ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Απειλές και προκλήσεις στο Διαδίκτυο των πραγμάτων (IoT) και ενίσχυση της αρχιτεκτονικής ασφαλείας του, αξιοποιώντας δυνατότητες των δικτύων που καθορίζονται από λογισμικό (Software Defined Networks-SDN)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΝΑΤΟΥΔΗ ΑΘΑΝΑΣΙΟΥ

(ΑΕΜ: 2461)

Επιβλέπων: Σπυρίδων Νικολάου

Λέκτορας

Καστοριά Απρίλιος - 2023

Η παρούσα σελίδα σκοπίμως παραμένει λευκή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Security Threats and Challenges of the Internet of Things (IoT) and enhancing its security architecture by leveraging features supported by Software Defined Networks (SDN)

ΠΤΥΧΙΑΚΗ ΡΓΑΣΙΑ

ΤΟΥ

ΝΑΤΟΥΔΗ ΑΘΑΝΑΣΙΟΥ

(ΑΕΜ:2461)

Επιβλέπων: Νικολάου Σπυρίδων

Λέκτορας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ημερομηνία εξέτασης

....

Καστοριά Απρίλιος - 2023

Ευχαριστίες

Με την ολοκλήρωση των προπτυχιακών σπουδών μου στο τμήμα πληροφορικής του Πανεπιστήμιου Δυτικής Μακεδονίας, μου δίνεται η ευκαιρία να εκφράσω τις ευχαριστίες μου σε όλους όσους έχουν συμβάλει στην λειτουργία του τμήματος και την συντήρηση του. Ένα μεγάλο ευχαριστώ οφείλω στους καθηγητές για την αμεσότητα και την ανταπόκριση που δείχνουν. Θα ήθελα χωριστά να ευχαριστήσω τον κύριο Νικολάου Σπυρίδων για την διδασκαλία του και για την κατεύθυνση που μου έδωσε κατά τη διάρκεια της συγγραφής της εργασίας μου. Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου, που με στήριξαν στην διάρκεια των σπουδών μου και ήταν ο λόγος που μπόρεσα να περάσω αυτό το σκαλοπάτι στη σταδιοδρομία μου.

Περίληψη

Στην εποχή που διανύουμε δισεκατομμύρια συσκευές βρίσκονται συνδεμένες στο Διαδίκτυο των Πραγμάτων (Internet of Things – IoT). Το γεγονός ότι οι ετερογενείς αυτές συσκευές πολλαπλασιάζονται και δημιουργούν τεράστιο όγκο δεδομένων γεννά κινδύνους και δυσκολίες που αφορούν την ασφάλεια και την διαχείριση τους. Ως εκ τούτου, οι προτεινόμενες λύσεις από τη σκοπιά της δικτύωσης του IoT πρέπει να λαμβάνουν υπόψη την επεκτασιμότητα των κόμβων IoT καθώς και το λειτουργικό κόστος ανάπτυξης της υποδομής δικτύωσης. Με την αύξηση του αριθμού των συσκευών που χρησιμοποιούνται στο Διαδίκτυο των Πραγμάτων, προέκυψε η ανάγκη για τη διαχείριση αυτών των συσκευών και των εφαρμογών τους.

Εκτός από την ανάγκη για την κατάλληλη και αποτελεσματική προστασία τους, ώστε να διασφαλίζεται η πλήρης λειτουργική τους απόδοση. Έχει προταθεί το Software-Defined Networking (SDN) για να ξεπεραστούν τα προβλήματα του παραδοσιακού δικτύου. Το SDN έγινε ικανό να διαχωρίσει τις λογικές λειτουργίες και τις λειτουργίες ελέγχου στις κατανεμημένες συσκευές που βρίσκονται στο επίπεδο δικτύου, μεταφέροντάς τες στο κεντρικό επίπεδο ελέγχου που διεκπεραιώνει τα διοικητικά θέματα αυτού του δικτύου.

Επιπλέον, εμφανίζονται ζητήματα ασφάλειας, λόγω του γεγονότος ότι μη αξιόπιστες συσκευές IoT διασυνδέονται απευθείας με δίκτυα που συγκεντρώνουν δεδομένα. Σε αυτά τα προβλήματα προσπαθεί να δώσει λύσεις η χρήση λογισμικών διαχείρισης δικτύων (SDN).

Στην παρούσα εργασία αναλύονται τα βασικά χαρακτηριστικά του Διαδικτύου των Πραγμάτων και δίνεται έμφαση στις απειλές και προκλήσεις ασφαλείας των εφαρμογών IoT. Επίσης, μελετώνται τρόποι αντιμετώπισης αυτών των θεμάτων ασφαλείας με τη χρήση SDN.

Λέξεις κλειδιά: Διαδίκτυο των Πραγμάτων (Internet of Things), Δίκτυα καθοριζόμενα από λογισμικό (Software Defined Networks), Ασφάλεια

Abstract

Nowadays, billions of devices are connected to the Internet of Things (IoT). The fact that these heterogeneous devices are multiplying and generating vast amounts of data creates risks and difficulties regarding their security and management. Therefore, the proposed solutions from an IoT networking perspective must consider the scalability of the IoT nodes as well as the operational cost of deploying the networking infrastructure. With the increase in the number of devices used on the Internet of Things, the need to manage these devices and their applications has arisen.

In addition to the need to protect them appropriately and effectively to ensure their full operational performance. Software-Defined Networking (SDN) has been proposed to overcome the problems of the traditional network. SDN has become capable of separating the logical and control functions in the distributed devices located at the network layer, moving them to the central control plane that oversees the administrative aspects of this network.

In addition, security issues arise since untrusted IoT devices are directly interconnected to networks that aggregate data. The use of network management software (SDN) tries to provide solutions to these problems.

In this paper, the key characteristics of the Internet of Things are analyzed, and the focus is on the security threats and challenges of IoT applications. Also, ways to address these security issues using SDN are studied.

Keywords: Internet of Things (IoT), Software Defined Networks (SDN), Security, Threats, Challenges, Security Architecture

Πίνακας περιεχομένων

Λίστα Εικόνων

1. Εισαγωγή

Υπάρχουν δισεκατομμύρια αντικείμενα συνδεμένα στο διαδίκτυο και μόνο την αύξηση τους μπορεί κανείς να προβλέψει. Ένα άμεσο παράδειγμα αποτελούν οι οικιακές συσκευές και συσκευές που συναντούμε καθημερινά όπως έξυπνοι σηματοδότες, έξυπνα οχήματα και άλλα αντικείμενα που κάνουν χρήση αισθητήρων και ενεργοποιητών. Η κίνηση των δεδομένων που παράγουν αυτές οι συσκευές αποτελεί πλέον τεράστιο μέρος του συνολικού όγκου δεδομένων στο διαδίκτυο. Φυσικά, αυτό επιφέρει κάποια πολύ σοβαρά προβλήματα. Παρατηρούμε να προκύπτουν πολλές απειλές και μια αύξηση των κινδύνων που οφείλονται σε επιθέσεις. Η ασφάλεια στο Διαδίκτυο των Πραγμάτων όπως ανακάλυψα, έχει τεράστια απήχηση στην επιστημονική κοινότητα.

Σε αυτή την εργασία, παρουσιάζεται το Διαδίκτυο των Πραγμάτων και να αναφέρονται το μοντέλο αρχιτεκτονικής, τα χαρακτηριστικά και κάποια βασικά πρωτόκολλα που αναπτύσσονται γύρω του. Επίσης γίνεται μια παρουσίαση των εφαρμογών που κάνουν χρήση του IoT και ακολουθεί η ανάλυση των προϋποθέσεων για ασφάλεια καθώς αποτελούν βασικό κριτήριο για την δημιουργία των εφαρμογών. Στη συνέχεια γίνεται αναφορά των κινδύνων που συναντώνται στο Διαδίκτυο των Πραγμάτων και επιχειρείται η κατανομή τους βάση το επίπεδο αρχιτεκτονικής που συναντώνται. Αφού αναλυθούν οι απειλές και οι προκλήσεις, παρουσιάζονται οι τεχνικές blockchain, Fog computing και Edge computing. Η ενσωμάτωση των τεχνολογιών edge και fog computing αποτελούν πολύ σημαντική λύση για το Διαδίκτυο των Πραγμάτων και παρέχουν χαρακτηριστικά όπως η επεξεργασία η αποθήκευση, η γρήγορη πρόσβαση σε δεδομένα και ενισχύουν την ασφάλεια.

Παρουσιάζεται η τεχνολογία SDN με αναφορά στην αρχιτεκτονική, τη λειτουργία τις δυνατότητες και τα στοιχεία που αποτελείται και εξηγούνται οι τρόποι που βελτιώνει την ασφάλεια στο Διαδίκτυο των Πραγμάτων. Τέλος παρουσιάζονται προτάσεις εφαρμογής του SDN σε περιβάλλοντα IoT.

Στόχος αυτής της εργασίας είναι να βοηθήσει τον αναγνώστη να καταλάβει πόσο σημαντικό είναι το Διαδίκτυο των Πραγμάτων στην εποχή μας και πόσο κρίσιμη είναι η ασφάλεια σε ότι το αφορά. Με την παρουσίαση του SDN και κάνοντας χρήση της βιβλιογραφίας, γίνεται

προσπάθεια να αναδειχθούν οι δυνατότητες του επί του πρακτέος και να επιδειχθεί ο σημαντικός ρόλος που μπορεί να παίξει στο Διαδίκτυο των Πραγμάτων.

2. Διαδίκτυο των Πραγμάτων (IoT)

Σε αυτό το κεφάλαιο θα παρουσιαστούν γενικές πληροφορίες σε ότι αφορά το Διαδίκτυο των Πράγματων και την χρησιμότητα του, και κάποιες ειδικές όπου εξηγούν με περισσότερες λεπτομέρειες την λειτουργία και τα χαρακτηριστικά του.

2.1 Τι είναι το Διαδίκτυο των Πραγμάτων

2.1.1 Ορισμός

Η παγκόσμια ένωση τηλεπικοινωνιών (International Telecommunications Union) ορίζει το Διαδίκτυο των πραγμάτων (IoT) ως την «παγκόσμια υποδομή για την κοινωνία της πληροφορίας, που επιτρέπει προηγμένες υπηρεσίες μέσω της διασύνδεσης (φυσικών και εικονικών) πραγμάτων που βασίζονται σε υπάρχουσες και εξελισσόμενες διαλειτουργικές τεχνολογίες πληροφοριών και επικοινωνιών».

2.1.2 Χαρακτηριστικά

Αν συγκρίνουμε το Διαδίκτυο των πραγμάτων με τις κινητές προσωπικές συσκευές (κινητά τηλέφωνα), εύκολα θα διακρίνουμε τον περιορισμό σε επεξεργαστικούς πόρους, χωρητικότητα και μνήμη. Για το λόγο αυτό, είναι συχνό φαινόμενο να συνδέονται σε κάποιο cloud/fog για την απαιτούμενη επεξεργασία δεδομένων. Τα κυριότερα μέρη που καθιστούν δυνατές τις λειτουργίες του, είναι το υλικό, το λογισμικό και η μεταφορά δεδομένων [1].

Οι συσκευές Διαδικτύου των πραγμάτων είναι ενσωματωμένες (embedded) συσκευές με τη δυνατότητα να εκπέμπουν πληροφορίες μέσω ενός δικτύου με στόχο τη βελτίωση της αλληλεπίδρασης μεταξύ ανθρώπων και άλλων συσκευών. Σημαντικό χαρακτηριστικό των συσκευών Διαδικτύου των πραγμάτων αποτελεί η ικανότητα τους να χρησιμοποιούν πολλούς αισθητήρες για διαφορετικές εφαρμογές. Οι αισθητήρες αυτοί συνήθως συντονίζονται από hubs. Τα hubs είναι συσκευές που παρέχουν ένα κοινό σημείο πρόσβασης που συγκεντρώνει και αποστέλλει τα δεδομένα από όλους τους αισθητήρες που εξυπηρετεί, στο σημείο που γίνεται η επεξεργασία. Με τη χρήση πρωτόκολλων όπως το Inter-Integrated Circuit (I2C) ή το Serial Peripheral Interface (SPI) γίνεται η μεταφορά δεδομένων μεταξύ των αισθητήρων και των εφαρμογών.

Άλλο χαρακτηριστικό του Διαδικτύου των πραγμάτων είναι οι πύλες (gateways). Οι πύλες αποτελούν λογισμικά ή αυτούσιες συσκευές, που συνδέουν τις συσκευές που βρίσκονται στο πεδίο με το cloud και συμπεριφέρονται ως δρομολογητές στο δίκτυο για την εξερχομένη και την εισερχόμενη κίνηση. Με την εξερχόμενη κίνηση μεταφέρονται δεδομένα στο cloud και με την εισερχόμενη κίνηση πραγματοποιούνται λειτουργίες συντήρησης, όπως ενημερώσεις firmware. Επίσης, βοηθά στην ασφάλεια κατά την μεταφορά των δεδομένων. Γίνεται χρήση modem Ethernet, Wi-Fi, 3G/4G/5G για τη σύνδεση του IoT gateway με το cloud και δημιουργείται ένα αμφίδρομο κανάλι επικοινωνίας για την μεταφορά δεδομένων [2]. Αναφορικά, κάποιες από τις σημαντικές λειτουργίες των πυλών είναι:

- Πραγματοποίηση συνδέσεων με παλαιότερου τύπου συσκευές και συσκευές που δεν συνδέονται στο διαδίκτυο.
- Προεπεξεργασία δεδομένων, καθαρισμός, φιλτράρισμα και βελτιστοποίηση
- Προσωρινή αποθήκευση δεδομένων. Αποθήκευση στην προσωρινή μνήμη (buffering) και ροή δεδομένων.
- Συγκέντρωση δεδομένων (aggregation).
- Επικοινωνία M2M (Machine-to-Machine).
- Λειτουργίες δικτύωσης και φιλοξενία δεδομένων σε πραγματικό χρόνο.
- Οπτικοποίηση και ανάλυση δεδομένων.
- Λειτουργίες ασφαλείας κατά την ανταλλαγή δεδομένων.

Βλέπουμε ότι ο ρόλος των πυλών είναι πολύ σημαντικός και η ασφάλεια τους είναι κρίσιμη και αναγκαία καθώς απειλούνται από επιθέσεις.

2.1.3 Πρωτόκολλα/Πρότυπα Διασύνδεσης/Επικοινωνίας συσκευών IoT

Οι κανόνες που καθορίζουν την ανταλλαγή πληροφοριών μεταξύ συσκευών στο Διαδίκτυο των Πραγμάτων είναι τα πρωτόκολλά ή αλλιώς πρότυπα διασύνδεσης και επικοινωνίας, Συγκεκριμένα για τις συσκευές IoT, θα πρέπει να λαμβάνεται υπόψη η ανάγκη για οικονομία ενέργειας. Έτσι η στοίβα πρωτοκόλλου θα πρέπει να διαφέρει από την παραδοσιακή του μοντέλου OSI. Τα πρωτόκολλα επικοινωνίας συσκευών IoT θα πρέπει να είναι μικρά και συμπαγή και η στοίβα τους μπορεί να θεωρηθεί ως μια επαυξημένη έκδοση των επιπέδων της

στοίβας του πρωτοκόλλου TCP/IP [3]. Τα τελευταία χρόνια και εφόσον έχει αναγνωριστεί η ανάγκη για τυποποίηση του αναπτυσσόμενου Διαδικτύου των Πραγμάτων πολλοί πάροχοι υπηρεσίας, δημιουργοί, προγραμματιστές, κ.α. έκαναν προσπάθειες για την δημιουργία τέτοιων προτύπων. Επιπλέον, εξέχοντες οργανισμοί όπως EPC global, European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), και Institute of Electrical and Electronics Engineers (IEEE) συμμετέχουν και ενισχύουν την δημιουργία τους. Τα πρωτόκολλα αυτά μπορούν να κατηγοριοποιηθούν σε τέσσερεις γενικές κατηγορίες: application protocol/πρωτόκολλο εφαρμογής, service discovery protocol/πρωτόκολλο εντοπισμού υπηρεσίας, connectivity and networking protocol/πρωτόκολλο συνδεσιμότητας και δικτύωσης και άλλα κυρίαρχα πρωτόκολλα. Στην εικόνα παρακάτω διακρίνονται αναφορικά οι κατηγορίες και τα πρωτόκολλα που εμπίπτουν σε αυτές. Έπειτα γίνεται μια μικρή αναφορά στα σημαντικότερα πρωτόκολλα.

Broad Category	Dominant Protocols		Functionality
Application protocol	CoAP, DDS, AMQP, MQTT, MQTT-SN, XMPP, HTTP REST		Services to end-users for various applications
Service discovery protocol	mDNS, DNS-SD		Domain name resolution, client pairing for service discovery
Connectivity and networking protocol	Routing protocol	RPL	Routing in low power lossy networks
	Network layer protocol	6LoWPAN, IPv4, IPv6	To provide networking for effective communication in IoT over the existing IPv4 and IPv6 infrastructure
	Data link layer protocol	IEEE 802.15.4	To provide channel access, coordination, scheduling, and resource management tasks.
	Connectivity protocol	LTE-A, EPC global, IEEE 802.15.4, Z-Wave	To interconnect IoT devices at the perception layer for effective communication

nent

Εικόνα 1. Protocols at various layers of IoT architecture with key functionality

Πηγή: https://www.mdpi.com/2071-1050/13/16/9463#B90-sustainability-13-09463

- **CoAP**: Το Constrained Framework Protocol, είναι πρωτόκολλο μεταφοράς όμοιο με το HTTP, σχεδιασμένο για συσκευές με περιορισμένες δυνατότητες. Με αυτό το πρωτόκολλο επιτυγχάνεται η επικοινωνία μεταξύ αυτού του είδους συσκευών και άλλων με υψηλότερες δυνατότητες. Είναι δυαδικό (binary) πρωτόκολλο και κάνει

χρήση του πρωτόκολλου UDP. Έχει μικρότερο overhead, είναι πιο ευέλικτο και μειώνει τις καθυστερήσεις. [2] [4]

- **mDNS**: Το multicast DNS, έχει παρόμοια χρήση με το πρωτόκολλο DNS στο μοντέλο TCP/IP. Καταγράφει τις διευθύνσεις IP και τα ονόματα των συσκευών IoT και τα συσχετίζει, δημιουργώντας έναν πίνακα για αναφορά. Είναι αρκετά ευέλικτο με γρήγορη απόκριση καθώς δεν απασχολεί την τοπική μνήμη και δεν χρειάζεται παραμετροποίηση [2] [5].
- **RPL**: Routing protocols for low power and noisy networks. Αποτελεί παράγοντα για τη δημιουργία τοπολογίας σε lossy συνδέσεις για τη μείωση της ανάγκης δρομολόγησης. [6] Υποστηρίζει μοντέλα point to point, point to multipoint, multipoint to point. [7] [2]
- **6LoWPAN**: IPv6 over Low power Wireless Personal Area. Είναι ένα πρωτόκολλο με χαμηλή κατανάλωση ενέργειας. Καθορίζει μια διεύθυνση IPv6 σε κάθε κόμβο και του επιτρέπει να συνδέεται απευθείας στο διαδίκτυο ανταλλάσσοντας IPv6 πακέτα μέσω του IEEE 802.15.4 και άλλων δικτύων. Προσφέρει πρόσβαση από άκρο σε άκρο χρησιμοποιώντας καθαρά IPv6 διευθύνσεις και έτσι παρέχεται η δυνατότητα για απευθείας σύνδεση σε πολλά είδη δικτύων αλλά και στο διαδίκτυο. Με τις ιδιότητες αυτές επιτρέπει τη σύνδεση αισθητήρων και την πρόσβαση στο διαδίκτυο μέσω τεχνολογιών wide area network (WAN) χαμηλής κατανάλωσης ισχύος όπως το LoRa (Long Range) και το SigFox.
- **IEEE 802.15.4**: Αποτελεί μέρος στοίβας που επιτρέπει την κοινή χρήση μέσου ή καναλιού, δηλαδή Medium Access Control (MAC) sublayer και ενός μέρους φυσικού Physical (PHY) layer για χαμηλού ρυθμού τοπικά/προσωπικά ασύρματα δίκτυα (LR-WPAN). Προσφέρει χαμηλή κατανάλωση σε πόρους επεξεργασίας και ενέργειας και υψηλό throughput με χαμηλό όμως ρυθμό μετάδοσης δεδομένων [8] [2].
- **LTE-A**: Long Term Evolution – Advanced. Είναι βασισμένο στην τεχνολογία επικοινωνίας μέσω κυψελών. Με την εκμετάλλευση του υπάρχοντος εξοπλισμού μειώνεται ραγδαία το κόστος υιοθέτησης του πρωτόκολλου, καθιστώντας το ως την πιο οικονομική λύση για το Διαδίκτυο των Πραγμάτων και παράλληλα προσφέρει καλύτερες επιδόσεις από άλλες λύσεις για το IoT [9].

