWC.2019.8666588.
[77] A. Dertat, “Applied Deep Learning - Part 3: Autoencoders,” Medium. Accessed: Apr. 10, 2024. [Online]. Available: https://towardsdatascience.com/applied-deep-learning-part-3-autoencoders-1c083af4d798
[78] M. A. Amanullah *et al.*, “Deep learning and big data technologies for IoT security,” *Comput. Commun.*, vol. 151, pp. 495–517, Feb. 2020, doi: 10.1016/j.comcom.2020.01.016.
[79] M. Abomhara and G. M. Køien, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,” *J. Cyber Secur. Mobil.*, pp. 65–88, May 2015, doi: 10.13052/jcsm2245-1439.414.
[80] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018, doi: 10.1016/j.future.2017.07.060.
[81] Z. Chen *et al.*, “Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats,” *ACM Comput. Surv.*, vol. 55, no. 5, pp. 1–37, May 2023, doi: 10.1145/3530812.
[82] A. Mosenia and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things,” *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 4, pp. 586–602, Oct. 2017, doi: 10.1109/TETC.2016.2606384.
[83] H. Akram, D. Konstantas, and M. Mahyoub, “A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, 2018, doi: 10.14569/IJACSA.2018.090349.
[84] C. Wheelus and X. Zhu, “IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework,” *IoT*, vol. 1, no. 2, pp. 259–285, Oct. 2020, doi: 10.3390/iot1020016.
[85] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, “IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges,” *IEEE Access*, vol. 8, pp. 168825–168853, 2020, doi: 10.1109/ACCESS.2020.3022842.
[86] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations,” *IEEE Commun. Surv. Tutor.*, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.
[87] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
[88] S. Duangphasuk, P. Duangphasuk, and C. Thammarat, “Review of Internet of Things (IoT): Security Issue and Solution,” in *2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, Phuket, Thailand: IEEE, Jun. 2020, pp. 559–562. doi: 10.1109/ECTI-CON49241.2020.9157904.
[89] Y. Chahid, M. Benabdellah, and A. Azizi, “Internet of Things Protocols Comparison, Architecture, Vulnerabilities and Security: State of the art,” in *Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems*, Larache Morocco: ACM, Nov. 2017, pp. 1–6. doi: 10.1145/3167486.3167554.
[90] B. Santos, “DoS vs DDoS: Are they the same thing? IPVanish.” Accessed: Feb. 28, 2024. [Online]. Available: https://www.ipvanish.com/blog/dos-vs-ddos/
[91] D. Rani, N. S. Gill, and P. Gulia, “CLASSIFICATION OF SECURITY ISSUES AND CYBER ATTACKS IN LAYERED INTERNET OF THINGS,” . *Vol.*, no. 13, 2022.
[92] G. Glissa, A. Rachedi, and A. Meddeb, “A Secure Routing Protocol Based on RPL for Internet of Things,” in *2016 IEEE Global Communications Conference (GLOBECOM)*, Washington, DC,

USA: IEEE, Dec. 2016, pp. 1–7. doi: 10.1109/GLOCOM.2016.7841543.
[93] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in *2015 International Conference on Pervasive Computing (ICPC)*, Pune, India: IEEE, Jan. 2015, pp. 1–6. doi: 10.1109/PERVASIVE.2015.7087034.
[94] K. Angrishi, "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets." arXiv, Feb. 13, 2017. Accessed: Nov. 27, 2023. [Online]. Available: http://arxiv.org/abs/1702.03681
[95] "Yandex Pummeled by Potent Meris DDoS Botnet." Accessed: Feb. 29, 2024. [Online]. Available: https://threatpost.com/yandex-meris-botnet/169368/
[96] "What is recursive DNS?," Cloudflare. Accessed: Feb. 29, 2024. [Online]. Available: https://www.cloudflare.com/learning/dns/what-is-recursive-dns/
[97] "Stuxnet explained: The first known cyberweapon," CSO Online. Accessed: Mar. 01, 2024. [Online]. Available: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html
[98] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia: IEEE, Nov. 2015, pp. 1–6. doi: 10.1109/MilCIS.2015.7348942.
[99] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Gener. Comput. Syst.*, vol. 100, pp. 779–796, Nov. 2019, doi: 10.1016/j.future.2019.05.041.