- **IEEE 1905.1**: Σχεδιάστηκε για να λύσει τις ασυμβατότητες στο Διαδίκτυο των Πραγμάτων. Έχει ως στόχο την ενσωμάτωση των ετερογενή τεχνολογιών με τα ψηφιακά οικιακά δίκτυα. Με αυτό το πρωτόκολλο μπορούν να συνυπάρξουν τα πρωτόκολλα IEEE 802.3, IEEE 802.11, IEEE 1901 και MoCa σε περιβάλλοντα IoT [10].
- **UDP**: User Datagram Protocol. Είναι πρωτόκολλο του επιπέδου μεταφοράς. Δεν δημιουργεί σταθερή σύνδεση, αναφέρεται ως connectionless protocol. Έχουμε τον αποστολέα που στέλνει δεδομένα χωρίς να έχει δημιουργηθεί σύνδεση με τον παραλήπτη. Επιτρέπει την ανταλλαγή μικρότερων πακέτων και παρέχει μικρότερο overhead με λιγότερο χρόνο αφύπνισης ή αλλιώς wake – up time [11].
- **EXI**: Efficient XML Interchange. Αναπτύχθηκε για να υποστηρίξει την χρήση XML σε συσκευές με περιορισμένους πόρους. Χρησιμοποιεί λιγότερο εύρος ζώνης και βελτιστοποιεί την κωδικοποίηση και αποκωδικοποίηση. Η συμπίεση (compression) EXI στοχεύει στη μείωση της χρήσης εγγράφων-αρχείων, δημιουργώντας μικρές ετικέτες βασισμένες στο XML. Το αρχείο αποτυπώνεται σε δυαδική μορφή και όλες οι ετικέτες του κάνουν χρήση κωδίκων στιγμιότυπου (event codes) [2].

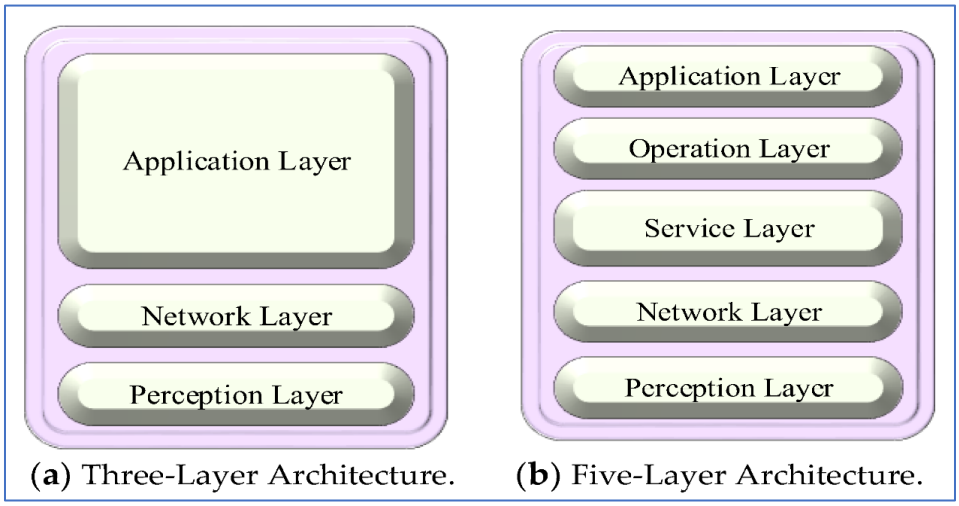
2.1.5 Διαφορές κλασικού διαδικτύου και διαδικτύου των πραγμάτων

Η πρώτη και πιο βασική διαφορά, είναι η διαφορά στις δυνατότητες των συσκευών. Στο κλασικό διαδίκτυο οι συσκευές διαθέτουν υπερβολικές δυνατότητες όπως οι προσωπικοί υπολογιστές οι servers και τα smartphones. Στο διαδίκτυο των πραγμάτων, οι συσκευές είναι περιορισμένων δυνατοτήτων όπως αισθητήρες, RFID tags/readers κ.α. όπου γίνεται χρήση πιο απλοϊκών αλγορίθμων ασφαλείας. Άλλη διαφορά είναι ότι στο διαδίκτυο των πραγμάτων χρησιμοποιούνται λιγότερο ασφαλή πρωτόκολλά gateway για την ασύρματη σύνδεση στο διαδίκτυο όπως Zigbee, 802.15.4e, SigFox, LoRa, και 802.11x το οποίο προκαλεί διαρροή δεδομένων και προβλήματα ασφαλείας. Επίσης μεγάλη διαφορά είναι ότι στο παραδοσιακό διαδίκτυο έχουμε παρόμοια λειτουργικά συστήματα και μορφές δεδομένων, ενώ στο διαδίκτυο των πραγμάτων διακρίνονται μεγάλες διαφορές στους τύπους δεδομένων λόγο των διαφόρων εφαρμογών και του μεγάλου αριθμού λειτουργικών συστημάτων. Εξαιτίας των διαφορών που αναφέραμε, δεν υπάρχει ακόμα κάποιο πρότυπο πρωτόκολλο που να εφαρμόζεται σε όλες τις συσκευές του διαδικτύου των πραγμάτων [12]. Σημαντική διαφορά

μπορούμε να θεωρήσουμε και το γεγονός ότι τα δεδομένα και το περιεχόμενο του κλασικού διαδικτύου παράγονται από αλληλεπιδράσεις ανθρώπων ενώ στον κόσμο του IoT είναι πολύ συχνό φαινόμενο τα δεδομένα που συλλέγονται να παράγονται από έξυπνες συσκευές, όπως αισθητήρες κ.α [1].

2.2 Αρχιτεκτονική / Μοντελοποίηση του Διαδικτύου των Πραγμάτων

Δεν θεωρείται πως υπάρχει κάποιο ευρέως υιοθετημένο πλαίσιο αναφοράς για το Διαδίκτυο των Πραγμάτων [2]. Στη βιβλιογραφία αναφέρονται κυρίως τρία μοντέλα αρχιτεκτονικής για το Διαδίκτυο των Πραγμάτων. Στην παρακάτω εικόνα φαίνονται τα δυο βασικά μοντέλα και τα διάφορα επίπεδα τους. Το μοντέλο τριών επιπέδων αποτελεί ένα από τα πρώτα μοντέλα που προτάθηκαν για το Διαδίκτυο των Πραγμάτων. Παρουσιάζει τα IoT ως μια προέκταση των ασυρμάτων δικτύων αισθητήρων (WSNs) που κάνουν χρήση των εξυπηρετητών νέφους ώστε να προσφέρουν υπηρεσίες στον χρήστη.



Εικόνα 2. Three-layer vs proposed five-layer architecture of IoT

Πηγή: https://www.mdpi.com/2071-1050/13/16/9463#B80-sustainability-13-09463

Το μοντέλο των πέντε επιπέδων [2] [13] αποτελεί μια εναλλακτική που στόχο είχε να καταστήσει δυνατές τις αλληλεπιδράσεις μεταξύ διαφόρων τομέων μιας επιχείρησης κατακερματίζοντας τα πολύπλοκα συστήματα της σε απλούστερες εφαρμογές με περισσότερο εμφανή μέρη. Το 2014 η Cisco πρότεινε μια προέκταση για τα παραδοσιακά μοντέλα τριών και πέντε επιπέδων. Το νέο μοντέλο αποτελείται από επτά επίπεδα, η ροή των δεδομένων

συνήθως είναι αμφίδρομη και ποια κατεύθυνση υπερτερεί συνήθως εξαρτάται από το είδος της εφαρμογής. Για παράδειγμα σε ένα σύστημα ελέγχου, τα δεδομένα κατευθύνονται από την κορυφή του μοντέλου (application level) προς τη βάση (Edge node level). Αντιθέτως σε ένα σύστημα καταγραφής, η ροή έχει κατεύθυνση από κάτω προς πάνω.

2.2.1 Μοντέλο τριών επιπέδων

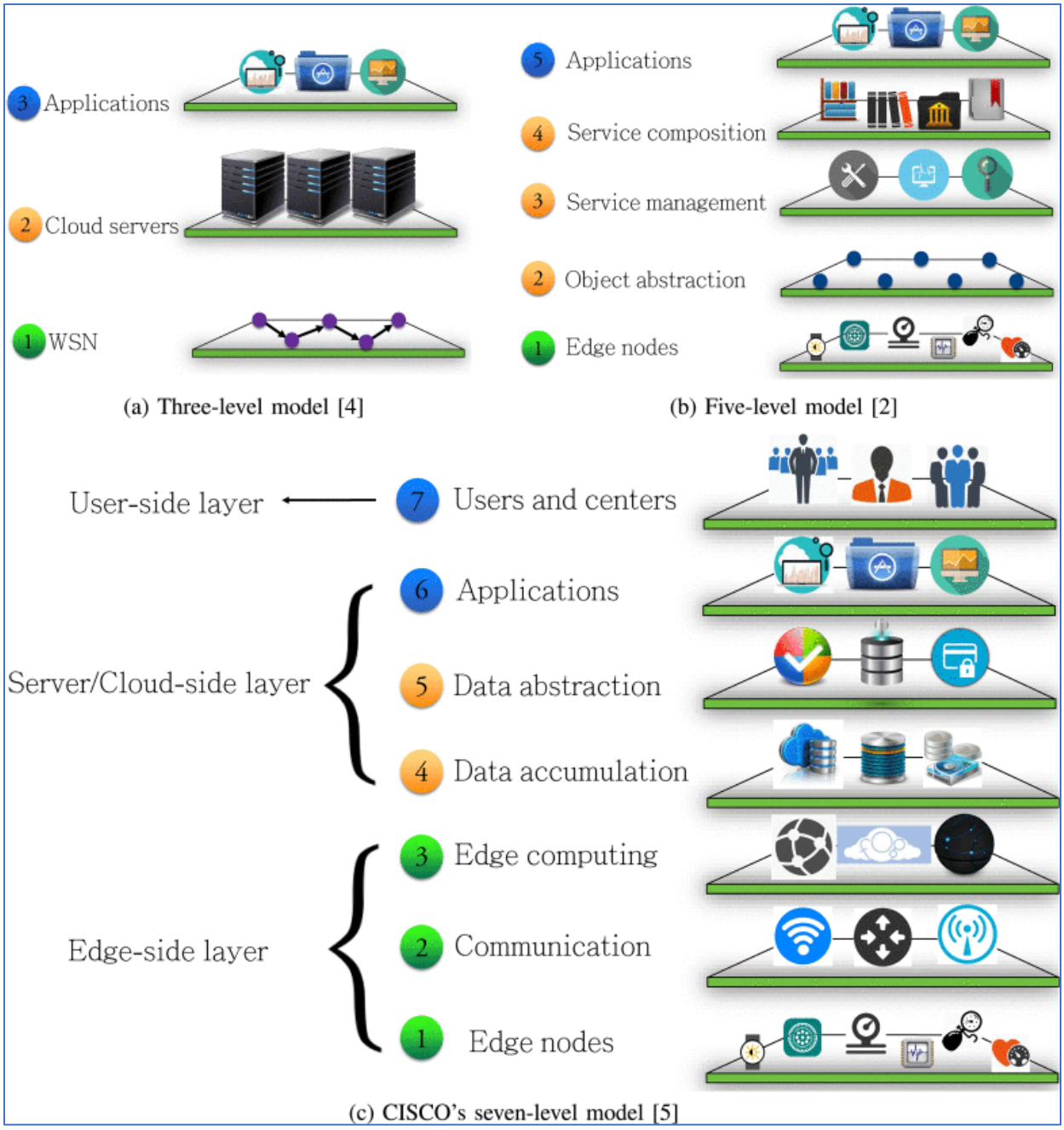
Το βασικότερο μοντέλο αρχιτεκτονικής που μπορούμε να πούμε ότι ακολουθείται περισσότερο είναι αυτό που αποτελείται από τρία επίπεδα. Από το επίπεδο αντίληψης (perception layer), το επίπεδο δικτύου (network layer) επίπεδο εφαρμογής (application layer).

- **Επίπεδο Αντίληψης ή αλλιώς Φυσικό επίπεδο (Perception layer)**: Αυτό το επίπεδο ασχολείται με τους αισθητήρες στο Διαδίκτυο των Πραγμάτων. Αισθητήριοι κόμβοι, αισθητήρες RFID, και άλλες τεχνολογίες αισθητήρων. Αυτοί οι αισθητήρες συλλέγουν τα δεδομένα όπως, υγρασία, θερμοκρασία, πίεση, ήχους κ.α. πραγματοποιούν μια προεπεξεργασία και τα προωθούν στο επίπεδο δικτύου. Άρα στο επίπεδο αυτό αποδίδουμε την συλλογή και την προώθηση των δεδομένων.
- **Επίπεδο Δικτύου (Network Layer):** Στο επίπεδο αυτό συναντούμε τα μέρη του δικτύου που επιτρέπουν την επικοινωνία. Εδώ λαμβάνει μέρος η ανταλλαγή δεδομένων μεταξύ των συσκευών του Διαδικτύου των Πραγμάτων. Συνδέει το φυσικό επίπεδο με το επίπεδο εφαρμογής. Ο ρόλος του είναι να διευθύνει και να καθοδηγεί τα δεδομένα που αποκτήθηκαν από το φυσικό επίπεδο. Τα δεδομένα αποστέλλονται μέσω του διαδικτύου σε άλλα υπολογιστικά συστήματα η σε IoT hubs.
- **Επίπεδο Εφαρμογής (Application layer):** Αποτελεί το ανώτερο επίπεδο. Αντλεί δεδομένα από το επίπεδο δικτύου και χρησιμοποιείται ως υπηρεσία για να εξυπηρετήσει τον σκοπό του χρήστη. Έχει το ρόλο να εξυπηρετεί και να προωθεί τα μηνύματα των εφαρμογών. Αποτελεί μια γεφύρωση μεταξύ των εφαρμογών και των χρηστών. Ορίζει την κατανομή των πόρων για την επεξεργασία και την διαλογή δυνατοτήτων. Είναι πελατοκεντρικό επίπεδο και υλοποιεί υψηλού επιπέδου έξυπνες εργασίες για τους χρήστες ανάλογα με τις προτιμήσεις τους [2].

2.2.2 Μοντέλο πέντε επιπέδων

Εκτός από το κλασσικό μοντέλο των τριών επιπέδων, αργότερα αναπτύχθηκε ένα μοντέλο με πέντε επίπεδα που αποσυνθέτει περεταίρω αυτό των τριών. Αποτελείται από το επίπεδο αντίληψης (perception layer), το επίπεδο δικτύου (network layer), το επίπεδο υπηρεσίας (service layer), το επίπεδο λειτουργίας (operation layer) και το επίπεδο εφαρμογής (application layer). Το επίπεδο εφαρμογής έχει διαχωριστεί σε τρία επίπεδα, το επίπεδο υπηρεσίας, λειτουργίας και εφαρμογής.

- **Επίπεδο Υπηρεσίας (Service layer):** Στο επίπεδο αυτό έχουμε την χρήση των ετερογενή συσκευών IoT όπως εργαλεία, πλατφόρμες και τους πειραματισμούς για μεγάλο εύρος εφαρμογών. Επίσης αναλαμβάνει και την κρίσιμη επεξεργασία του τεράστιου όγκου δεδομένων του επιπέδου δικτύου.
- **Επίπεδο Λειτουργίας (Operation layer):** Αποτελεί το επίπεδο που δημιουργούνται τα επιχειρηματικά πλάνα του Διαδικτύου των Πραγμάτων και η οπτικοποίηση των δεδομένων, όπως και το σημείο που λαμβάνονται αποφάσεις κ.α. Έχει την ευθύνη για την παροχή ποιότητας υπηρεσίας (QoS) σε όλα τα επίπεδα. Σε αυτό το επίπεδο, πραγματοποιείται παρακολούθηση σε πραγματικό χρόνο, έλεγχοι και αξιολογήσεις των διαφόρων παραμέτρων που αφορούν τις εφαρμογές Διαδικτύου των Πραγμάτων.
- **Επίπεδο Εφαρμογής (Application layer):** Ο πρωτεύον ρόλος αυτού του επιπέδου είναι να παρέχει υπηρεσίες, που αφορούν τις εφαρμογές, στους τελικούς χρήστες. Μέσα στο τεράστιο εύρος εφαρμογής του Διαδικτύου των Πραγμάτων, έξυπνες πόλεις, έξυπνα σπίτια, έξυπνη γεωργία, industry 4.0, υπηρεσίες υγείας, παρακολούθηση περιβάλλοντος κ.α., αυτό είναι το επίπεδο που αλληλεπιδρούν οι τελικοί χρήστες ώστε να κάνουν χρήση της υπηρεσίας.



Εικόνα 3. Three IoT reference models

Πηγή https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6245516/8128656/7562568/mosen1-2606384-large.gif

2.2.3 Μοντέλο επτά επιπέδων

Επίπεδο Αντίληψης (Perception Layer/Edge devices): Το πρώτο επίπεδο κατά κύριο λόγο αποτελείται από υπολογιστικούς κόμβους (computing nodes), όπως για παράδειγμα έξυπνοι ελεγκτές, αισθητήρες, RFID readers κ.α. Από αυτό το επίπεδο και πάνω πρέπει να λαμβάνεται υπόψη η εμπιστευτικότητα και η ακεραιότητα.

Επίπεδο Επικοινωνίας (Abstraction Layer/Communication): Αυτό το επίπεδο αποτελείται από τα μέρη που επιτρέπουν τη μετάδοση της πληροφορίας και των εντολών. Αναφορικά, έχουμε επικοινωνία μεταξύ συσκευών στο πρώτο επίπεδο, μεταξύ των μερών του δεύτερου επιπέδου και μεταξύ του πρώτου και του τρίτου επιπέδου.

Επίπεδο Δικτύου (Network Layer/Edge computing): Το Edge computing ή αλλιώς Fog computing, είναι το επίπεδο όπου ξεκινά η επεξεργασία των δεδομένων. Αυτό εξασφαλίζει τη μείωση του βάρους εργασίας που θα αντιμετωπίσουν τα πάνω επίπεδα αλλά παράλληλα βελτιώνει την απόκριση. Οι περισσότερες εφαρμογές πραγματικού χρόνου πραγματοποιούν υπολογισμούς όσο πιο κοντά στο άκρο του δικτύου γίνεται. Το μέγεθος των υπολογισμών σε αυτό το επίπεδο εξαρτάται από τον πάροχο της υπηρεσίας, τους servers και τους υπολογιστικούς κόμβους. Συνήθως πραγματοποιούνται υπολογισμοί επεξεργασίας σημάτων και αλγορίθμων εκμάθησης.

Επίπεδο Μεταφοράς (Transport Layer/Data accumulation): Το μεγαλύτερο μέρος των εφαρμογών δεν απαιτούν επεξεργασία δεδομένων. Σε αυτό το επίπεδο πραγματοποιείται η αποθήκευση των δεδομένων για μελλοντική ανάλυση ή για διαμοιρασμό με υψηλού επιπέδου υπολογιστικούς server. Πραγματοποιείται η μετατροπή του τύπου δεδομένων, από πακέτα δικτύου σε πίνακες βάσης δεδομένων. Παράλληλα μειώνεται ο όγκος δεδομένων μέσα από φιλτράρισμα και επιλεκτική αποθήκευση. Αποφασίζεται επίσης αν τα δεδομένα είναι χρήσιμα για τα ανώτερα επίπεδα.

Επίπεδο Υπολογισμού (Computing Layer/Data abstraction): Αυτό το επίπεδο δίνει τη δυνατότητα να μετατραπούν και να αποθηκευτούν τα δεδομένα με τέτοιο τρόπο ώστε η επεξεργασία τους να γίνεται με πιο απλό και αποδοτικό τρόπο. Σε αυτό το επίπεδο

πραγματοποιούνται η κανονικοποίηση, αποκανονικοποίηση, δημιουργία καταλόγου και η συγχώνευση των δεδομένων.

Επίπεδο Λειτουργίας(Operation Layer/Applications): Το επίπεδο εφαρμογής προσφέρει ερμηνεία της πληροφορίας, όπου το λογισμικό συνεργάζεται με τα επίπεδα συσσώρευσης δεδομένων (data accumulation) και αφαίρεσης δεδομένων (data abstraction). Οι εφαρμογές του Διαδικτύου των Πραγμάτων είναι πολλές και ποικίλλουν μεταξύ των διαφόρων αγορών και βιομηχανικών αναγκών.

Επίπεδο Εφαρμογής (Application Layer/Users and centers): Σε αυτό το υψηλότερο επίπεδο του Διαδικτύου των Πραγμάτων βρίσκονται οι χρήστες, όπου χρησιμοποιούν τις εφαρμογές και τα δεδομένα τους [13].

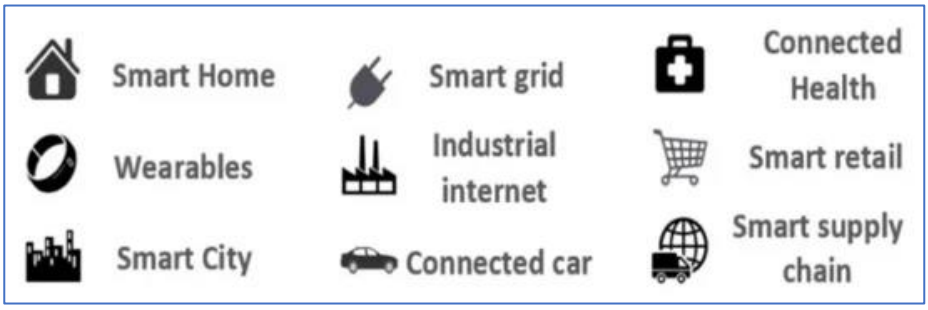
Αναφορικά, **το μοντέλο τεσσάρων επιπέδων** αποτελείται από το επίπεδο αντίληψης (Perception Layer), το επίπεδο δικτύου (Networking/Transparent Layer), το επίπεδο middleware (Service/management Layer) και το επίπεδο εφαρμογών (Application Layer). Το επίπεδο αντίληψης αποτελείται από αισθητήρες και μηχανισμούς ενεργοποίησης. Από το επίπεδο αυτό τα μη επεξεργασμένα δεδομένα δρομολογούνται στο επίπεδο του δικτύου. Έπειτα από εκεί, μετά από την επεξεργασία τους δρομολογούνται μέσω της υποδομής του δικτύου. Εκεί αναλαμβάνει το επίπεδο middleware την επιπλέον επεξεργασία και δίνει την δυνατότητα να γίνουν οι διάφορες προκαθορισμένες ενέργειες και λειτουργίες της κάθε ανεξάρτητης εφαρμογής που θα εκτελεστεί στο επίπεδο εφαρμογών. Το επίπεδο εφαρμογών είναι αυτό που δίνει τη δυνατότητα σε ανεξάρτητους δημιουργούς να δημιουργούν και να εκτελούν τις εφαρμογές τους, που αποθηκεύουν και επεξεργάζονται επιπλέον τα δεδομένα της συσκευής [14].

2.3 Εφαρμογές Διαδικτύου των Πραγμάτων

Το Διαδίκτυο των Πραγμάτων είναι μέρος της καθημερινής μας ζωής [1], μέσα από συσκευές καταγραφής ασφαλείας, έξυπνα ρολόγια, συσκευές καταγραφής άσκησης, έως και πολύπλοκες εφαρμογές όπως αυτόνομα οχήματα και ασύρματες συσκευές – αισθητήρες σώματος (WBAN) και ασύρματων ιατρικών αισθητήρων (MWSN). Πρακτικά έχουν κατακλύσει

την αγορά και έχουν διεισδύσει σε κάθε πιθανό τομέα της ζωής μας, από τα σπίτια, τις εταιρείες, τους δρόμους, τις πόλεις και τα σώματα μας.

Η έκταση που έχουν καλύψει οι συσκευές του διαδικτύου στην καθημερινότητα μας είναι κάτι που μπορούμε να αντιληφθούμε εύκολα απλά κοιτώντας το περιβάλλον που βρισκόμαστε. Οι εφαρμογές του είναι αμέτρητες και αφορούν κάθε τομέα της ζωής μας. Τα έξυπνα σπίτια και κτήρια, τα ηλεκτρονικά βοηθήματα υγείας και τα έξυπνα οχήματα είναι μόνο μερικές από τις εφαρμογές αυτές. Παρόλα αυτά, οι προοπτικές για περεταίρω εξέλιξη είναι πολλές και δεν πλησιάζεται καν το σημείο εξάντλησής τους. Το Διαδίκτυο των Πραγμάτων μας δίνει τη δυνατότητα να συνδυάσουμε την χρήση αισθητήρων, την επικοινωνία, τη δικτύωση, την πιστοποίηση, την ταυτοποίηση, την υπολογισιμότητα και άλλες πολλές υπηρεσίες που επιθυμούμε, όπως η πρόσβαση σε πληροφορίες από κάθε έξυπνο αντικείμενο οποιαδήποτε στιγμή. Θα περιγράψουμε στη συνέχεια ορισμένες από τις κυριότερες εφαρμογές του Διαδικτύου των Πραγμάτων [13].



Εικόνα 4. Forms of IoT

Πηγή: https://www.mdpi.com/computers/computers-09-00008/article_deploy/html/images/computers-09-00008-g001-550.jpg

1) **Έξυπνα οχήματα:** Τα έξυπνα οχήματα αποτελούν την εξέλιξη του παραδοσιακού τρόπου μετακίνησης. Συστήματα βασισμένα στο Διαδίκτυο των Πραγμάτων δίνουν δυνατότητες στα οχήματα όπως απομακρυσμένους χειρισμούς (κλείδωμα/ξεκλείδωμα), λήψη πληροφοριών διαδρομής, πληροφορίες για την κίνηση κ.α. Επίσης αξίζει να αναφέρουμε ότι τα οχήματα με πρόσβαση στο διαδίκτυο προσφέρουν περισσότερη ασφάλεια.
2) **Έξυπνα κτήρια:** Τα έξυπνα κτήρια και σπίτια επιτρέπουν την αποτελεσματική διαχείριση ενέργειας. Μέσα από την εκμετάλλευση συσκευών IoT, όπως έξυπνοι θερμοστάτες με

ενσωματωμένους αισθητήρες που κάνοντας χρήση αλγορίθμων ανάλυσης δεδομένων, βοηθούν στη θέρμανση η την ψύξη στα επιθυμητά επίπεδα. Ακόμη, συναντούμε ελεγκτές που μεταβάλουν τον φωτισμό, σύμφωνα με τις ανάγκες των χρηστών. Οι διάφορες συσκευές που συναντούμε στα περισσότερα κτήρια/σπίτια όπως ψυγεία, τηλεοράσεις και συστήματα ασφαλείας όπως κάμερες κ.α. πλέον είναι κατά το πλείστων συνδεμένα στο διαδίκτυο και διαθέτουν δική τους μονάδα επεξεργασίας. Με αυτές τις δυνατότητες, οι συσκευές πλέον μπορούν να εκτελούν απομακρυσμένες εντολές και να επηρεάζουν το γύρο περιβάλλον και την ποιότητα ζωής.

3) **Παρακολούθηση/επίβλεψη υγείας:** Οι τελευταίες εξελίξεις στον τομέα των βιοϊατρικών αισθητήριων, της επεξεργασίας σημάτων, των συσκευών χαμηλής κατανάλωσης ενέργειας και της ασύρματης επικοινωνίας έχουν φέρει επανάσταση στις επιστήμες υγείας. Βλέπουμε να εμφανίζονται συσκευές Διαδικτύου των πραγμάτων με δυνατότητες μακράς καταγραφής ζωτικών πληροφοριών υγείας και συστήματα χορήγησης φαρμάκων, όπου οι τιμές των οργανικών λειτουργιών, σε μορφή σημάτων, καταγράφονται και αποθηκεύονται για μελλοντική χρήση. Αυτές οι δυνατότητες αποτελούν μια θεμελιώδη αλλαγή στην επιστήμη της υγείας [15]. Οι έξυπνες αυτές συσκευές έχουν διαδοθεί επίσης και στον τομέα της φυσικής αγωγής, της σωστής δίαιτας και του υγιεινού τρόπου ζωής. Ακόμη, υπάρχουν εξελίξεις και στην περιοχή της πρόγνωσης ασθενειών.
4) **Διαχείριση ενέργειας:** Το Διαδίκτυο των Πραγμάτων κάνοντας χρήση των ενσωματωμένων αισθητήρων και των εξαρτημάτων ενεργοποίησης, παρέχουν την δυνατότητα για την βέλτιστη κατανάλωση ενέργειας. Με τις συσκευές όπως λάμπες, πρίζες, έξυπνες τηλεοράσεις, έξυπνα πλυντήρια, έξυπνα ψυγεία κ.α. απομακρυσμένου χειρισμού, μπορούν να μοιραστούν πληροφορίες με παρόχους ενέργειας για να βελτιώσουν την κατανάλωση ενέργειας στα έξυπνα σπίτια. Με αυτές τις συσκευές ο χρήστης έχει τη δυνατότητα να τα χειριστεί με τρόπο που του παρέχουν άνεση, ευκολία, αλλά και να προγραμματίσει τη λειτουργία τους για να μειώσει την ενεργειακή κατανάλωση.
5) **Διαχείριση κατασκευής υποδομών:** Η παρακολούθηση και η διαχείριση των μοντέρνων υποδομών, όπως γέφυρες, γραμμές τραίνων, κτήρια, φανάρια κυκλοφορίας, είναι

σημαντικές εφαρμογές του Διαδικτύου των Πραγμάτων. Το Διαδίκτυο των πραγμάτων παρέχει τη δυνατότητα να ελέγχει απότομες αλλαγές στις δομικές συνθήκες που μπορούν να οδηγήσουν σε ρίσκα ασφαλείας. Επίσης επιτρέπει σε κατασκευαστικές εταιρίες και εταιρίες συντήρησης να κοινοποιήσουν πληροφορίες για τα σχέδια τους.

6) **Καταγραφή/παρακολούθηση του περιβάλλοντος:** Εδώ μπορεί να φανεί χρήσιμο το Διαδίκτυο των Πραγμάτων με τη χρήση ενσωματωμένων αισθητήρων. Οι αισθητήρες αυτοί παρακολουθούν τις συνθήκες στο περιβάλλον και αναγνωρίζουν επείγουσες καταστάσεις όπως πυρκαγιές, πλημύρες, παγετούς κ.α. Ακόμη παρέχουν δυνατότητα για τον έλεγχο της ποιότητας του αέρα και του νερού αλλά και το ποσοστό υγρασίας και θερμοκρασίας στον περιβάλλοντα χώρο.
7) **Διαχείριση γραμμής παραγωγής και συναρμολόγησης:** Έξυπνα συστήματα που βασίζονται στο Διαδίκτυο των Πραγμάτων, επιτρέπουν την ταχεία κατασκευή και συναρμολόγηση νέων προϊόντων. Τα συστήματα αυτά αποτελούν αισθητήρες και συσκευές παρακολούθησης/καταγραφής που αλληλεπιδρούν. Επιπρόσθετα άλλο ένα προτέρημα της χρήσης τους είναι η βελτίωση της κατανάλωσης ενέργειας και της ασφάλειας.
8) **Αλυσίδα εφοδιασμού τροφίμων:** Σε ένα τόσο πολύπλοκο και διαμοιρασμένο μοντέλο παραγωγής όπως αυτό της αλυσίδας παραγωγής τροφίμων το Διαδίκτυο των Πραγμάτων μπορεί να συλλέξει σημαντικές πληροφορίες για τους διαχειριστές και να διασφαλίσει την προστασία και τη σωστή λειτουργία των μηχανισμών, την απασχόληση του προσωπικού και την ασφάλεια των προϊόντων. Οι συσκευές αυτές μπορούν να προβλέπουν και να προειδοποιούν σε περιπτώσεις βλάβης, μη ορθής λειτουργίας και μη εξουσιοδοτημένης ενέργειας σε οποιοδήποτε σημείο της αλυσίδας παραγωγής.

3. Ασφάλεια στο Διαδίκτυο των Πραγμάτων

Πριν την εμφάνιση του Διαδικτύου των Πραγμάτων οι απειλές που συναντούσε κανείς περιορίζονταν στην κλοπή χρημάτων και πνευματικής ιδιοκτησίας. Πλέων με την εμβέλεια που έχει αποκτήσει η χρήση εφαρμογών του διαδικτύου των πραγμάτων αλλά και με την κρισιμότητα των εφαρμογών που κάνουν χρήση της τεχνολογίας μπορεί να οδηγήσουν σε απώλεια ζωής, εισβολές σε κρίσιμες υποδομές όπως πυρηνικά, δίκτυο ηλεκτρισμού και υπηρεσίες εθνικής ασφάλειας [16]. Άρα η ασφάλεια καθίσταται ουσιώδεις και αναγκαία. Δημιουργείται λοιπόν η ανάγκη για την εξασφάλιση της ορθής λειτουργίας. Ορθή λειτουργία μπορούμε να ορίσουμε την λειτουργία που εγγυάται την συνεχή διαθεσιμότητα, την εμπιστευτικότητα, την ακεραιότητα, την εξάλειψη περίπτωσης άρνησης εξυπηρέτησης, την ιδιωτικότητα και την αυθεντικοποίηση. Παρατηρούμε ότι τα κενά είναι πολλά και παρουσιάζεται μεγάλη ανάγκη για ένα γενικό πλαίσιο ασφάλειας και δημιουργία προτύπων του Διαδικτύου των Πραγμάτων. Για να ανακαλύψουμε τις απειλές και να εξασφαλίσουμε την άμεση αντίδραση θα πρέπει να υπάρχουν καθορισμένες οδηγίες και πρακτικές. Προτείνεται να ερευνηθούν οι πρακτικές από οργανισμούς όπως, Cisco, TCG, IBM Watson IoT και AT&T για ένα ενοποιημένο πλαίσιο ασφάλειας στο διαδίκτυο των πραγμάτων [12].

3.1 Προϋποθέσεις για Ασφάλεια

Για την βασική ή αλλιώς τυπική ασφάλεια, είτε αφορά τις συσκευές είτε το δίκτυο ή ακόμη και τον ίδιο τον χρήστη, πρέπει να πληρούνται κάποιες προϋποθέσεις. Αυτές οι βασικές προϋποθέσεις είναι και αυτές που αναλογικά χρησιμεύουν περισσότερο, καθώς οι περισσότεροι κίνδυνοι για τις συσκευές διαδικτύου των πραγμάτων είναι σχετικά απλοϊκοί και έχουν στόχο την διείσδυση και την απόκτηση ευαίσθητων η και όχι πληροφοριών ή την μεταπήδηση σε άλλο κόμβο του δικτύου μέσω προσβεβλημένης συσκευής [17].

Στον τομέα του Διαδικτύου των Πραγμάτων ασχολούμαστε κυρίως με δυο όρους, τον όρο ασφαλές πράγμα και τον όρο επίθεση ασφάλειας [13]. Είναι σημαντικό να γνωρίζουμε τα χαρακτηριστικά που ορίζουν την ασφάλεια ώστε να μπορέσουμε να ορίσουμε το ασφαλές πράγμα. Οι προϋποθέσεις για ασφάλεια μπορούν να αναλυθούν σε τρεις κατηγορίες:

εμπιστευτικότητα (confidentiality), **ακεραιότητα** (integrity), **διαθεσιμότητα** (availability) εν συντομία CIA [13].

Η **εμπιστευτικότητα (confidentiality)** θέτει κανόνες για να εμποδίσει τη μη εξουσιοδοτημένη πρόσβαση σε συγκεκριμένα δεδομένα, κυρίως σε συσκευές Διαδικτύου των Πραγμάτων που χειρίζονται ιατρικά δεδομένα και δεδομένα που περιέχουν απόρρητες πληροφορίες.

Με την **ακεραιότητα (integrity)** εξασφαλίζουμε την αξιοπιστία της υπηρεσίας όταν η συσκευή κάνει έλεγχο των δεδομένων και εντολών που δέχεται και είναι νόμιμες, από αξιόπιστες πηγές. Δίχως αυτούς τους ελέγχους θα υπήρχε κίνδυνος για επιθέσεις όπου μπορούν να προκαλέσουν σοβαρές επιπτώσεις. Τέλος, για ένα σύστημα συσκευών του Διαδικτύου των Πραγμάτων είναι απαραίτητο να διασφαλίσουμε την **διαθεσιμότητα (availability)** ώστε να υπάρχει αδιάκοπη επικοινωνία και ανταλλαγή δεδομένων μεταξύ κρίσιμων συσκευών του δικτύου. Αν κάποιο στοιχείο από τα τρία που αναφέραμε δεν εξασφαλιστεί, τότε τίθεται το θέμα της ανεπάρκειας [18]. Οι Cherdantseva et al. μας δείχνουν ότι η τριάδα CIA δεν λαμβάνει υπόψιν νέες απειλές που προκύπτουν. Έτσι παρουσιάζουν μια νέα λίστα από προϋποθέσεις για ασφάλεια. Έπειτα από ανάλυση πολλών κριτηρίων καταλήγουν στην οκτάδα - IAS όπου και προτάθηκε ως επέκταση της τριάδας – CIA. Στον παρακάτω πίνακα βλέπουμε τη λίστα IAS.

Requirement	Definition	Abbreviations
Confidentiality	Ensuring that only authorized users access the information	C
Integrity	Ensuring completeness, accuracy, and absence of unauthorized data manipulation	I
Availability	Ensuring that all system services are available, when requested by an authorized user	A
Accountability	An ability of a system to hold users responsible for their actions	AC
Auditability	An ability of a system to conduct persistent monitoring of all actions	AU
Trustworthiness	An ability of a system to verify identity and establish trust in a third party	TW
Non-repudiation	An ability of a system to confirm occurrence/non-occurrence of an action	NR
Privacy	Ensuring that the system obeys privacy policies and enabling individuals to control their personal information	P

Εικόνα 5. Security Requirements

Πηγή: https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6245516/8128656/7562568/mosen.t1-2606384-large.gif

3.1.1 Επίπεδο Δεδομένων

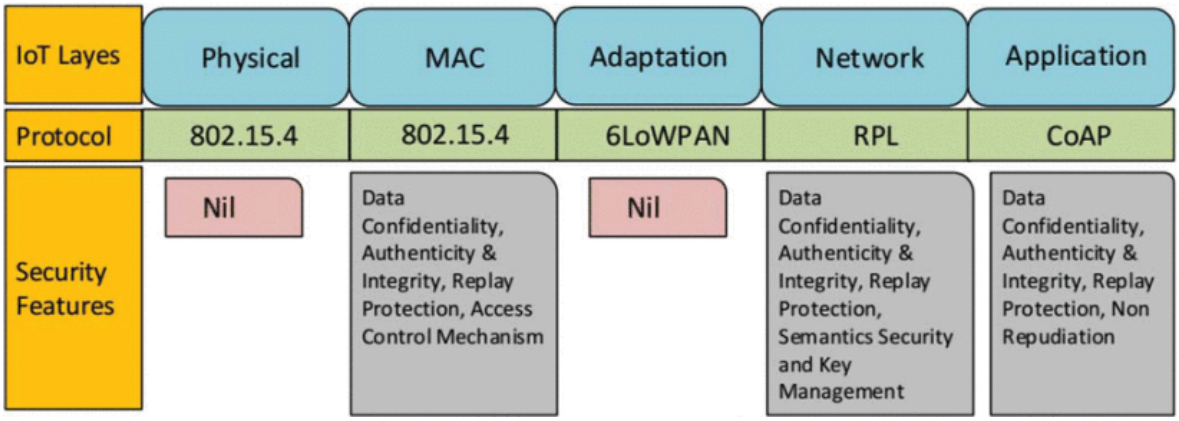
Το επίπεδο δεδομένων [17] είναι αυτό που θα διασφαλίσει την ακεραιότητα του διαμοιρασμού (αποστολή - λήψη) των δεδομένων. Πρέπει να εξασφαλίζεται η ανωνυμία της προέλευσης των δεδομένων όπως και η εμπιστευτικότητα, ώστε να αποφευχθούν λήψεις από τρίτους.

3.1.2 Επίπεδο Πρόσβασης

Σε αυτό το επίπεδο βρίσκουμε τους μηχανισμούς που χειρίζονται την πρόσβαση στο δίκτυο. Πρώτος και βασικός μηχανισμός είναι οι εφαρμογές ελέγχου πρόσβασης (access controls), όπου ελέγχουν και φιλτράρουν την πρόσβαση στο δίκτυο. Έπειτα βρίσκουμε τον μηχανισμό πιστοποίησης των συσκευών (Authentication), όπου ανάλογα τον κατασκευαστή και την αρχιτεκτονική του δικτύου συγκρίνουν τα πιστοποιητικά της συσκευής και αν υπάρχει το δικαίωμα να συνδεθεί η συσκευή. Τέλος, η εξουσιοδότηση δικαιωμάτων (Authorization) θα παραχωρήσει τα δικαιώματα χρήσης στους χρήστες και τις συσκευές του δικτύου [17].

3.1.3 Επίπεδο Λειτουργικότητας

Το επίπεδο αυτό συμβάλει στην ασφάλεια με την αναγνώριση της ανθεκτικότητας του δικτύου, αλλά και την ικανότητα να αναπροσαρμόζεται μετά από αλλαγές ώστε να μένει λειτουργικό και απρόσβλητο [17].



Εικόνα 6. Σύνοψη προϋποθέσεων ασφάλειας των βασικών κατηγοριών εφαρμογών IoT .

Πηγή: https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6488907/9219268/9099839/abbas.t3-2997651-large.gif

IoT APPLICATIONS	Availability	Confidentiality	Integrity	Non -Repudiation	Privacy	Authentication
Smart Grids	✓	✓	✓	✓	✓	X
Healthcare	X	✓	✓	X	✓	✓
Transportation Systems	✓	X	X	✓	✓	✓
Smart Cities	✓	✓	✓	X	X	✓
Smart Manufacturing	✓	✓	✓	X	X	✓
Smart Homes	✓	✓	✓	X	X	✓
Smart Wearables	X	✓	✓	X	✓	✓
Smart Farming	✓	X	X	X	X	✓
Smart Supply Chain	✓	✓	✓	X	✓	✓
Smart Security Systems	✓	✓	✓	X	✓	✓

Εικόνα 7. Security features offered by IoT communication protocols.

Πηγή: https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6488907/9219268/9099839/abbas5-2997651-large.gif)

4. Κίνδυνοι και Προκλήσεις στο Διαδίκτυο των Πραγμάτων

Οι περισσότερες συσκευές IoT έχουν ως κοινό στοιχείο την απλή σχεδίαση που παρέχει γρήγορη και απλή λειτουργία. Η κάθε συσκευή της καθημερινότητας μπορεί να μετατραπεί σε συσκευή IoT, απλά προσθέτοντας τη δυνατότητα να συνδεθεί στο διαδίκτυο [1]. Σε πολλές περιπτώσεις οι συσκευές IoT δεν πληρούν ούτε τους βασικούς κανόνες ασφαλείας κινδυνεύοντας να προσβληθούν η να γίνουν μέσο προσβολής άλλων συσκευών. Έχουμε φτάσει στο σημείο όπου η αποδοχή των συσκευών του διαδικτύου των πραγμάτων είναι μεγάλη και η επένδυση και κατασκευή τέτοιων συσκευών από μεγάλες και γνωστές εταιρείες προσδίδουν μια ψευδαίσθηση ασφάλειας στον καταναλωτή. Αυτό σε συνδυασμό με τον κατακλυσμό της αγοράς με τεράστιο αριθμό συσκευών αμφιβόλου ποιότητας που εμφανίζουν συνήθως μεγάλη απόκλιση στην τιμή ικανοποιώντας όμως τις ίδιες λειτουργίες, αφήνουν τον καταναλωτή ευάλωτο [17]. Χωρίς την κατάλληλη κατάρτιση και πολλές φορές με άγνοια του κινδύνου ο χρήστης κοινοποιεί πληροφορίες ζωτικής σημασίας σε τρίτα πρόσωπα και παραχωρεί άδειες διαχείρισης προσωπικών δεδομένων με μεγάλη ευκολία.