[100] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, ON, Canada: IEEE, Jul. 2009, pp. 1–6. doi: 10.1109/CISDA.2009.5356528.
[101] Y. Meidan *et al.*, "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: 10.1109/MPRV.2018.03367731.
[102] "IoT-23 Dataset: A labeled dataset of Malware and Benign IoT Traffic.," Stratosphere IPS. Accessed: Apr. 19, 2024. [Online]. Available: https://www.stratosphereips.org/datasets-iot23
[103] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.
[104] S. García, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," *Comput. Secur.*, vol. 45, pp. 100–123, Sep. 2014, doi: 10.1016/j.cose.2014.05.011.
[105] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of Encrypted and VPN Traffic using Time-related Features:," in *Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, Rome, Italy: SCITEPRESS - Science and and Technology Publications, 2016, pp. 407–414. doi: 10.5220/0005740704070414.
[106] A. Habibi Lashkari, G. Draper Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of Tor Traffic using Time based Features:," in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, Porto, Portugal: SCITEPRESS - Science and Technology Publications, 2017, pp. 253–262. doi: 10.5220/0006105602530262.
[107] A. Habibi Lashkari, G. Kaur, and A. Rahali, "DIDarknet: A Contemporary Approach to Detect and Characterize the Darknet Traffic using Deep Image Learning," in *Proceedings of the 2020 10th International Conference on Communication and Network Security*, in ICCNS '20. New York, NY, USA: Association for Computing Machinery, Mar. 2021, pp. 1–13. doi: 10.1145/3442520.3442521.
[108] Z. Ahmad *et al.*, "Anomaly Detection Using Deep Neural Network for IoT Architecture," *Appl. Sci.*, vol. 11, no. 15, Art. no. 15, Jan. 2021, doi: 10.3390/app11157050.
[109] R. Panigrahi and S. Borah, "A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems," *Int. J. Eng. Technol.*, vol. 7, pp. 479–482, Jan. 2018.
[110] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning," in *2019 IEEE 9th Annual*

*Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA: IEEE, Jan. 2019, pp. 0305–0310. doi: 10.1109/CCWC.2019.8666450.
[111] M. Bensalem, S. K. Singh, and A. Jukan, "On Detecting and Preventing Jamming Attacks with Machine Learning in Optical Networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2019, pp. 1–6. doi: 10.1109/GLOBECOM38437.2019.9013238.
[112] M. Hasan, Md. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, p. 100059, Sep. 2019, doi: 10.1016/j.iot.2019.100059.
[113] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a Lightweight Intrusion Detection System for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019, doi: 10.1109/ACCESS.2019.2907965.
[114] G. Thamilarasu and S. Chawla, "Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things," *Sensors*, vol. 19, no. 9, Art. no. 9, Jan. 2019, doi: 10.3390/s19091977.
[115] D. Wang, X. Wang, Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning," *J. Inf. Secur. Appl.*, vol. 46, pp. 42–52, Jun. 2019, doi: 10.1016/j.jisa.2019.02.008.
[116] Y. Zhang, P. Li, and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019, doi: 10.1109/ACCESS.2019.2903723.
[117] Q. Abu Al-Haija and S. Zein-Sabatto, "An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks," *Electronics*, vol. 9, no. 12, p. 2152, Dec. 2020, doi: 10.3390/electronics9122152.
[118] A. Amouri, V. T. Alaparthy, and S. D. Morgera, "A Machine Learning Based Intrusion Detection System for Mobile Internet of Things," *Sensors*, vol. 20, no. 2, Art. no. 2, Jan. 2020, doi: 10.3390/s20020461.
[119] Y. Arjoune, F. Salahdine, Md. S. Islam, E. Ghribi, and N. Kaabouch, "A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication," in *2020 International Conference on Information Networking (ICOIN)*, Jan. 2020, pp. 459–464. doi: 10.1109/ICOIN48656.2020.9016462.
[120] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," *IEEE Access*, vol. 8, pp. 114066–114077, 2020, doi: 10.1109/ACCESS.2020.2996214.
[121] Y.-W. Chen, J.-P. Sheu, Y.-C. Kuo, and N. Van Cuong, "Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning," in *2020 European Conference on Networks and Communications (EuCNC)*, Jun. 2020, pp. 122–127. doi: 10.1109/EuCNC48522.2020.9200909.