Κατά κύριο λόγο αυτά αφορούν τον απλό καταναλωτή που κάνει χρήση συσκευών για προσωπικούς λόγους,. Υπάρχει όμως και η περίπτωση που ο χρήστης - καταναλωτής είναι μια μεγάλες εταιρίες, εργοστάσια, βιομηχανίες, κοινότητες, δήμοι ακόμη και κράτη. Εκεί οι ανάγκες και το ρίσκο είναι μεγαλύτερο όπως και το ενδιαφέρον για εξασφάλιση της καλής λειτουργίας της αξιοπιστίας και της ασφάλειας.

Είναι ευνόητο ότι με τη διασύνδεση και την επικοινωνία των συσκευών στο διαδίκτυο ελλοχεύουν κίνδυνοι που πηγάζουν από κακόβουλες ενέργειες η από κακή σχεδίαση λογισμικού ή αρχιτεκτονικής δικτύου ή ακόμη και από κακή συντήρηση συσκευών που αποτελούν το δίκτυο που λειτουργούν οι συσκευές. Οι κίνδυνοι αυτοί μπορούν να χωριστούν σε κατηγορίες ανάλογα με το επίπεδο δικτύου όπου συναντώνται, με το είδος συσκευής που προσβάλουν, την αρχιτεκτονική και το είδος του δικτύου που προσβάλουν, το αποτέλεσμα που επιδιώκει ο θύτης κ.α.

4.1 Ευπάθειες

Ονομάζουμε ευπάθεια, κάθε ελάττωμα στη σχεδίαση ενός πλαισίου (framework) που το καθιστά χρήσιμο για κάποιον θύτη και του επιτρέπει να εκτελεί εντολές, να αποκτά μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες και να εκτελεί επιθέσεις DDoS. Οι θύτες μπορούν να εκμεταλλευτούν τα προβλήματα των συσκευών του Διαδικτύου των Πραγμάτων ώστε να εισβάλουν σε δίκτυα. Από επιθέσεις που υλοποιούνται με την επανασύνδεση DNS, που επιτρέπουν την αποκόμιση πληροφοριών σε εσωτερικά δίκτυα έως και επιθέσεις side – channel, όπως αυτές που εισάγονται με λέιζερ υπέρυθρων σε έξυπνες συσκευές στα σπίτια και σε περιβάλλοντα εργασίας. Αυτά και άλλα πολλά, αποτελούν ευπάθειες στο Διαδίκτυο των Πραγμάτων και μπορούν να εντοπιστούν σε διάφορα μέρη των συστημάτων [2].

Ας δούμε τα δυο κεντρικά μέρη των δομών του Διαδικτύου των Πραγμάτων, το υλικό και το λογισμικό. Βρίσκονται εκτεθειμένα σε σχεδιαστικά σφάλματα. Στην προσπάθεια για δημιουργία σύνδεσης διαφορετικών συσκευών, αναγνωρίζονται πολλά σφάλματα και ξεκινά η επίλυση τους. Όσον αφορά τα ελαττώματα υλικού, δύσκολα αναγνωρίζονται και δυσκολότερα επιλύονται. Σφάλματα επίσης μπορούμε να συναντήσουμε σε λειτουργικά συστήματα, λογισμικά προγραμματισμού και λογισμικά ελέγχου. Επίσης ο ανθρώπινος παράγοντας κατά την σύνθεση των λογισμικών σε συνδυασμό με την πολυπλοκότητα τους αποτελούν παράγοντες που δημιουργούν ελαττώματα [19]. Άλλοι παράγοντες που οδηγούν σε αύξηση των ευπαθειών είναι η κακή συνεννόηση μεταξύ του δημιουργού και του πελάτη, η ελλείψεις σε πόρους, έλλειψη τεχνικής, έλλειψη εμπειρίας και αδυναμία ελέγχου και συντήρησης του προϊόντος λόγο κακής ερμηνείας των τεχνικών χαρακτηριστικών. Αυτοί οι παράγοντες βλέπουμε πως προκύπτουν από την εμπλοκή του ανθρώπου κατά τη δημιουργία των υποδομών Διαδικτύου των Πραγμάτων.

4.2 Πιθανοί θύτες και τα κίνητρα τους

Για να καταλάβουμε πόσο σημαντική είναι η ασφάλεια στο Διαδίκτυο των Πραγμάτων, θα πρέπει πρώτα να δούμε ποιοι είναι οι υποψήφιοι θύτες και οι λόγοι που τους οδηγούν στο να προβούν σε τέτοιες ενέργειες.

Από τη στιγμή που οι συσκευές IoT έχουν τη δυνατότητα να διαχειρίζονται τεράστιες ποσότητες δεδομένων που αφορούν τη βιομηχανία και καταγράφουν στοιχεία που αφορούν την υγειά, αμέσως τις καθιστούν πολύτιμες για συγκεκριμένους κακόβουλους σκοπούς. Συνήθως οι ενδιαφερόμενοι αναφέρονται ως hackers,cybercriminals, hacktivists αλλά ακόμη και κυβερνήσεις κ.α.

Οι πιθανοί θύτες μπορούν να προσπαθήσουν να αποκτήσουν ευαίσθητες πληροφορίες όπως αριθμούς πιστωτικών και χρεωστικών καρτών, τοποθεσία, τραπεζικούς λογαριασμούς, κωδικούς και πληροφορίες που αφορούν την υγεία, μέσω εισβολής σε συσκευές Διαδικτύου των Πραγμάτων. Ακόμη δίνεται η δυνατότητα μέσω της παράνομης σύνδεσης σε συσκευές απομακρυσμένης παρακολούθησης όπως κάμερες, μικρόφωνα κ.α. να παρακολουθείται κάποιος με στόχο την απόκτηση σημαντικών προσωπικών στοιχείων που θα οδηγήσουν σε σοβαρότερη επίθεση σε άλλο χρόνο. Τέλος παρουσιάζεται ενδιαφέρον από τους hacktivists ώστε με την επίθεση σε έξυπνες συσκευές να πραγματοποιούν διαμαρτυρίες εναντίων οργανισμών [13].

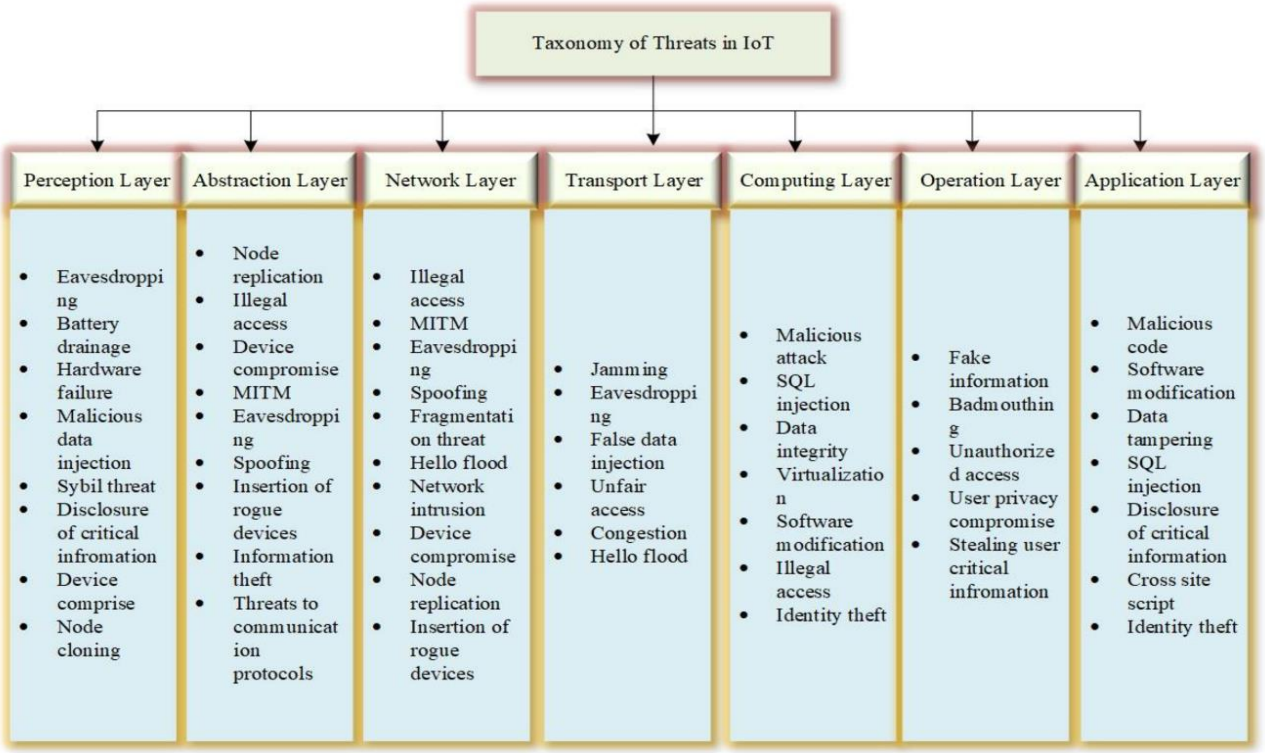
4.3 Απειλές και Επιθέσεις

Ορίζουμε ως απειλή μια δραστηριότητα ή κάποιο γεγονός/συμβάν που εκμεταλλεύεται τα ελαττώματα ασφάλειας ενός συστήματος και του προκαλεί αρνητικές επιπτώσεις. Οι δυο κύριες πηγές απειλών για την ασφάλεια είναι οι άνθρωποι και το περιβάλλον [20]. Ένα προφανές παράδειγμα αποτελούν οι πλημμύρες, οι σεισμοί, οι πυρκαγιές και άλλοι φυσικοί κίνδυνοι που μπορούν εύκολα να προκαλέσουν βλάβες σε υπολογιστικά συστήματα. Η αντιμετώπιση αυτού του είδους απειλών είναι πολύ δύσκολη, καθώς δεν προβλέπονται εύκολα και δεν ελέγχονται αν εξελιχθούν σε μεγάλη κλίμακα. Η καλύτερη αντιμετώπιση αυτών των απειλών θα μπορούσε να θεωρηθεί η δημιουργία αντιγράφων ασφαλείας. Στην περίπτωση όμως των απειλών που προέρχονται από ανθρώπινη ενέργεια, μπορούμε να τις χωρίσουμε σε εσωτερικές απειλές (με πρόσβαση) και σε εξωτερικές (εκτός δικτύου) [2]. Το γεγονός ότι συναντούμε πολλών ειδών απειλές που προκαλούνται από τον άνθρωπο μας οδηγεί στην ανάγκη να της κατηγοριοποιήσουμε ως εξής:

- **Unstructured threats/Αδόμητες απειλές:** Υλοποιούνται συνήθως από ανθρώπους χωρίς ιδιαίτερες γνώσεις, κάνοντας χρήση έτοιμων λογισμικών hacking [2].
- **Structured threats/Δομημένες απειλές:** Υλοποιούνται από ανθρώπους με γνώσεις των ευπαθειών των συστημάτων. Γνωρίζουν πως να χειρίζονται τον κώδικα και να κατασκευάζουν κακόβουλα λογισμικά [2]**.**
- **Advanced Persistent Threats (APT)/Προηγμένες επίμονες απειλές:** Αποτελούν πολύπλοκες επιθέσεις δικτυών που έχουν ως στόχο την κλοπή δεδομένων υψηλής σημασίας και αξίας, συνήθως από μεγάλες βιομηχανίες, εθνικές υπηρεσίες και τράπεζες [21].

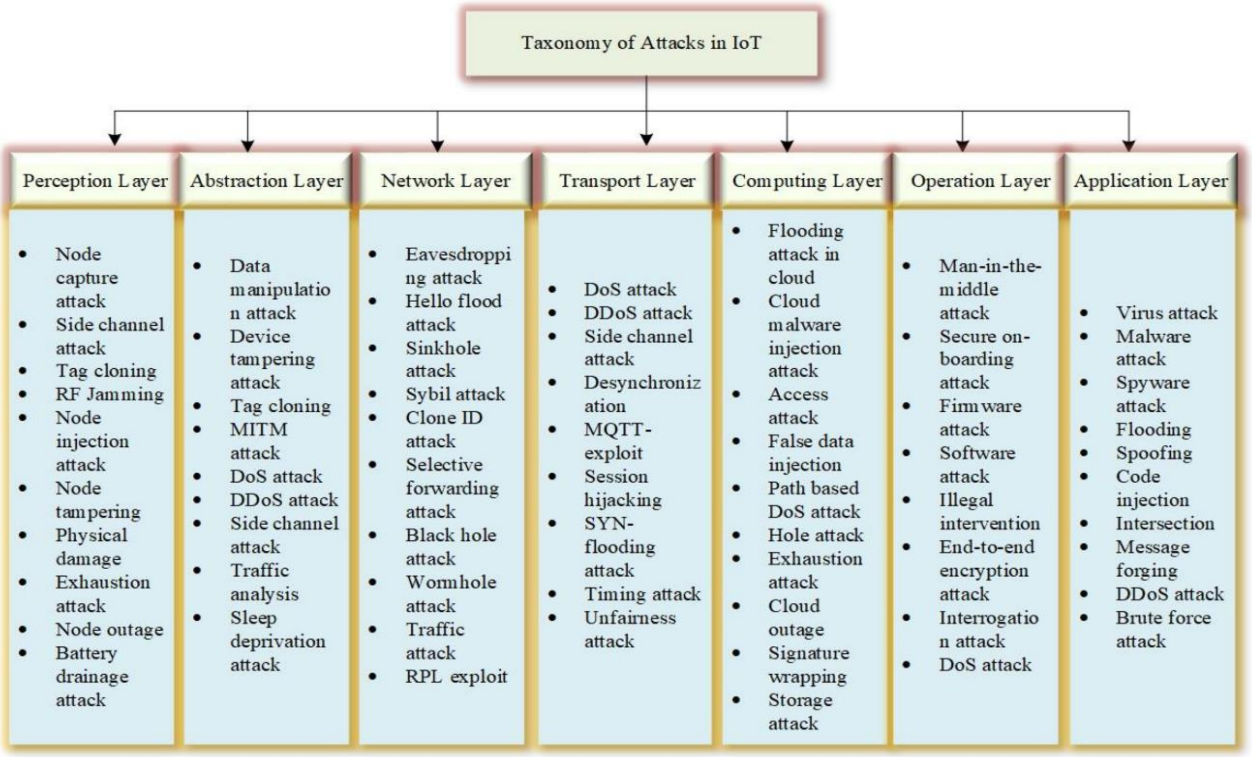
4.4 Κατανομή απειλών και επιθέσεων στα επίπεδα του IoT

Σε αντίθεση με την απειλή που μπορεί να υπάρχει ή να μην υπάρχει δόλος, στην περίπτωση της επίθεσης, πάντα συναντούμε κάποιον δόλο και πρόθεση για πρόκληση ζημιάς. Πολλές τέτοιες απειλές και επιθέσεις συναντώνται στο Διαδίκτυο των Πραγμάτων και μπορούν να αναλυθούν με βάση το μοντέλο αναφοράς του.



Εικόνα 8. Taxonomy of threats in IoT.

Πηγή: https://www.mdpi.com/sustainability/sustainability-13-09463/article_deploy/html/images/sustainability-13-09463-g009.png



Εικόνα 9. Taxonomy of attacks in IoT.

Πηγή: https://www.mdpi.com/sustainability/sustainability-13-09463/article_deploy/html/images/sustainability-13-09463-g010.png

4.4.1 Απειλές στο επίπεδο Αντίληψης / Perception Layer

Τα συστήματα διαχείρισης αισθητήρων δεν επαρκούν για την ασφάλεια τους. Οι απειλές που βασίζονται σε χρήση αισθητήρων αφορούν παθητικές και ενεργητικές κακόβουλες δράσεις που υλοποιούνται με τη χειραγώγηση των αισθητήρων. Άλλες απειλές που συναντούμε στο επίπεδο αντίληψης είναι η λαθρακρόαση, η αποστράγγιση μπαταρίας, η αποτυχία/αστοχία υλικού, η έγχυση κακόβουλων δεδομένων, η επίθεση Sybil, η αποκάλυψη κρίσιμων πληροφοριών, η παραβίαση συσκευής, η κλωνοποίηση κόμβου, η απόκτηση κόμβου, η Side Channel Attack (SCA), η κλωνοποίηση ετικετών, η παρεμβολή ραδιοσυχνοτήτων (RF), η έγχυση κόμβου, η εξάντληση, η διακοπή λειτουργίας κόμβου κ.α. [2]. Παρακάτω θα αναλύσουμε μερικές από αυτές τις απειλές. Πιο εκτεταμένη και λεπτομερής αναφορά γίνεται στα [22] [23].

Λαθρακρόαση / Eavesdropping

Κακόβουλες συσκευές ίδιου τύπου, όπως π.χ. τελικοί κόμβοι, συνδέονται σε συστήματα διαδικτύου των πραγμάτων. Οι θύτες πραγματοποιούν παθητικό sniffing στη ροή των δεδομένων που ανταλλάσσονται για να προσκομίσουν κάποια χρήσιμη πληροφορία [24] [2].

Κακόβουλη έγχυση δεδομένων (Malicious data injection)

Σε αυτή την περίπτωση βρίσκουμε συσκευές που έχουν εισχωρήσει σε κάποιο σύστημα διαδικτύου των πραγμάτων και παραποιούν τα δεδομένα που χρησιμοποιούν οι εφαρμογές. Τα παραποιημένα δεδομένα μπορούν να εισαχθούν με φυσική πρόσβαση ή ακόμη και με τη χρήση του δικτύου Bluetooth, Wi-Fi, GPS κ.α. [2]. Έτσι τελικά έχουμε ως αποτέλεσμα, την απορρόφηση δεδομένων, την προώθηση τεχνητών κακόβουλων μηνυμάτων ή τον κορεσμό του ασύρματου καναλιού ώστε να μην είναι διαθέσιμο [25].

Sybil Attack

Σε αυτή τη περίπτωση οι κακόβουλοι κόμβοι μπορούν να παριστάνουν τους πραγματικούς ή να χρησιμοποιούν ψεύτικες ταυτότητες αντιγράφοντας τις πρωτότυπες. Ένας κακόβουλος μπορεί να έχει πολλές ταυτότητες ταυτοχρόνως ή σε διαφορετικές περιστάσεις.

Αποκάλυψη κρίσιμων πληροφοριών / Disclosure of Critical Information

Κάνοντας χρήση των αισθητήρων που βρίσκονται στις συσκευές του Διαδικτύου των Πραγμάτων, αυξάνονται οι πιθανότητες διαρροής ή υποκλοπής κωδικών πρόσβασης, κλειδιών ασφαλείας, στοιχεία πιστωτικών καρτών κ.α. Με τη χρήση αυτών των στοιχείων μπορεί ο θύτης να προβεί σε παραβίαση του απορρήτου ή να κρατήσει τα στοιχεία για μελλοντική χρήση.

Side-Channel Attacks

Με αυτού του είδους τις επιθέσεις ο υποτιθέμενος θύτης, μέσω του reverse engineering, έχει τη δυνατότητα να συλλέξει τα στοιχεία ταυτότητας της κρυπτογραφημένης συσκευής IoT. Οι πληροφορίες αυτές συλλέγονται από τις συσκευές κρυπτογράφησης. Οι επιθέσεις side-channel, έχουν ως στόχο την απόκτηση του κλειδιού της συσκευής χρησιμοποιώντας δεδομένα. Σε άλλες περιπτώσεις συναντούμε παράλληλα και επιθέσεις συγχρονισμού (timing attacks), επιθέσεις power analysis, failure analysis και ηλεκτρομαγνητικές επιθέσεις.

Επίθεση αποστράγγισης μπαταρίας

Σε αυτό το είδος επιθέσεων στέλνονται αιτήματα αυθυεντικοποίησης αδιακόπως σε συσκευές Διαδικτύου των Πραγμάτων με περιορισμένες δυνατότητες ενεργειακής αυτονομίας. Αυτό εμποδίζει τις συσκευές να μπουν σε λειτουργία ύπνου ή εξοικονόμησης ενέργειας [12].

Δυσλειτουργία υλικού

Οι συσκευές διαδικτύου των πραγμάτων, καθότι είναι πολύ σημαντικές και πλέον απαραίτητες σε κλάδους όπως μεταφορές, υγεία, έξυπνα σπίτια και πόλεις ή έξυπνα ενεργειακά δίκτυα είναι κρίσιμο να λειτουργούν αδιάκοπα και απροβλημάτιστα. Οι αστοχίες αυτών των συσκευών, εξαιτίας σφαλμάτων κατά την φάση της παραγωγής ή κυβερνοεπιθέσεων, ασκούν μεγάλη επιρροή στα συστήματα αλλά και στις ζωές των ανθρώπων που τις χρησιμοποιούν [26] [27] [12].

Κλωνοποίηση κόμβου / Node cloning

Η κλωνοποίηση κάποιας συσκευής κατά βάση προϋποθέτει κάποιον θύτη που έχει πρόσβαση στη τοπολογία και στον εξοπλισμό, άρα συνήθως την χαρακτηρίζουμε σαν επίθεση εκ των έσω. Ο θύτης αλλάζει την συσκευή του συστήματος με κάποια άλλη κατασκευασμένη για άλλο σκοπό. Υπάρχει και η περίπτωση κλωνοποίησης μιας συσκευής κατά τη λειτουργία της. Με την κλωνοποιημένη συσκευή μπορεί κάποιος να έχει πρόσβαση σε πληροφορίες, όπως παραμέτρους ασφαλείας και αλλαγές στο firmware. Μπορεί να συμβεί κατά την περίοδο κατασκευής ή της λειτουργίας [28] [12] [2].

Απόκτηση μη εξουσιοδοτημένης πρόσβασης στη συσκευή

Είναι μια από τις κύριες αδυναμίες της ασφάλειας των συσκευών Διαδικτύου των Πραγμάτων. Η χρήση των εργοστασιακών στοιχείων ταυτοποίησης από τους χρήστες, οδηγούν στην εύκολη πρόσβαση από κακόβουλους στις συσκευές [12]. Επίσης, υπάρχουν περιπτώσεις που οι κατασκευαστές σκόπιμα χρησιμοποιούν μη ασφαλή APIs για απομακρυσμένη πρόσβαση [29]. Παράδειγμα η επίθεση που έγινε στη κάμερα Summer Baby Zoom WiFi από τον Fowler [30] όπου χρησιμοποιούσε ενσωματωμένα στοιχεία admin,admin.

Επίθεση εξάντλησης / Exhaustion attack

Η κατανάλωση ενέργειας μπορεί να επηρεάσει της συσκευές Διαδικτύου των Πραγμάτων που λειτουργούν με μπαταρία αν ο θύτης επιτίθεται στο δίκτυο συνεχώς, όπως για παράδειγμα κατά τις επιθέσεις παρεμβολών και DoS. Η συνεχής προσπάθεια για εκπομπή, δημιουργεί συγκρούσεις στα πρωτόκολλα MAC του IoT και τελικά εξάντληση της ενέργειας.

4.4.2 Απειλές στο Αφαιρετικό επίπεδο / Abstraction Layer

Στο αφαιρετικό επίπεδο, συναντούμε διαφόρων ειδών επιθέσεις όπως η δημιουργία αντιγράφου κόμβου, η παράνομη πρόσβαση, η διακινδύνευση συσκευής, MITM, λαθρακρόαση, spoofing, εισαγωγή κακόβουλων συσκευών, κλοπή πληροφοριών, απειλές στα πρωτόκολλα επικοινωνίας, χειραγώγηση των δεδομένων, παραβίαση των συσκευών, κλωνοποίηση ετικετών, DoS, DDoS, SCA, ανάλυση κίνησης και στέρηση ύπνου [2]. Παρακάτω θα αναλυθούν μερικές από αυτές. Επίσης λεπτομερέστερες αναφορές γίνονται στα [22] [23].

Παράνομη πρόσβαση / Illegal access

Τέτοιου είδους απειλές προκύπτουν κατά την επεξεργασία ευαίσθητων πληροφοριών σε συσκευές του Διαδικτύου των Πραγμάτων που το υλικό βρίσκεται εκτεθειμένο, όπως γεωργικοί αισθητήρες, αισθητήρες σε πόλεις και στη φύση.

MITM (Man In The Middle)

Αποτελεί ένα σύστημα που παρακολουθεί την κίνηση ανάμεσα σε μια έξυπνη συσκευή και την πύλη. Όλη η κίνηση δρομολογείται μέσω του εξοπλισμού του θύτη, που κάνει χρήση της επίθεσης ARP poisoning.

Spoofing

Αποτελούν επιθέσεις πολύ υψηλού κινδύνου. Στις επιθέσεις Spoofing ο θύτης μιμείται μια συσκευή κόμβο. Έτσι, η μετάδοση φαίνεται να προέρχεται από γνωστή πηγή. Η απειλή αυτή μπορεί να πραγματοποιηθεί σε όλα τα επίπεδα του Διαδικτύου των Πραγμάτων.

Απειλές στα πρωτόκολλα επικοινωνίας

Τα περισσότερα πρωτόκολλα επικοινωνίας τηρούν το μοντέλο αρχιτεκτονικής OSI. Το φυσικό επίπεδο, δεν ενισχύεται με μεθόδους ασφαλείας στα επάνω επίπεδα. Αυτό προσθέτει

προβλήματα στο μοντέλο ασφαλείας IoT/CPS. Από την άλλη όμως και οι κυψελωτές τεχνολογίες όπως UTMS, GSM, LTE διαθέτουν προβλήματα ασφάλειας. Καθώς οι στοίβες συχνοτήτων είναι γνωστές και ανοιχτές τα ασύρματα δίκτυα είναι εκτεθειμένα σε hacking και κυβερνοεπιθέσεις.

Κλωνοποίηση ετικετών

Με τη χρήση του reverse engineering ή με απευθείας πρόσβαση μπορεί ο υποτιθέμενος θύτης να κλωνοποιήσει κάποιο RFID tag και να αποκομίσει πληροφορίες.

Denial-of-Service (DoS)

Είναι ένας τύπος επίθεσης κατά τον οποίο μια συσκευή ή μια εφαρμογή αρνείται με κακόβουλο σκοπό την κανονική λειτουργία. Μπορεί να είναι ενεργητικές επιθέσεις, όπου αντιμετωπίζουμε ολική άρνηση σε μια συγκεκριμένη εφαρμογή, ή παθητική, όπου σταματώντας μια υπάρχουσα εφαρμογή, μπορεί να προκαλέσει πρόβλημα σε κάποια άλλη εφαρμογή.

DDoS

Οποιαδήποτε συσκευή, δίκτυο ή πρόγραμμα λογισμικού IoT θα μπορούσε να τερματιστεί από μια κατανεμημένη επίθεση άρνησης υπηρεσίας (DoS), καθιστώντας την υπηρεσία μη προσβάσιμη για τους χρήστες. Αυτές οι επιθέσεις μπορούν να λάβουν πολλές διαφορετικές μορφές και είναι πιο επικίνδυνες από τις επιθέσεις DoS, καθώς κάνουν χρήση πολλών ειδών διαφορετικών συσκευών.

Ανάλυση κίνησης

Το μοτίβο που ακολουθεί η κίνηση σε ένα δίκτυο, αποτελεί πολύ χρήσιμη πληροφορία για ένα θύτη. Με την ανάλυση τέτοιων μοτίβων, αντλούνται χρήσιμες πληροφορίες για την τοπολογία του δικτύου. Σε δίκτυα ασύρματων αισθητήρων (WSNs), αποκαλύπτονται πληροφορίες για την απόσταση των αισθητήρων με βάση τον όγκο δεδομένων. Όσο πιο πολλά δεδομένα διαχειρίζονται, τόσο πιο κοντά στη βάση βρίσκονται. Ομοίως και στα clusters, όπου όσο περισσότερη κίνηση βλέπουμε, τόσο πιο κεντρικός ο κόμβος. Γνωστοποιώντας τους κεντρικούς κόμβους, δίνεται η δυνατότητα για πιο στοχευμένες επιθέσεις.

Στέρηση ύπνου

Η στέρηση ύπνου σε μια συσκευή που κάνει χρήση μπαταρίας μπορεί να οδηγήσει σε εξάντληση της ενέργειας της. Αυτό συνήθως προκύπτει με αδιάκοπες χειραψίες μεταξύ των συσκευών και αποτρέπει την πρόσβαση στο στάδιο ύπνου.

4.4.3 Απειλές στο επίπεδο Δικτύου / Network Layer

Οι πύλες και τα συστήματα δικτύωσης βοηθούν στη δρομολόγηση των πακέτων δεδομένων στον προορισμό τους. Αν οι πύλες επικοινωνούν κάνοντας χρήση πρωτόκολλων ασύρματης δικτύωσης, ο θύτης θα τα εκμεταλλευτεί για να συνδεθεί. Έτσι, θα μπορέσει να πραγματοποιήσει επιπλέον επιθέσεις, όπως ARP poisoning, MITM, έγχυση πακέτων (packet injection) και sniffing. Υπάρχουν όμως και άλλων ειδών απειλές και επιθέσεις που αποτελούν πολύ σοβαρούς κινδύνους στο επίπεδο του δικτύου, όπως η παράνομη πρόσβαση, αντιγραφή κόμβου, εισχώρηση κακόβουλων συσκευών, επίθεση sinkhole, επίθεση sybil, επίθεση αντιγραφής ταυτότητας (clone ID), επίθεση επιλεκτικής προώθησης, επίθεση μαύρης τρύπας (blackhole), επίθεση κίνησης (traffic) και εκμεταλλεύσεις RPL [2]. Μερικές από αυτές θα παρουσιαστούν παρακάτω. Επιπλέον στοιχεία και λεπτομέρειες αναφέρονται στα [22] [23].

Hello flood

Πραγματοποιείται με τη συνεχή αποστολή αιτημάτων εγκατάστασης νέας σύνδεσης σε κάποιο κόμβο του δικτύου. Οι κόμβοι, αποδέχονται τα μηνύματα αυτά, καθώς θεωρούν ότι προέρχονται από το δίκτυο και τα κατηγοριοποιούν ως ξέχωρα αιτήματα για νέες συνδέσεις. Αυτού του είδους οι επιθέσεις αποτελούν έναν από τους μεγαλύτερους κινδύνους στο επίπεδο δικτύου.

Sinkhole

Κατά την επίθεση sinkhole ο θύτης εκθέτει σε κίνδυνο τον κεντρικό κόμβο του δικτύου και τον παρακάμπτει ώστε να τον αχρηστέψει. Είναι ένας πολύ αποδοτικός τρόπος να ελέγξει κάποιος κακόβουλος ολόκληρη την υποδομή του δικτύου.

Blackhole

Με την επίθεση blackhole, έχουμε τον εξαναγκασμό ενός κόμβου να απορρίψει (drop) όλα τα πακέτα. Από αυτού του είδους την επίθεση επηρεάζεται ολόκληρο το δίκτυο. Ο θύτης γεμίζει

με κακόβουλα δεδομένα το δίκτυο για να ανακαλύψει την πιο αποδοτική διαδρομή για το στόχο. Ο κόμβος απαντά στα αιτήματα του θύτη και με τη σειρά του ο θύτης τα απορρίπτει (drop). Έτσι απασχολείται ο κόμβος και δεν προωθείται η πραγματική κίνηση στον προορισμό της. Αυτές οι επιθέσεις έχουν πολύ υψηλό αντίκτυπο σε ένα δίκτυο.

Traffic Analysis

Από την ανάλυση τις κίνησης σε ένα δίκτυο ο θύτης αποκτά πληροφορίες για τα δεδομένα που κινήθηκαν στη σύνδεση. Αυτές τις πληροφορίες που απέκτησε, τις αποθηκεύει για να τις χρησιμοποιήσει αργότερα. Η ίδια κίνηση δεδομένων που επικοινωνούσε η διεπαφή με την πύλη μπορεί να του δώσει τη δυνατότητα να πάρει τον έλεγχο της.

Wormhole

Οι επιθέσεις wormhole παρεμβάλουν και υποκλέπτουν την κίνηση δεδομένων σε ένα δίκτυο και την εξαναγκάζουν να ανακατευθυνθεί σε ένα άλλο δίκτυο. Αυτό θα μπορούσε να επιφέρει συμφόρηση στο δίκτυο και να μειώσει την απόδοση του.

Selective forwarding

Στην επίθεση selective forwarding έχουμε αρχικά την εισβολή ενός θύτη σε κάποιο δίκτυο. Εκεί ο δράστης αναγκάζει συσκευές να απορρίψουν δεδομένα. Κάποια από τα δεδομένα απορρίπτονται ενώ άλλα επιλέγονται και προωθούνται. Έτσι το εύρος ζώνης του δικτύου μπορεί να αντιμετωπίσει προβλήματα και να υπάρξουν καθυστερήσεις και κολλήματα. Καλό είναι να αναφερθεί ότι αυτές οι επιθέσεις είναι δύσκολο να ανιχνευτούν, καθώς τα δίκτυα IoT λειτουργούν με τεχνικές lossy.

RPL exploit

Όπως αναφέραμε, το Διαδίκτυο των Πραγμάτων αποτελείται από συσκευές με περιορισμένες δυνατότητες. Οι συσκευές λαμβάνουν ενέργεια από μικρές, χαμηλής απόδοσης μπαταρίες και οι μνήμες τους όπως και η επεξεργαστική τους ισχύς είναι περιορισμένες. Για αυτό το λόγο κατασκευάστηκε το πρωτόκολλο διευθυνσιοδότησης RPL (routing protocol for low power and lossy networks) και εφαρμόστηκε σε multi-point-to-point επικοινωνίες και στο Διαδίκτυο των Πραγμάτων. Το συγκεκριμένο πρωτόκολλο δεν διαθέτει όλα τα χαρακτηριστικά που θα βρίσκαμε σε ένα κλασσικό πρωτόκολλο διευθυνσιοδότησης. Στις επιθέσεις που απειλούν το

πρωτόκολλο RPL, εντοπίζουμε κακόβουλους κόμβους που προσπαθούν να τροποποιήσουν τις διαδρομές (paths) που ακολουθούν τα δεδομένα. Επιθέσεις sinkhole ή και επιθέσεις blackhole συνηθίζεται να υλοποιούνται για την ολοκλήρωση των κακόβουλων προσπαθειών.

4.4.4 Απειλές στο επίπεδο Μεταφοράς / Transport Layer

Οι διάφορες απειλές που συναντούμε στο επίπεδο μεταφοράς είναι η δημιουργία παρεμβολών (jamming), η λαθρακρόαση ή αλλιώς υποκλοπή, η μόλυνση με κακόβουλα δεδομένα (false data injection), η αθέμιτη πρόσβαση (unfair access), η συμφόρηση (congestion), η επίθεση hello flood, DoS, DDoS, SCA, αποσυγχρονισμού (desynchronization), κακόβουλη εκμετάλλευση MQTT, πειρατεία συνεδρίας (session hijacking), SYQ-flooding, επίθεση χρονισμού (timing attack) κ.ά. [2]. Παρακάτω αναλύονται κάποιες από τις απειλές και επιθέσεις. Επιπλέον στοιχεία και λεπτομέρειες αναφέρονται στα [22] [23].

Desynchronization

Αφορά τον αποσυγχρονισμό των μεταδόσεων μεταξύ δυο κόμβων και επιτρέπει την διακοπή της σύνδεσης τους, παραδείγματος χάριν με την αποστολή λανθασμένων τύπων flags. Αναγκάζοντας τους να χάσουν την επαφή τους και τους αποτρέπει από το να επικοινωνούν.

Session hijacking

Στις επιθέσεις hijacking, ο θύτης αποσπά την ταυτότητα της συνεδρίας και προσποιείται τον πραγματικό χρήστη. Έτσι, αποκτά πρόσβαση και χειρίζεται τη συνεδρία σαν δική του. Έπειτα έχει τη δυνατότητα να ξεγελά την ταυτοποίηση και να προβαίνει σε οποιαδήποτε ενέργεια θα μπορούσε και ο νόμιμος χρήστης του δικτύου.

4.4.5 Απειλές στο επίπεδο Υπολογισμού / Computing Layer

Στο επίπεδο που λαμβάνουν χώρα η αποθήκευση δεδομένων και ο απομακρυσμένος χειρισμός υπολογιστών, αν δεν πέτυχουμε την σωστή διαμόρφωση των διακομιστών νέφους, μπορεί να οδηγηθούμε σε κακόβουλη εκμετάλλευση των διακομιστών και των έξυπνων συσκευών. Διάφορες απειλές και προκλήσεις στο επίπεδο του υπολογισμού είναι η κακόβουλες επιθέσεις, SQL injection, απειλή της ακεραιότητας των δεδομένων (data integrity), εικονικοποίηση (virtualization), τροποποιήσεις λογισμικού (software modification), παράνομη πρόσβαση (illegal access), κλοπή ταυτότητας, flooding attack σε περιβάλλον νέφους, έγχυση

κακόβουλου λογισμικού σε περιβάλλον νέφους (cloud malware injection), access attack, false data injection, path-based DoS, hole attack, επίθεση εξάντλησης (exhaustion attack), cloud outage, signature wrapping, επίθεση στην αποθήκευση (storage attack), κ.α. [2]. Παρακάτω θα αναλυθούν κάποιες από τις απειλές και επιθέσεις. Επιπλέον στοιχεία και λεπτομέρειες αναφέρονται στα [22] [23] [31].

Malicious Attack

Με την λήψη στοιχείων από το διαδίκτυο, αυξάνεται το ρίσκο της εισροής κακόβουλου λογισμικού (malware) στις συσκευές. Το malware, έχει τη δυνατότητα να εξαπλώνεται στο εσωτερικό δίκτυο και να θέτει σε κίνδυνο πολλές άλλες συσκευές. Μέσω κάποιας μολυσμένης συσκευής ο θύτης αποκτά τη δυνατότητα να εισβάλει στο σύστημα Διαδικτύου των Πραγμάτων που βρίσκεται σε σύνδεση με το δίκτυο και να προβεί σε διάφορες κακόβουλες πράξεις.

SQL injection

Με την επίθεση SQL injection, δίνεται η δυνατότητα για παρέμβαση στα αιτήματα μιας διαδικτυακής εφαρμογής προς τη βάση δεδομένων. Έτσι δημιουργείται μια πρόσβαση σε δεδομένα, που υπό άλλες συνθήκες, δεν θα έπρεπε να είναι κοινά. Εφόσον υπάρχει πρόσβαση στα δεδομένα, δημιουργείται και η δυνατότητα για αλλαγή ή και διαγραφή των δεδομένων που θα έφερνε ως αποτέλεσμα την εσφαλμένη λειτουργία της εφαρμογής.

Illegal Access

Η παράνομη πρόσβαση, αποτελεί μια από τις μεγαλύτερες απειλές για τα συστήματα νέφους. Επιτρέπει την διακοπή της ροής δεδομένων και μπορεί να επηρεάσει διάφορες λειτουργίες. Το γεγονός ότι η τεχνολογία νέφους κάνει χρήση διαφόρων απομακρυσμένων συστημάτων, αποτελούμενα από ξεχωριστά δίκτυα, που τα διαχειρίζονται άλλοι οργανισμοί, κάνει την διασφάλιση προστασίας δυσκολότερη. Η περίπτωση που οι συσκευές του Διαδικτύου των Πραγμάτων δεν είναι διαμορφωμένες με σωστό τρόπο, μπορούν να φέρουν σε κίνδυνο ολόκληρο το δίκτυο.

Storage Attack

Η επίθεση στους αποθηκευτικούς πόρους εμφανίζει μεγάλη δυσκολία ως προς την ανίχνευση και την αντιμετώπιση. Κρατώντας τα αποθηκευτικά μέσα σε συνεχή λειτουργία, συνήθως εφαρμόζοντας cryptohacking, έχουμε ως αποτέλεσμα τις καθυστερήσεις στην απόκριση και τη λειτουργία τον συσκευών σε συστήματα νέφους. Έτσι η επίθεση αυτή μπορεί να ερμηνευτεί ως μια απλή δυσκολία των συσκευών, που δεν οφείλεται σε κάτι κακόβουλο και αποδίδεται συχνά σε εσφαλμένες ενημερώσεις λογισμικού και κακής ποιότητας σύνδεσης δικτύου.

Access Attack

Αναφέρεται και ως Προηγμένη επίμονη απειλή (Advanced persistent threat). Εφαρμόζεται με την μη εξουσιοδοτημένη είσοδο του θύτη σε κάποιο δίκτυο συσκευών IoT. Ο σκοπός είναι να παραμείνει για αρκετό χρονικό διάστημα στο δίκτυο για να αποσπάσει χρήσιμες πληροφορίες, άρα πρέπει να υπάρχει χαμηλό προφίλ και να μην επηρεάζει τη λειτουργία του δικτύου.

Software modification

Σε αυτή την περίπτωση, έχουμε την τροποποίηση του λογισμικού και του υλικολογισμικού (firmware) μιας συσκευής IoT. Αυτή η ενέργεια μπορεί να πραγματοποιηθεί με φυσική πρόσβαση ή ακόμη και εξ αποστάσεως. Με την προσθήκη αλλαγών στον κώδικα, δίνετε η δυνατότητα να υπάρξει επιπλέων εκμετάλλευση.

4.4.6 Απειλές στο επίπεδο Λειτουργιών / Operation Layer

Απειλές και επιθέσεις που εντοπίζουμε στο επίπεδο λειτουργειών είναι οι ψευδείς πληροφορίες (fake information), το badmouthing, η μη εξουσιοδοτημένη πρόσβαση (unauthorized access), η διακινδύνευση της ιδιωτικότητας του χρήστη (users' privacy compromise), η κλοπή σημαντικών πληροφοριών του χρήστη (stealing users' critical information),οι επιθέσεις MITM, οι επιθέσεις secure on-boarding, επιθέσεις ηλικολογισμικού (firmware attack), επιθέσεις λογισμικού (software attack), η παράνομη παρέμβαση (illegal intervention), η επίθεση στην κρυπτογράφηση από άκρο σε άκρο (end-to-end encryption attack), η επίθεση ανάκρισης (interrogation attack), επίθεση DoS κ.ά. [2]. Παρακάτω θα αναλυθούν κάποιες από τις απειλές και επιθέσεις που αφορούν το επίπεδο λειτουργιών.

Illegal Intervention

Οι διεπαφές χρήστη και τα APIs που παρέχονται από τους παρόχους υπηρεσιών νέφους, βοηθούν στην λειτουργία τους και δίνεται μεγάλη προσπάθεια για τη συντήρηση και τη βελτίωση τους. Τα APIs και οι διεπαφές αυτές, κοινοποιούνται στους κατασκευαστές (developers) που χρησιμοποιούν την υπηρεσία νέφους για τις δίκες τους εφαρμογές. Εφόσον είναι γνωστά και εκτεθειμένα, αυτά τα λογισμικά μπορεί να τα εκμεταλλευτεί κάποιος για να αποκτήσει πρόσβαση σε άλλες διεπαφές που είναι συνδεμένες ή να του δώσει τη δυνατότητα να αποσπάσει πιστοποιητικά που χρησιμοποιούνται.