[122] T. M. Hoang, N. M. Nguyen, and T. Q. Duong, "Detection of Eavesdropping Attack in UAV-Aided Wireless Systems: Unsupervised Learning With One-Class SVM and K-Means Clustering," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 2, pp. 139–142, Feb. 2020, doi: 10.1109/LWC.2019.2945022.
[123] F. Khalid, S. R. Hasan, S. Zia, O. Hasan, F. Awwad, and M. Shafique, "MacLeR: Machine Learning-Based Runtime Hardware Trojan Detection in Resource-Constrained IoT Edge Devices," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 39, no. 11, pp. 3748–3761, Nov. 2020, doi: 10.1109/TCAD.2020.3012236.
[124] L. Peng, J. Zhang, M. Liu, and A. Hu, "Deep Learning Based RF Fingerprint Identification Using Differential Constellation Trace Figure," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 1091–1095, Jan. 2020, doi: 10.1109/TVT.2019.2950670.
[125] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, and S. Gordon, "Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques," *Int. J. Environ. Res. Public. Health*, vol. 17, no. 24, p. 9347, Dec. 2020, doi: 10.3390/ijerph17249347.
[126] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8852–8859, Sep. 2020, doi: 10.1109/JIOT.2020.2996425.
[127] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning

algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Gener. Comput. Syst.*, vol. 107, pp. 433–442, Jun. 2020, doi: 10.1016/j.future.2020.02.017.
[128] H. Zhang, Y. Li, Z. Lv, A. K. Sangaiah, and T. Huang, "A real-time and ubiquitous network attack detection based on deep belief network and support vector machine," *IEEECAA J. Autom. Sin.*, vol. 7, no. 3, pp. 790–799, May 2020, doi: 10.1109/JAS.2020.1003099.
[129] Z. Lv, L. Qiao, J. Li, and H. Song, "Deep-Learning-Enabled Security Issues in the Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9531–9538, Jun. 2021, doi: 10.1109/JIOT.2020.3007130.
[130] I. H. Sarker, "CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks," *Internet Things*, vol. 14, p. 100393, Jun. 2021, doi: 10.1016/j.iot.2021.100393.
[131] S. Rachmadi, S. Mandala, and D. Oktaria, "Detection of DoS Attack using AdaBoost Algorithm on IoT System," in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, Bandung, Indonesia: IEEE, Oct. 2021, pp. 28–33. doi: 10.1109/ICoDSA53588.2021.9617545.
[132] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.
[133] K. Yang, S. Kpotufe, and N. Feamster, "An Efficient One-Class SVM for Anomaly Detection in the Internet of Things." arXiv, Apr. 22, 2021. doi: 10.48550/arXiv.2104.11146.
[134] S. I. Popoola, B. Adebisi, M. Hammoudeh, H. Gacanin, and G. Gui, "Stacked recurrent neural network for botnet detection in smart homes," *Comput. Electr. Eng.*, vol. 92, p. 107039, Jun. 2021, doi: 10.1016/j.compeleceng.2021.107039.
[135] Q. Abu Al-Haija, M. Krichen, and W. Abu Elhaija, "Machine-Learning-Based Darknet Traffic Detection System for IoT Applications," *Electronics*, vol. 11, no. 4, p. 556, Feb. 2022, doi: 10.3390/electronics11040556.
[136] B. Lahasan and H. Samma, "Optimized Deep Autoencoder Model for Internet of Things Intruder Detection," *IEEE Access*, vol. 10, pp. 8434–8448, 2022, doi: 10.1109/ACCESS.2022.3144208.
[137] O. Salman, I. H. Elhajj, A. Chehab, and A. Kayssi, "A machine learning based framework for IoT device identification and abnormal traffic detection," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3743, 2022, doi: 10.1002/ett.3743.
[138] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," *J. Supercomput.*, vol. 79, no. 3, pp. 3392–3411, Feb. 2023, doi: 10.1007/s11227-022-04783-y.
[139] M. Mansour *et al.*, "Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions," *Energies*, vol. 16, no. 8, p. 3465, Apr. 2023, doi: 10.3390/en16083465.