Unauthorized Access

Στα frameworks που υποστηρίζουν ταυτόχρονη/παράλληλη είσοδο και δυνατότητες για ταυτόχρονες αλλαγές/παράλληλες σε δεδομένα, με προσθήκη, αφαίρεση και μετατροπή, μπορεί να οδηγήσει σε λειτουργικές δυσκολίες. Σε IoT frameworks η χρήση access controls είναι πολύ σημαντική καθώς η φύση των λειτουργιών είναι τέτοια που απαιτεί την ταυτόχρονη είσοδο πολλαπλών συσκευών. Αν αποτύχει ο έλεγχος και δοθεί πρόσβαση σε μη εξουσιοδοτημένη οντότητα, μπορεί να κινδυνεύσει από επιθέσεις ολόκληρη η δομή του δικτύου.

4.4.7 Απειλές στο επίπεδο Εφαρμογής / Application Layer

Το επίπεδο εφαρμογής, αντιμετωπίζει κάποια προβλήματα που οφείλονται σε απειλές και επιθέσεις και διαφέρουν λίγο η πολύ ανάλογα με την εφαρμογή που απευθύνονται. Τέτοιες απειλές και επιθέσεις είναι ο κακόβουλος κώδικας (malicious code), η τροποποίηση λογισμικού (software modification), η αλλοίωση δεδομένων (data tampering), SQL injection, αποκάλυψη κρίσιμων πληροφοριών (disclosure of critical information), cross-site script. κλοπή ταυτότητας (identity theft), επίθεση από ιό (virus attack), επίθεση malware, επίθεση spyware, flooding, spoofing, έγχυση κώδικα (code injection), code intersection, παραποίηση μηνυμάτων (message forging), επίθεση DDoS, επίθεση brute force κ.ά. [2]. Παρακάτω θα αναλύσουμε κάποιες από τις απειλές και επιθέσεις που αφορούν το επίπεδο εφαρμογής. Επιπλέον στοιχεία και λεπτομέρειες αναφέρονται στα [22] [23] [2].

Malicious code

Ο κακόβουλος κώδικας, είναι ένας τρόπος να εκμεταλλευθεί κάποιος τις αδυναμίες των συσκευών Διαδικτύου των Πραγμάτων μέσω του διαδικτύου. Έτσι δίνεται η δυνατότητα στους hackers να βλάψουν τις συσκευές που δέχθηκαν αρχικά την επίθεση, άλλα και άλλες τελικές συσκευές και εφαρμογές που βρίσκονται στο δίκτυο.

Software Modification

Αλλαγές στα συστήματα και της δομές των εφαρμογών μπορούν να προκαλέσουν προβλήματα. Όσο αλλάζει η δομή μιας εφαρμογής τόσο αυτά τα προβλήματα μπορούν να αποτελέσουν μεγαλύτερο κίνδυνο. Αν δεν εξασφαλιστεί η σωστή ανάπτυξη των λογισμικών, δίνεται η ευκαιρία για εξ αποστάσεως επαναπρογραμματισμό και hacking των συσκευών IoT.

Data tampering

Σε αυτού του είδους επιθέσεις, κακόβουλοι εισβολείς αλλοιώνουν τις πληροφορίες που στέλνει μια τελική συσκευή. Αφού ανακαλύψουν το είδος και τον τύπο των δεδομένων, κατασκευάζουν παρόμοια δεδομένα, ώστε να είναι δύσκολο να πιστοποιηθεί η ακρίβεια και η εγκυρότητα τους.

Cross-site script

Αναφέρεται και ως XSS και αποτελεί μια τεχνική όπου χρησιμοποιεί την προσθήκη κακόβουλου κώδικα σε κάποιο έμπιστο ισότοπο. Το αποτέλεσμα είναι να βρεθεί ο έλεγχος του συστήματος Διαδικτύου των Πραγμάτων στα χέρια του θύτη.

Identity Thefts

Είναι γεγονός ότι τα συστήματα του Διαδικτύου των πραγμάτων χειρίζονται μεγάλο αριθμό προσωπικών δεδομένων. Γίνεται εκτεταμένη χρήση μεθόδων και πρωτόκολλων ασφαλείας, όπως η απομόνωση των δεδομένων (data isolation), η κρυπτογράφηση των δεδομένων (data encryption), η ταυτοποίηση του χρήστη (user authentication), η ταυτοποίηση του δικτύου (network authentication) κ.α. Παρόλα αυτά, σε κάποιες περιπτώσεις, η απειλή είναι δύσκολο να περιοριστεί και καταλήγουμε σε διαρροές δεδομένων προσωπικού χαρακτήρα.

Virus attack

Επηρεάζουν κυρίως smartphones, κόμβους sink και άλλου είδους πύλες Διαδικτύου των Πραγμάτων. Ο στόχος τους είναι να καταρρίψουν την εμπιστευτικότητα του συστήματος.

Spyware attack

Το spyware συναντάται εγκατεστημένο σε συσκευές του Διαδικτύου των Πραγμάτων χωρίς τη συγκατάθεση του χρήστη. Με αυτού του είδους την επίθεση δίνεται η δυνατότητα για συλλογή ευαίσθητων δεδομένων που αφορούν τους χρήστες και τις συνήθειες τους. Άρα αφορά αρκετά προσωποποιημένα δεδομένα που χρησιμοποιούνται για τον καθορισμό επόμενων τρόπων επίθεσης.

Code Injection

Για την διεκπεραίωση αυτής της επίθεσης, ο θύτης θα ελέγξει ποια είναι η πιο αδύναμη συσκευή του δικτύου, συνήθως αυτές με κακογραμμένο κώδικα που δεν έχει περάσει τα απαραίτητα τεστ. Έπειτα θα χρησιμοποιήσει αυτή τη συσκευή σαν τον πιο απλό τρόπο για να εισβάλει στο δίκτυο.

Intersection

Ο κίνδυνος σε αυτή την επίθεση προκύπτει από την συνεχή και επαναλαμβανόμενη επικοινωνία μεταξύ των συσκευών που προστατεύονται από συστήματα που υπό άλλες συνθήκες προσφέρουν ανωνυμία. Στις περιπτώσεις που εντοπίζεται κάποια αλλαγή στην ροή δεδομένων, όπως σε περίπτωση που κάποιες συσκευές σταματούν να επικοινωνούν, έχουν ως αποτέλεσμα να εντοπίζεται μέρος κάποιων μηνυμάτων αποκαλύπτονται χρήσιμες πληροφορίες που αυξάνουν τον κίνδυνο για περεταίρω επιθέσεις.

Brute force attack

Αυτή η τεχνική απαιτεί τον συνεχή έλεγχο για πιθανούς συνδυασμούς που καταλήγουν σε αποκάλυψη του κωδικού που δίνει πρόσβαση στο σύστημα.

Layers	Technology/Protocols	Threat	Susceptibility	IoT Security challenges	Ref
Physical/ Perception	NFC,RFID Tags,ODB2, Rs-232, ModBus, PLC, RJ-45, USB	Eavesdropping	Lack of encryption	Confidentiality	H. Ning et al.
		Battery drainage attacks	No white listing and black listing, No spam control	Resource Constraintness	A. Reziouk et al.
		Hardware failure/exploitation /Device compromise	Casualness by the manufacturers, Developers fault, Unprotected interfaces, No Physical security	Lack of Standard, Physical Security	J. Wurm et al. O. Arias et al. Kumar et al.
		Malign data injection, Cloning of node	Lack of strong access control, No tamper-proofing	Integrity of Device/Data	D. Puthal et al. P. Paganini
		Unauthorized admittance to the devices	Usage of default or hard coded credentials	No standard, Integrity, Confidentiality	Thomas Brewster B.Fowler
MAC/ Adaptation/ Network	NFC, RFID, BLE, Ant, Insteon,MiMAC, WirelessHART, Wifi802.11, 3GPP (NB-IoT, eMTC, EC-GSM), LoRaWAN, Symphony Link, Weightless, SIGFOX, DASH7, Ant+, EnOcean, ZWave, ZigBee, DigiMesh	DoS attacks (collision attack, channel congestion attack, battery exhaustion attack)	Flaw in communication protocols	Availability, Heterogeneity	A. Reziouk et al. T. Borgohain et al. R. M. Savola et al.
		Eavesdropping, MITM attack	Lack of strong authentication mechanism and data security	Confidentiality/ Source integrity	D. Puthal et al.
		Storage attacks	No duplication of data storage, Centralized storage, Malware threats such as crypt locker and ransom ware	Resource Constraintness	Kumar et al.
Application	MQIT, AMQP, DDS, XMPP, PTP, Https, SEP 2.0, SSH, FTP, Telnet, COAP,	Malign codes	No application/web security, Lack of authentication and authorization mechanism	Authentication, Authorization, Integrity	A.R. Sadeghi et al.
		Escalated privileges and data tampering, SQL injection, Disclosure of private data	Weak authentication and authorization mechanism	Access control, Data Authentication, Confidentiality	Dave
		Cross Site Scripting attack	Web vulnerabilities		acunetix
Semantic	HDFS, MapReduce, Kakfa, Rapid MQ, Scribe, Luxun	Theft of Identity and compromise of user privacy	No data and application security	Identity, Leak of Private Data, Confidentiality	K. Hamlen et al.

Εικόνα 10. Layerwise Security Threats, Vulnerabilities, and Corresponding Security Challenges are Highlighted Along With Protocols Being Used in Each Layer.

Πηγή: https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6488907/9219268/9099839/abbas.t2-2

4.5 Απειλές που αφορούν τις IoT πύλες (IoT gateways)

Αναφέραμε σε προηγούμενο κεφάλαιο τον σημαντικό ρόλο που παίζουν οι πύλες για τις λειτουργίες των συσκευών του Διαδικτύου των Πραγμάτων. Οι πύλες αυτές διατρέχουν κινδύνους που κατηγοριοποιούνται ως εξής:

- Επίθεση Υλικού (Physical Attack): Αφορούν τη μη εξουσιοδοτημένη πρόσβαση στο υλικό (hardware) που υλοποιούνται οι πύλες Διαδικτύου των Πραγμάτων.
- Επίθεση Λογισμικού (Software Attack): Επιθέσεις Trojan, Worms, Virus, Jamming, DoS.
- Επίθεση Δικτύου (Network Attack): Κατάληψη κόμβου/Node capture, Υπονόμευση κόμβου/node subversion, Δυσλειτουργία κόμβου/node malfunctioning, Διαφθορά μηνυμάτων/message corruption, Επιθέσεις διυθυνσιοδότησης/Routing attacks, Ψευδή κόμβου/False node.
- Επίθεση Κρυπτοανάλυσης (Cryptanalysis Attack): Γνωστό απλό κείμενο/Known-plaintext, Man-In-The-Middle-Attack (MITM), Χρήση μόνο κρυπτογραφημένου κειμένου/Ciphertext only, Χρήση μόνο επιλεγμένου απλού κειμένου/Chosen plaintext.
- Επίθεση Side Channel (Side Channel Attack): Microprobing, Reverse engineering.

4.6 Νομικές και Κοινωνικές Προκλήσεις

Νέες νομικές ευθύνες εμφανίζονται με αιτία τις νέες έξυπνες υπηρεσίες που παρέχονται από τις τεχνολογίες διαδικτύου των πραγμάτων. Οι προκλήσεις αυτές αναφέρονται με τον όρο **Διαμάχη Ευθύνης** (Liability Dispute) [12]. Ακόμη ένας σημαντικός παράγοντας θεωρείται η **Εμπορευματοποίηση Δεδομένων.** Η διαχείριση του όγκου δεδομένων φέρει στο παρασκήνιο το πρόβλημα που προκύπτει με την ιδιοκτησία των δεδομένων. Κάποια από τα ερωτήματα που εγείρονται είναι το, πώς μπορεί κανείς να διαχειριστεί τα δεδομένα σαν προϊόν με κατοχυρωμένο τρόπο (standardized), ποιος θεωρείται ο ιδιοκτήτης των δεδομένων και αν καθίσταται δυνατή η συναλλαγή των δεδομένων. Η δανειοδότηση και η άρση αυτής για τη συλλογή δεδομένων πρέπει να είναι δικαίωμα των ιδιοκτητών.

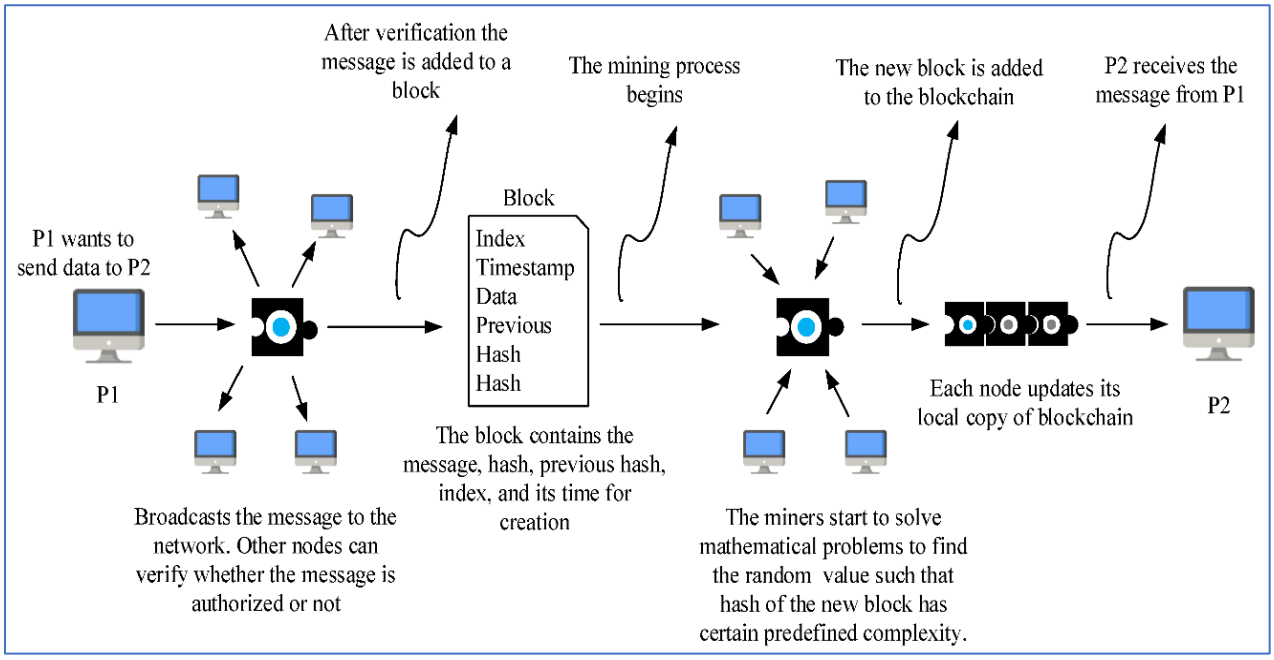
4.7 Γενικευμένοι κίνδυνοι

Σε αυτή τη κατηγορία θα τοποθετήσουμε κινδύνους που δεν προκύπτουν από κάποια συγκεκριμένη αιτία που χρήζει αντιμετώπισης με κάποιο από τους κλασσικούς τρόπους που χειριζόμαστε κινδύνους. Εδώ θα αναφερθούν πρώτα οι **αδυναμίες υλικού,** όπου προκύπτουν κατά τη δημιουργία των εμπορικών προϊόντων διαδικτύου των πραγμάτων, καθώς παρατηρείται ότι τον βασικό ρόλο κατά τη δημιουργία των εμπορικών προϊόντων διαδικτύου των πραγμάτων τον έχουν οι λειτουργίες και όχι η ασφάλεια τους [12]. Έπειτα, το **social engineering,** καθώς από τη στιγμή που οι συσκευές διαδικτύου των πραγμάτων έγιναν κομμάτι της καθημερινότητας των περισσότερων ανθρώπων και με τον όγκο προσωπικών δεδομένων που συλλέγουν δημιουργούν τον κίνδυνο που δίνει εθελούσια πρόσβαση σε κακόβουλους τρίτους (hackers), μέσω παγίδων. Έτσι μπορούν να λάβουν τον έλεγχο και πολλές φορές χωρίς ο νόμιμος χρήστης - ιδιοκτήτης να το αντιληφθεί.

5. Τεχνολογίες που ενισχύουν την ασφάλεια στο IoT

5.1 Blockchain

Η τεχνολογία blockchain αποτελεί ένα δίκτυο από κόμβους peer-to-peer που αποθηκεύουν αντίγραφα των συναλλαγών, τα ονομαζόμενα blocks. Αυτά τα blocks αποτελούν την αλυσίδα (chain) που περιέχει τις βάσεις δεδομένων. Το blockchain είναι κατανεμημένο σύστημα. Οι συσκευές Διαδικτύου των Πραγμάτων συλλέγουν δεδομένα πραγματικού χρόνου από διάφορους αισθητήρες και με τη χρήση του blockchain τα κρατά ασφαλή, συντηρώντας ένα αποκεντρωμένο, κατανεμημένο, κοινόχρηστο αρχείο καταγραφής [32]. Όλες οι συναλλαγές δεδομένων που πραγματοποιούνται σε αυτό το αρχείο υπογράφονται με την υπογραφή του ιδιόκτητη. Αυτό πιστοποιεί τα δεδομένα, τα καθιστά πολύ σταθερά και τα προστατεύει από διάφορες απειλές. Κάθε οντότητα είναι συνδεμένη με την προηγούμενη, καθώς σημειώνεται και ο χρόνος που καταχωρήθηκε. Αυτά τα χαρακτηριστικά καθιστούν το blockchain ως ένα ασφαλές, κατανεμημένο και ανοικτό σύστημα αντιμετώπισης δεδομένων για το Διαδίκτυο των Πραγμάτων.

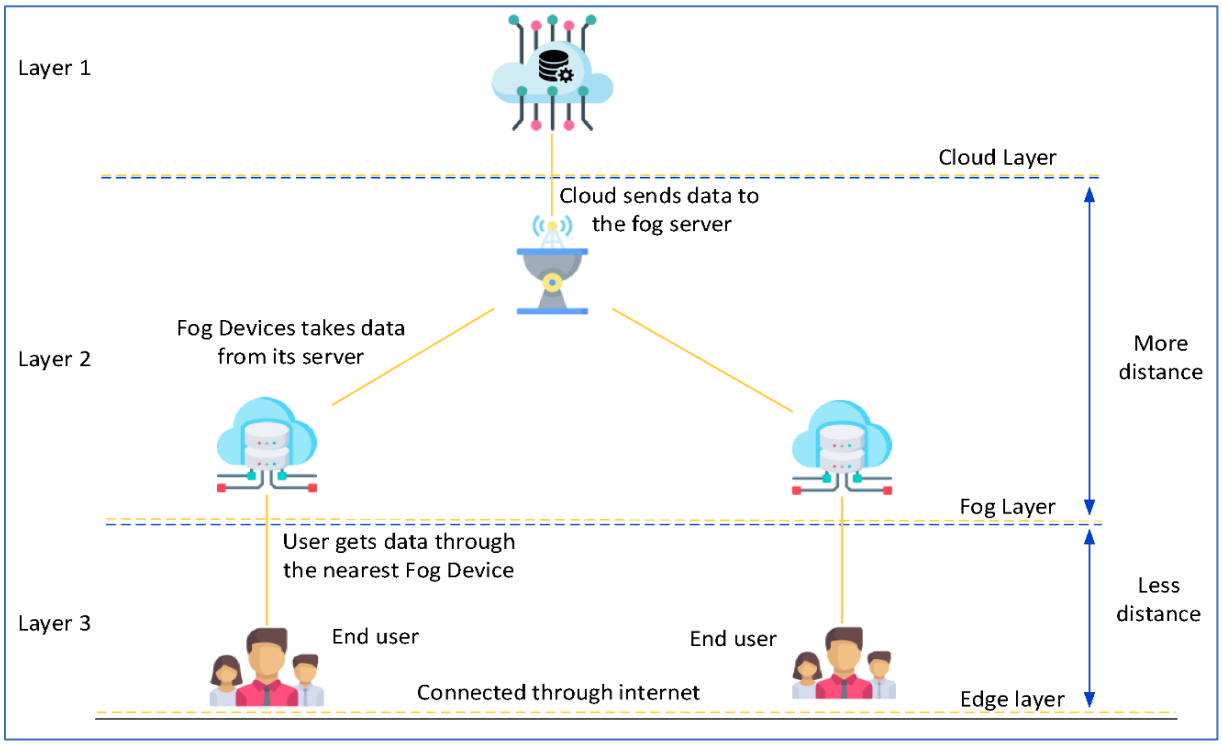


Εικόνα 11. Basics of BC for enhancing security and privacy in IoT.

Πηγή: https://www.mdpi.com/sustainability/sustainability-13-09463/article_deploy/html/images/sustainability-13-09463-g011.png

5.2 Fog Computing

Με το Fog computing, μεταφέρουμε τις διαδικασίες της επεξεργασίας δεδομένων, της αποθήκευσης και τους ελέγχους στα άκρα (edge) του δικτύου και κοντά στις συσκευές, με τη χρήση των Fog-Device Framework και Fog Cloud Framework [33]. Με τη χρήση αυτών των frameworks, οι υπηρεσίες μεταφέρονται στον χρήστη χωρίς να εμπλέκονται οι διακομιστές cloud. Αφήνοντας μόνο τις σημαντικές αποφάσεις να απασχολούν το cloud [34].



Εικόνα 12. An elementary overview of FC.

Πηγή: https://www.mdpi.com/sustainability/sustainability-13-09463/article_deploy/html/images/sustainability-13-09463-g013.png

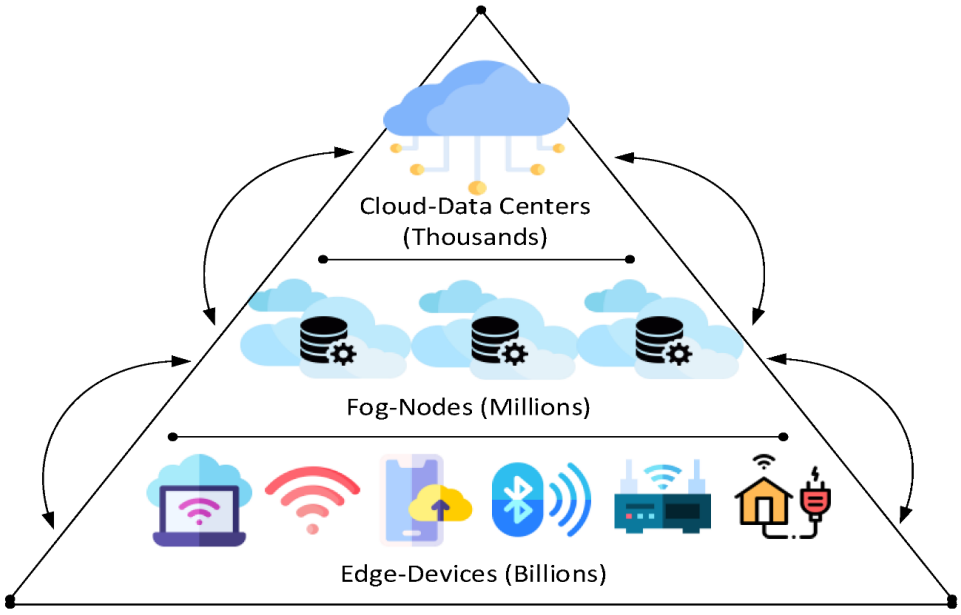
Οι κόμβοι Fog παρέχουν κρυπτογραφικούς υπολογισμούς στις εφαρμογές Διαδικτύου των Πραγμάτων και έτσι βοηθούν στην ενίσχυση της ασφάλειας στις επικοινωνίες [35]. Άλλες δυνατότητες του Fog computing που ενισχύουν την ασφάλεια είναι:

- Η προσθήκη υπηρεσιών που δρουν μόλις ανιχνεύσουν δυσλειτουργία **(Incident response services**).
- Η ενίσχυση των συσκευών Edge σε περίπτωση που κάποιος προσπαθήσει να της βλάψει (**Resource-constraint issues**).

- Η επικοινωνία μόνο μεταξύ συσκευών τελικού χρήστη και fog κόμβων για να μειωθεί η κίνηση στο δίκτυο (**Eavesdropping**).
- Τη χρήση ασφαλών κόμβων fog αντί των συσκευών Διαδικτύου των Πραγμάτων, για καλύτερη ασφάλεια των δεδομένων (**Data transit attacks**).
- Παρέχει μια ασπίδα προστασίας μεταξύ του cloud και τον τελικό χρήστη και προλαμβάνει βλαβερές ενέργειες πριν φτάσουν βαθύτερα στο σύστημα (**Man-in-the-middle attack**).

5.3 Edge Computing

Όπως και το Fog computing, το Edge computing παρέχει υπηρεσίες για την μείωση των δεδομένων που φτάνουν στο cloud, κάνουν πιο αποτελεσματικούς υπολογισμούς ενσωματώνουν την ετερογένεια κ.α. Ο κύριος στόχος όμως είναι να μεταφέρουν τους υπολογισμούς και τους χειρισμούς πιο κοντά στα άκρα του δικτύου. Σε πολλά σημεία όμως διαφέρουν. Αυτά είναι ο διαφορετικός τρόπος λειτουργίας και ο τρόπος που χειρίζονται τα δεδομένα. Μπορούμε να πούμε ότι το Fog computing λαμβάνει χώρα σε μεγαλύτερη απόσταση από ότι το Edge computing [36]. Προκύπτει λοιπόν ότι μια εφαρμογή έχει τη δυνατότητα να στείλει λιγότερα δεδομένα εκτός δικτύου.



Εικόνα 13. An elementary architecture of EC.

Πηγές: https://www.mdpi.com/sustainability/sustainability-13-09463/article_deploy/html/images/sustainability-13-09463-g014.png

5.4 Machine Learning

Αποτελεί ένα πολύ καλό τρόπο να αυξηθεί η ασφάλεια στο Διαδίκτυο των Πραγμάτων κατά των απειλών που αντιμετωπίζει. Προσφέρει δυνατότητες που ξεφεύγουν από τους παραδοσιακούς τρόπους αντιμετώπισης επιθέσεων. Χρησιμοποιεί έξυπνες λύσεις που πηγάζουν από την ανάλυση παλαιότερων συμβάντων. Μαθαίνει χρησιμοποιώντας αλγόριθμους εκμάθησης και έπειτα βάση «εμπειρίας» βελτιώνει την άμυνα. Πρακτικά χρησιμοποιεί, εκπαιδεύει και αποτρέπει την απώλεια δεδομένων στον εξοπλισμό IoT ώστε να ανιχνεύσει ανωμαλίες και ανεπιθύμητες ενέργειες [2]. Μερικές από τις προτεινόμενες λύσεις που βασίζονται στο machine learning [37] [38] [39] είναι οι εξής:

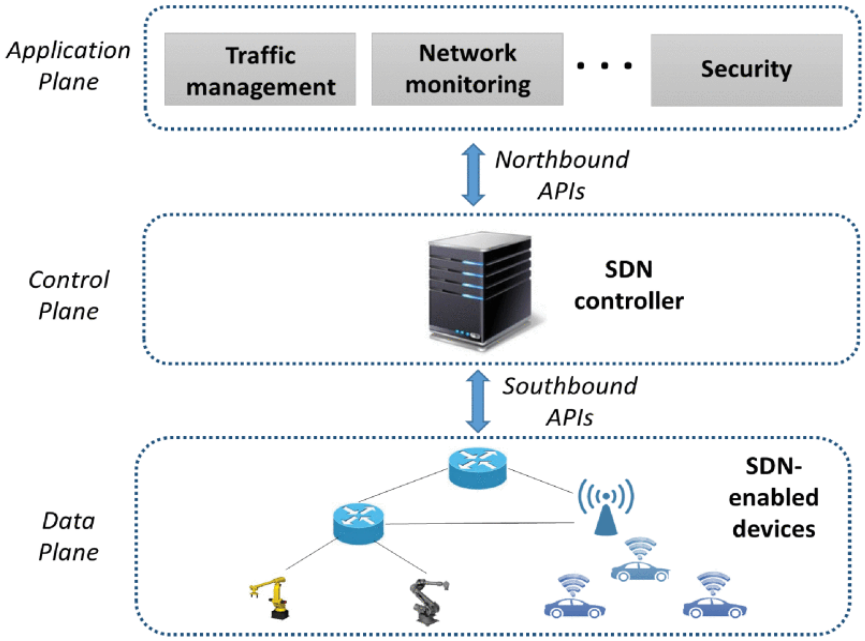
- Η εφαρμογή του πρωτόκολλου multilayer perception (MLP) για την διασφάλιση των δικτύων κατά των επιθέσεων **DoS**.
- Εφαρμογή machine learning τεχνικών όπως q-learn και Dyna-Q για την προστασία των συσκευών εναντίων των επιθέσεων **eavesdropping.**
- Η χρήση δακτυλικών αποτυπωμάτων, ένας οικονομικός και αξιόπιστος τρόπος που αυξάνει την εμπιστοσύνη στις συσκευές IoT.

6. Δίκτυα που καθορίζονται από λογισμικό (SDN)

Οι παραδοσιακές αρχιτεκτονικές δικτύου αδυνατούν να καλύψουν τις σύγχρονες ανάγκες των επιχειρήσεων, των παρόχων και των απλών χρηστών. Για το λόγο αυτό, τα δίκτυα που καθορίζονται από λογισμικό έχουν αναλάβει να μετασχηματίσουν την αρχιτεκτονική δικτύων [40]. Το SDN είναι πολλά υποσχόμενος τρόπος διασύνδεσης συσκευών Διαδικτύου των Πραγμάτων. Αυξάνει την δυνατότητα για προγραμματισμό των συσκευών και τον δυναμικό χειρισμό των πόρων του δικτύου. Αυτά τα χαρακτηριστικά αυξάνουν τις δυνατότητες διαχείρισης που έχει κάποιος στο δίκτυο. Παρέχει επιλογές για εφαρμογή τεχνικών που ενισχύουν την ασφάλεια και επιτρέπουν την καλύτερη αντιμετώπιση απειλών. Ακόμη απλοποιεί και αποφορτίζει το δίκτυο και αναλαμβάνει τους ελέγχους και τους χειρισμούς των συσκευών για πιο γρήγορη απόκριση και αποτελεσματικότητα σε περίπτωση βλάβης. Με την δημιουργία ενός πιο απλού προγραμματιζόμενου περιβάλλοντος, επιτρέπεται στις εφαρμογές να ορίζουν αυτές τη συμπεριφορά που ζητούν από το δίκτυο [41].

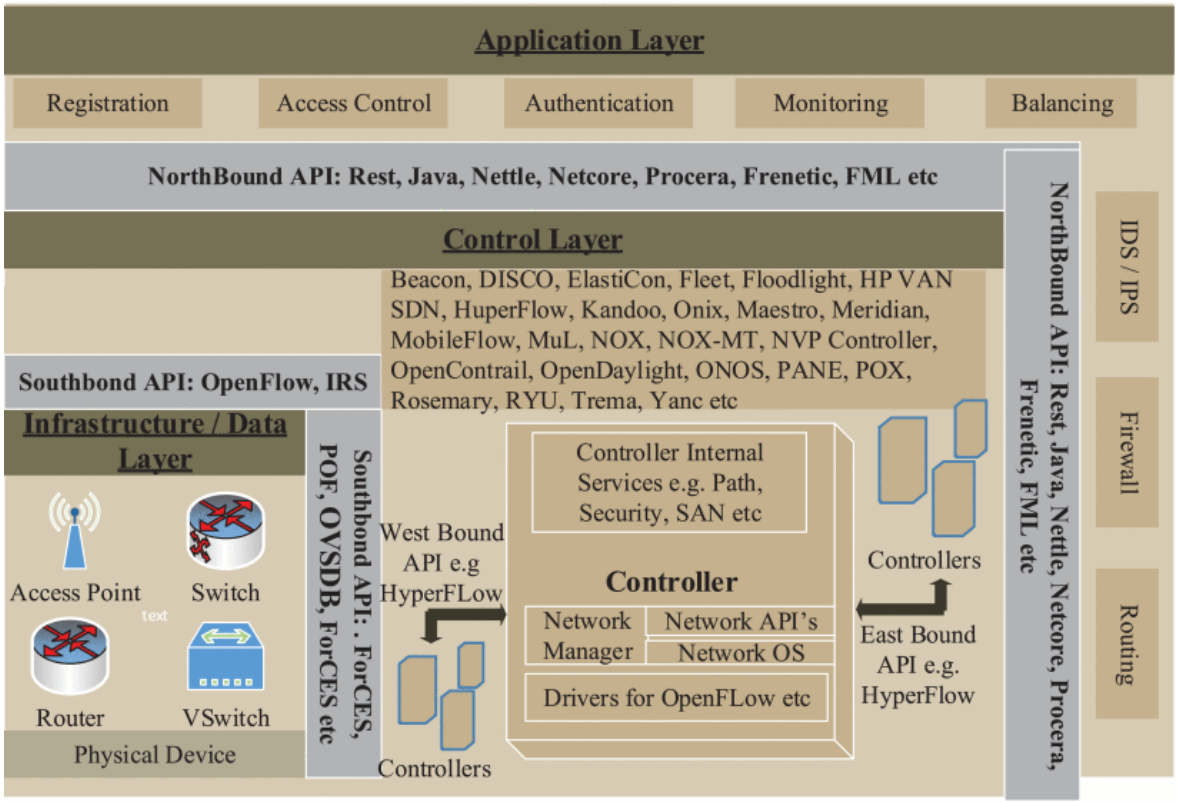
6.1 Αρχιτεκτονική SDN

Σύμφωνα με την ONF (Open Networking Foundation) [40], το μοντέλο αναφοράς της αρχιτεκτονικής του SDN αποτελείται από τρεις στιβάδες, τις εφαρμογές (applications), το επίπεδο ελέγχου (control plane) και το επίπεδο δεδομένων (data plane). Οι εφαρμογές που συντελούν το SDN ορίζουν τις προϋποθέσεις για τον έλεγχο της κίνησης στα δίκτυα μέσω των **Northbound APIs.** Ο **controller** είναι αυτός που, χειρίζεται το επίπεδο ελέγχου και γεφυρώνει το επίπεδο εφαρμογών με το επίπεδο δεδομένων, αναγνωρίζει τις ανάγκες των εφαρμογών και τις μεταφράζει σε ροές δεδομένων που πραγματοποιούνται από τους μεταγωγείς (switches) του δικτύου. Ο ρόλος του **Southbound API** είναι να παρέχει πρόσβαση στον controller, στις λειτουργίες των συσκευών SDN. Οι λειτουργίες αυτές μπορεί να αφορούν την δημιουργία αναφορών για την κατάσταση του δικτύου και την διαχείριση της προώθησης των πακέτων. Με τη χρήση τυποποιημένων διεπαφών, όπως το OpenFlow, επιτυγχάνεται η διαλειτουργικότητα μεταξύ των συσκευών του δικτύου που έχουν σχεδιαστεί από διαφορετικούς κατασκευαστές [41].



Εικόνα 14. The three layers in SDN architecture.

Πηγή: https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/9739/8649699/8424018/taleb4-2862350-large.gif



Εικόνα 15. SDN protocol stack.

Πηγή: https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6488907/9219268/9099839/abbas9-2997651-large.gif

6.2 Περιγραφή λειτουργίας και δυνατοτήτων SDN

Ένα δίκτυο που καθορίζεται από λογισμικά είναι αυτό που κάνει χρήση της αρχιτεκτονικής που του επιτρέπει τον προγραμματισμό του δικτύου κάνοντας χρήση καθορισμένων διεπαφών. Ένα δίκτυο που καθορίζεται από λογισμικό παρέχει τη δυνατότητα να δημιουργηθούν νέες υπηρεσίες και ποιο αποτελεσματικές εφαρμογές, λαμβάνοντας υπόψη την κίνηση, την ασφάλεια και τη ποιότητα του δικτύου [16].

Καθώς τα δίκτυα χαρακτηρίζονται από ετερογένεια, λόγο της μεγάλης διαθεσιμότητας υλικού και λογισμικού από διάφορους κατασκευαστές και λόγο των πολλών πρωτόκολλων δικτύωσης που χρησιμοποιούνται. Είναι δύσκολο να συντονίσει κανείς όλους αυτούς τους πόρους και να επιτύχει την ομαλή λειτουργία τους. Τα δίκτυα που καθορίζονται από λογισμικά δίνουν τη δυνατότητα διαχείρισης των πόρων, καθώς:

- Επιτρέπουν τον διαχωρισμό ανάμεσα σε υπηρεσίες του επιπέδου ελέγχου και του επιπέδου δεδομένων. Ο διαχωρισμός του επιπέδου ελέγχου από το επίπεδο προώθησης επιτρέπει την αφαίρεση λειτουργιών χαμηλού επιπέδου.
- Επιτρέπουν την αντιμετώπιση του δικτύου με βάση τη λογική, ώστε να πραγματοποιούνται τεχνικές βελτιστοποίησης. Εφαρμόζονται επίσης τεχνικές που ενισχύουν την αρχιτεκτονική με δικλείδες ασφαλείας και πλεονάζουσες συσκευές για την αποφυγή αστοχιών που προκύπτουν από έλλειψη εναλλακτικών οδών.
- Ακόμη επιτρέπουν τον προγραμματισμό του δικτύου ώστε να εισάγονται γρήγορα και δυναμικά νέες δικτυακές υπηρεσίες.

6.3 SDN βασισμένο στο πρωτόκολλο Open Flow

«Η ONF είναι μια μη κερδοσκοπική κοινοπραξία που ηγείται της εξέλιξης των SDN και της προτυποποίησης των κρίσιμων στοιχείων της αρχιτεκτονικής SDN, όπως το πρωτόκολλο Open Flow, το οποίο δομεί την διασύνδεση μεταξύ του επιπέδου ελέγχου και του επιπέδου δεδομένων σε συμβατές συσκευές δικτύου. Είναι η πρώτη στάνταρ διεπαφή που σχεδιάστηκε ειδικά για τα SDN. Παρέχει υψηλών επιδόσεων έλεγχο ροής μεταξύ συσκευών δικτύων

διαφόρων κατασκευαστών» [40]. Είναι πρωτόκολλο ανοιχτού κώδικα που αποτελεί βασικό μέρος στη δημιουργία δικτύων που καθορίζονται από λογισμικά. Επιτρέπει στους ελεγκτές (controllers) ενός δικτύου να καθορίζουν τις διαδρομές ροής μέσω των μεταγωγέων (switches). Έτσι επιτυγχάνεται η εύκολη διαχείριση της κυκλοφορίας μέσω του διαχωρισμού του επιπέδου ελέγχου από το επίπεδο προώθησης.

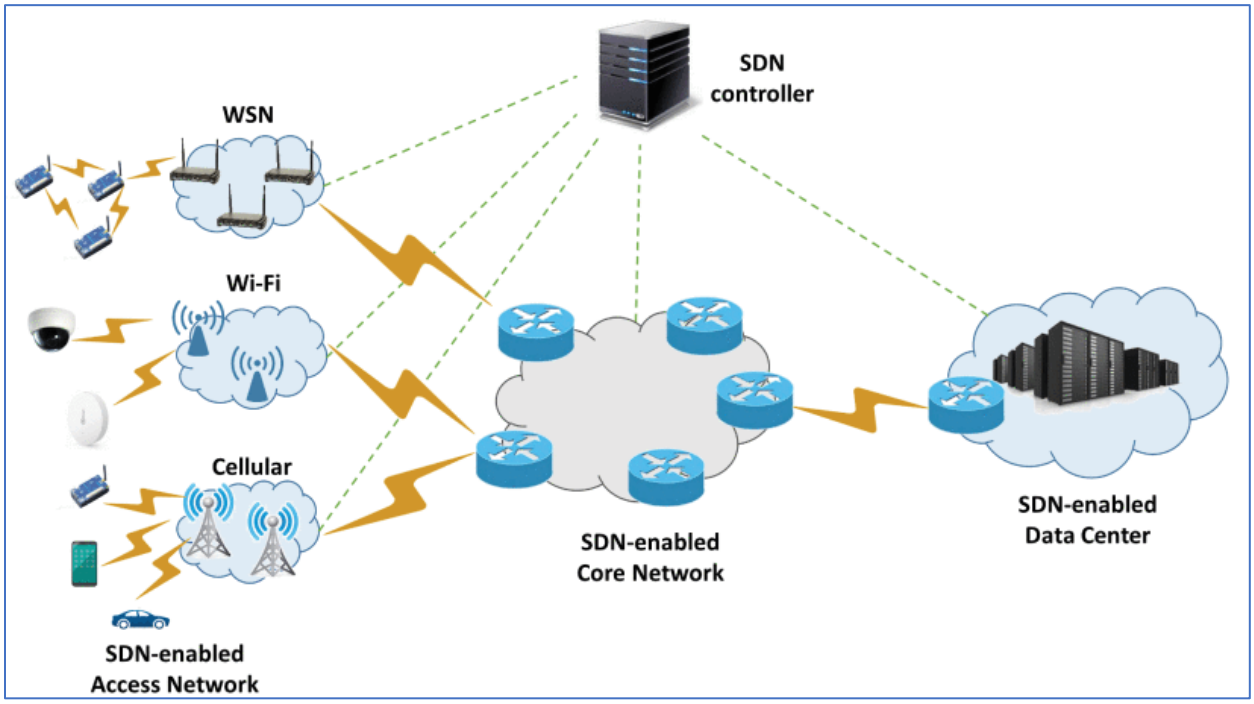
Ο μεταγωγέας OpenFlow διαθέτει ένα ή και περισσοτέρους πίνακες ροής, ένα πίνακα του συνόλου συσκευών, όπως επίσης και ένα κανάλι OpenFlow σε κάποιον εξωτερικό ελεγκτή. Με τους πίνακες, αναζητά και προωθεί πακέτα και με τον ελεγκτή SDN διαχειρίζεται τον μεταγωγέα μέσω του πρωτόκολλου OpenFlow. Έτσι λοιπόν ο ελεγκτής μπορεί να προσθέσει, να ανανεώσει και να διαγράψει ροές.

6.4 Περιγραφή λειτουργίας SDN Controller

Αποτελεί μια οντότητα λογισμικού που διαθέτει τον αποκλειστικό έλεγχο σε ένα αφηρημένο σύνολο πόρων που αποτελείται από δεδομένα. Συναντούμε διάφορες υλοποιήσεις ελεγκτών SDN ανοιχτού κώδικα, αναφορικά ONOS, ODL, Ryu, OK, NOX, Beacon κ.α. Οι εφαρμογές έχουν τη δυνατότητα να εκτελούνται πάνω από έναν SDN ελεγκτή ώστε να προσφέρουν προηγμένες υπηρεσίες δικτύου. Οι εφαρμογές ασφαλείας που κάνουν χρήση του SDN θα αναφερθούν αργότερα [16].

7. SDN και IoT

Η δυνατότητα της διαχειρισιμότητας που προσφέρει το SDN, το καθιστά κατάλληλο για τις εφαρμογές end-to-end στο Διαδίκτυο των Πραγμάτων. Μπορούμε να εφαρμόσουμε το SDN σε πολλά επίπεδα, όπως για παράδειγμα σε data center, σε δίκτυα κορμού (core) και σε δίκτυα πρόσβασης (access). Έτσι καλύπτουμε την κίνηση του Διαδικτύου των Πραγμάτων από τα δεδομένα των συσκευών, έως και τις υπηρεσίες νέφους που επεξεργάζονται αυτά τα δεδομένα. Κάθε επίπεδο του δικτύου έχει και διαφορετικές ανάγκες ως προς τη χρήση του SDN [42] [41]. Στο Διαδίκτυο των Πραγμάτων, υπάρχει η ανάγκη για ενοποίηση των ασύρματων και ενσύρματων δικτύων [43]. Η ποικιλομορφία που εμφανίζουν οι συσκευές IoT, από αισθητήρες περιορισμένων δυνατοτήτων έως και βιομηχανικούς εξοπλισμούς, οδηγεί στην δημιουργία πολλών διαφορετικών τρόπων διασύνδεσης. Τέτοιες λύσεις μπορεί να είναι τα δίκτυα μικρής εμβέλειας για τα WSNs και τα κυψελωτά δίκτυα χαμηλής ενέργειας για το 5G. Αυτή την ποικιλομορφία έρχεται να στηρίξει η χρήση του SDN, με την αποδοτική διαχείριση διαφορετικών συστημάτων Διαδικτύου των Πραγμάτων [41].



Εικόνα 16. Deployment scenarios of SDN paradigm for IoT systems.

Πηγή: https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/9739/8649699/8424018/taleb5-2862350-large.gif

7.1 Πώς το SDN συμβάλει στην ασφάλεια του IoT

Η τακτική των κατασκευαστών συσκευών διαδικτύου των πραγμάτων, να εμπλουτίζουν τα προϊόντα με δυνατότητες και λειτουργίες χωρίς να λαμβάνουν υπόψιν την ασφάλιση τους από διάφορες απειλές και προκλήσεις, σε συνδυασμό με τις περιορισμένες επεξεργαστικές δυνατότητες συσκευών αυτής της κατηγορίας καθιστούν τους παραδοσιακούς τρόπους ασφάλειας μη επαρκή και μη αξιοποιήσιμους [1].

Δημιουργείται η ανάγκη για προστασία σε χαμηλότερο επίπεδο, το επίπεδο του δικτύου, που δεν χρησιμοποιεί την επεξεργαστική ισχύ της συσκευής και δεν επηρεάζει την λειτουργία της. Σε αυτό το επίπεδο μπορεί να εφαρμοστεί ένα πρόγραμμα διαχείρισης δικτύου (SDN). Παρακάτω θα αναφερθούν τα χαρακτηριστικά που καθιστούν τα δίκτυα SDN καλή λύση για να ασφαλίσει κανείς την υποδομή του Διαδικτύου των Πραγμάτων.

Διαχωρισμός του επιπέδου ελέγχου από το επίπεδο δεδομένων: Με αυτό τον τρόπο μπορούμε να σχεδιάσουμε αρχιτεκτονικές ασφαλείας βασισμένες σε συγκεκριμένες πολιτικές (policy based) στον ελεγκτή (controller) του SDN στο επίπεδο ελέγχου και να εφαρμόζουμε τις διάφορες πολιτικές των συσκευών όπως switches και συσκευές του Διαδικτύου των Πραγμάτων στο επίπεδο δεδομένων. Ο controller επικοινωνεί με τα switches στο επίπεδο δεδομένων χρησιμοποιώντας ανοικτά και τυποποιημένα πρωτόκολλα (OpenFlow) και διεπαφές. Αυτό χρησιμεύει στην δημιουργία ασφαλούς επικοινωνίας μεταξύ του δημιουργού των πολιτικών ασφαλείας στον controller και των μηχανισμών υλοποίησης στις συσκευές IoT και τα switches.

Network Domain View (Εποπτεία Δικτύου): Ο ελεγκτής έχει τη δυνατότητα να παρακολουθεί ολόκληρο τον τομέα δικτύου που βρίσκεται στη δικαιοδοσία του. Με τον τρόπο αυτόν μπορούμε να πετύχουμε ασφαλή διαχείριση των συσκευών Δικτύου των Πραγμάτων και των ροών στην υποδομή του δικτύου. Δημιουργείται μια βάση δεδομένων στον ελεγκτή με πληροφορίες της τοπολογίας, όπου καταγράφονται πληροφορίες που αφορούν όλες τις συσκευές προώθησης που συνδέονται με τον ελεγκτή. Σε μια αρχιτεκτονική που βασίζεται σε πολιτικές ασφαλείας κάτι τέτοιο αποτελεί βασικό εργαλείο.

Dynamic Flow Control (Δυναμικός Έλεγχος Ροής): Σημαντικό χαρακτηριστικό του SDN αποτελεί η δυνατότητα του ελεγκτή (controller) να εγκαθιστά και να ανανεώνει κανόνες προώθησης, ώστε να διαχειρίζεται τις ροές των δεδομένων. Αυτή η δυνατότητα αυξάνει τη διαχειρισιμότητα του δικτύου και την πιθανότητα για εφαρμογή σωστών μηχανισμών ασφαλείας, όπως δυναμικών access control [44].

Security Network Programmability (Προγραμματισμός δικτύου ασφαλείας): Με την δυνατότητα για προγραμματισμό του δικτύου που παρέχεται από τον ελεγκτή του SDN, ενισχύεται η κατασκευή και η λειτουργία των εφαρμογών που παρέχουν ασφάλεια. Επίσης πλεονεκτήματα παρουσιάζονται και με την βελτίωση των northbound APIs και τη κατασκευή προγραμματιστικών γλωσσών για το SDN (SDN-oriented) [45].

Εφαρμογές SDN Northbound: Τα δίκτυα που καθορίζονται από λογισμικά παρέχουν northbound APIs και με αυτό τον τρόπο οι δημιουργοί έχουν τη δυνατότητα να παράγουν ασφαλή εφαρμογές ή ακόμη και να χρησιμοποιούν εφαρμογές τρίτων ώστε να ελέγχουν της συσκευές Διαδικτύου των Πραγμάτων και των κόμβων δικτύου SDN.

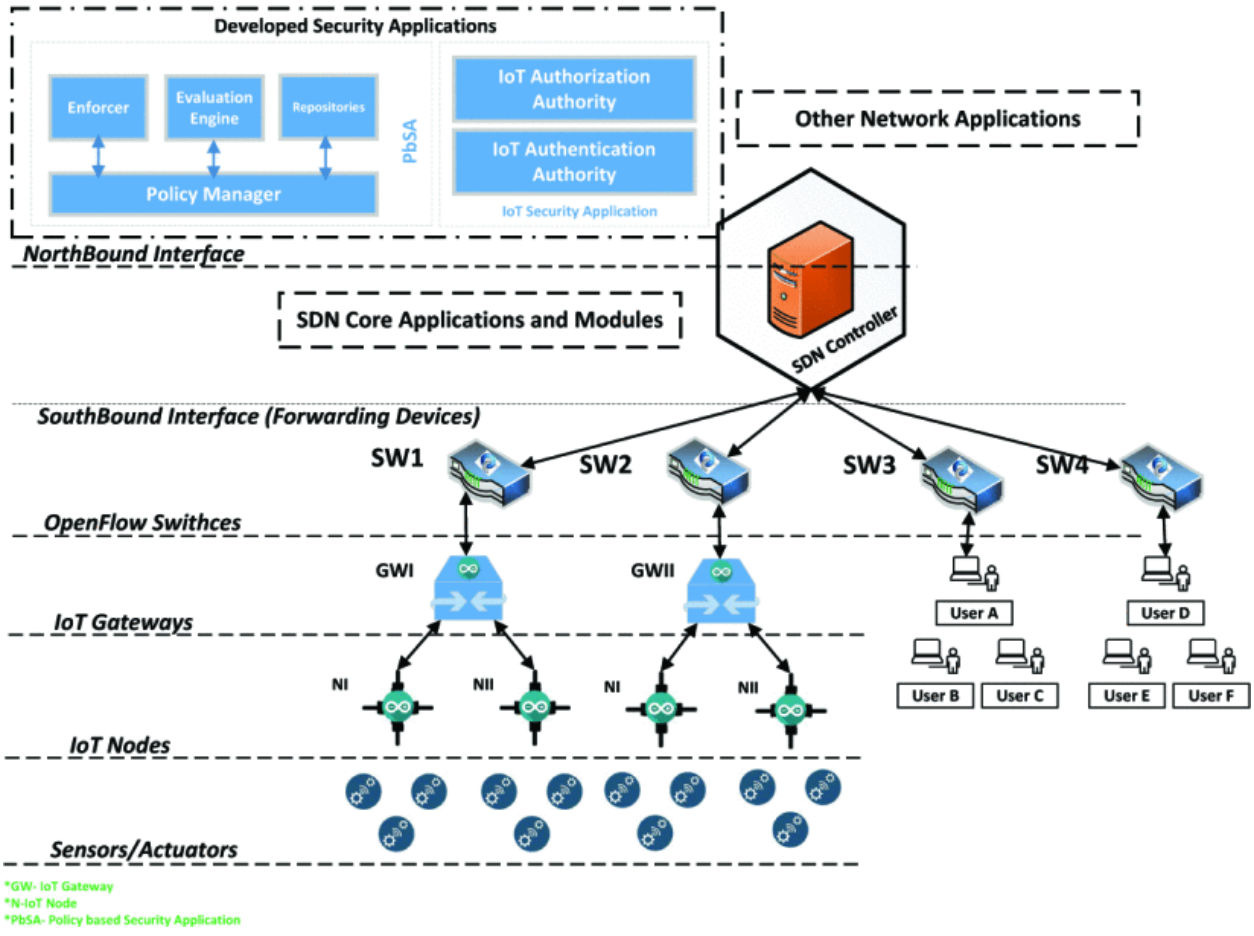
7.2 Προτάσεις αξιοποίησης SDN για ενίσχυση της ασφάλειας του IoT

7.2.1 Πρόταση των K.K.Karmakar V.Varadharajan S.Nepal U.Tupakula

Η συγκεκριμένη πρόταση χρησιμοποιεί πολιτικές (policies) για να ελέγξει τις συσκευές IoT, τις διεργασίες και άλλες συσκευές δικτύου όπως switches, κόμβους δικτύου και gateways. Την καρδιά της ασφάλειας αποτελεί controller όπου βρίσκονται και αξιολογούνται οι καθορισμένες πολιτικές ασφάλειας. Οι τελικές συσκευές IoT είναι οι αισθητήρες και οι ενεργοποιητές που συνδέονται στους κόμβους IoT. Οι IoT κόμβοι συνδέονται στις IoT πύλες (Gateways), είτε με ενσύρματο είτε με ασύρματο τρόπο. Οι IoT Gateways είναι συνδεμένες στον SDN Controller. Σε ορισμένες περιπτώσεις, τα OpenFlow switches δρουν και σαν IoT Gateways/Nodes. Στην υλοποίηση τους τα OpenFlow switches δρουν σαν IoT Gateways και οι χρήστες είναι συνδεμένοι σε αυτά.

Γίνεται χρήση συσκευών IoT διαφορετικής φύσεως με διαφορετικά πρωτόκολλα διασύνδεσης και μηχανισμούς ταυτοποίησης και λειτουργούν σε διάφορες πλατφόρμες λειτουργίας και

εφαρμογών. Για το λόγο αυτό κατέληξαν σε μια κλιμακούμενη λύση που να εξυπηρετεί τις διάφορες δυνατότητες των συσκευών IoT. Δημιουργήσαν ένα μηχανισμό επίβλεψης για κάθε γκρουπ συσκευών IoT βάση του προτύπου τους. Το κάθε πρότυπο διαφέρει σε πρωτόκολλο, κατασκευαστή, μηχανισμό ταυτοποίησης κ.α. Αυτή η λειτουργία ενσωματώνεται στην κύρια εφαρμογή του ελεγκτή και του δίνει τη δυνατότητα να ελέγχει τις IoT συσκευές κατά τη λειτουργία τους. Στη συγκεκριμένη υλοποίηση έχουμε δυο εφαρμογές ασφαλείας που εκτελούνται σε έναν SDN ελεγκτή και ελέγχουν τη συμπεριφορά των συσκευών IoT. Οι εφαρμογές ονομάζονται Policy based Security Application(PbSA) και IoT Security Application (ISA). Η εφαρμογή ISA έχει δυο υποεφαρμογές αναφορικά, την IoT Authentication Authority και την IoT Authorization Authority. Στην παρακάτω εικόνα βλέπουμε την αρχιτεκτονική ασφαλείας που βασίζεται σε SDN.



Εικόνα 17. Security Architecture for IoT Network Infrastructure.

Πηγή: https://ieeeInfrastructure.mediastore_new/IEEE/content/media/8713766/8717786/8717819/karma1-p5-karma-large.gif

7.2.2 Πρόταση Richard Vilalta et. al.

Στην περίπτωση αυτή [16] ο τελικός κόμβος SDN/NFV αποτελεί μια κατανεμημένη υπολογιστική υποδομή (fog computing) στην οποία πραγματοποιούνται κάποιες υπηρεσίες στο άκρο του δικτύου. Ο κόμβος αυτός έχει ως στόχο να βελτιώσει την αποτελεσματικότητα και να μειώσει τον όγκο δεδομένων που μεταφέρονται, για επεξεργασία, ανάλυση και αποθήκευση, στο cloud. Ως αποτέλεσμα έχουμε την βελτιστοποίηση του δικτύου αλλά και την ενίσχυση της ασφάλειας και της συμβατότητας.

Οι λειτουργίες του κόμβου fog είναι: Να αποτελεί ένα OpenFlow μεταγωγέα ώστε να χειρίζεται τις διάφορες συνδεμένες πύλες IoT και επιπλέον να συνδέει δίκτυα aggregation και δίκτυα transport.

Να λειτουργεί σαν εικονική μηχανή που εκτελεί διάφορες υπηρεσίες όπως μια βάση δεδομένων IoT, για την αποθήκευση στοιχείων από τις μετρήσεις αισθητήρων ώστε να επεξεργαστούν τοπικά.

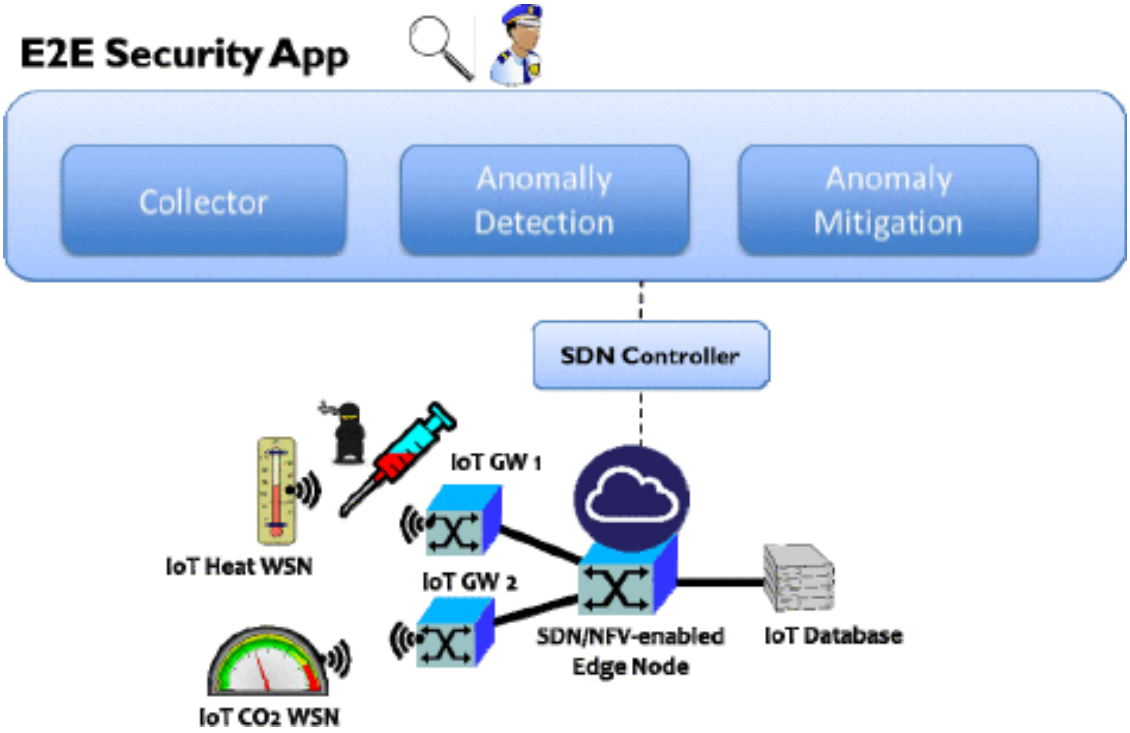
Οι λειτουργίες του SDN controller είναι: Να υποστηρίζει τη χρήση OpenFlow για τον έλεγχο των πινάκων της κίνησης των μέτρων και των ενεργειών.

Η **End-to-end εφαρμογή** θα επιβλέπει τις ροές χρησιμοποιώντας μηχανισμούς αναγνώρισης ανωμαλιών και θα αναγνωρίζονται οι κακόβουλες ροές. Έτσι, τελικά η εφαρμογή, που αποτελείται από τρία μέρη, τον συλλέκτη (collector), την ανίχνευση ανωμαλιών (Anomaly Detection) και την εξόντωση ανωμαλιών (Anomaly Mitigation), θα θέτει τις κατάλληλες πολιτικές ασφαλείας για την αντιμετώπιση των απειλών.

Ο **συλλέκτης (collector)** μαζεύει τα δεδομένα που αφορούν τις ροές και τα παραδίδει στο λειτουργικό μέρος της ανίχνευσης ανωμαλιών. Διάφορες ανωμαλίες που ανιχνεύονται στη ροή των δεδομένων, βοηθούν στην ανίχνευση των εισβολών ή των δυσλειτουργιών και προκύπτουν από την ανάλυση των στατιστικών.

Τα δεδομένα που παραδίδονται στο λειτουργικό μέρος της **ανίχνευσης ανωμαλιών** συλλέγονται σε διακριτά χρονικά παράθυρα. Έτσι, για κάθε παράθυρο εξετάζονται οι εισερχόμενες ροές και εμφανίζονται οι ανωμαλίες που προδίδουν τον θύτη ή αναδεικνύουν το

θύμα. Στο ρόλο της αντιμετώπισης των ανωμαλιών (anomaly mitigation) πραγματοποιείται προσπάθεια για την εξουδετέρωση των επιθέσεων. Στο σημείο αυτό εγκαθίστανται μέτρα, με υψηλότερη προτεραιότητα, στον πίνακα ροής του μεταγωγέα OpenFlow ώστε να μπλοκάρεται η κακόβουλη κίνηση.



Εικόνα 18 SDN-enabled security framework.

Πηγή:https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/7840067/7841475/7841889/7841889-fig-1-source-large.gif

8. Συμπεράσματα

Το Διαδίκτυο των Πράγματων (IoT) αποτελεί αναπόσπαστο κομμάτι της καθημερινότητας και η χρησιμότητα του, προσπερνά κάθε φαντασία. Η συνεχή εξέλιξη του προσελκύει όλο και περισσότερους εγκληματίες του κυβερνοχώρου που στοχεύουν στην εκμετάλλευση των ευπαθειών των συστημάτων IoT για την πραγματοποίηση κακόβουλων επιθέσεων. Οι συμβατικοί μηχανισμοί ασφαλείας έχουν αποδειχθεί αναποτελεσματικοί, λαμβάνοντας υπόψη την ετερογένεια, τη διεισδυτικότητα και την κινητικότητα των συσκευών IoT. Από την άλλη πλευρά, η δικτύωση με βάση το λογισμικό αλλάζει ραγδαία τη βιομηχανία τηλεπικοινωνιών, φέρνοντας την επανάσταση και στον τομέα της ασφάλειας του IoT.

Το SDN προτείνεται ως μια ευκαιρία για την επίλυση των προβλημάτων που αναφέρθηκαν προηγουμένως. Με το SDN, οι λογικές εφαρμογές υλοποιούνται σε ξεχωριστό επίπεδο, γεγονός που διευκολύνει την ανάπτυξη και την εγκατάσταση. Το SDN φιλοδοξεί να παρέχει στη δικτύωση μια κεντρική και ανοιχτή προγραμματιζόμενη διεπαφή.

Υπάρχουν αρκετές ερευνητικές προτάσεις τόσο σε ακαδημαϊκό επίπεδο όσο και σε τομείς της βιομηχανίας που προσπαθούν να αξιοποιήσουν τις δυνατότητες που παρέχει το SDN, έτσι ώστε με την κατάλληλη διαμόρφωσή του να παρέχει αποτελεσματικούς τρόπους αντιμετώπισης προκλήσεων και θεμάτων ασφάλειας στην υποδομή του IoT.

Υπό μια άλλη έννοια, το SDN δεν επιλύει κάποιο συγκεκριμένο πρόβλημα, αλλά επεκτείνει πιο ευέλικτους τρόπους για την αναβάθμιση της διαχείρισης του δικτύου IoT, συντελώντας στην αποδοτικότερη διαχείριση και ασφαλέστερη λειτουργία του.

Στη συγκεκριμένη εργασία παρουσιάστηκε η αρχιτεκτονική SDN και τα χαρακτηριστικά της, με ανάλυση των προοπτικών ασφάλειας που μπορεί να παρέχει. Έγινε αναφορά σε ερευνητικές προτάσεις και υλοποιήσεις, που εμπράκτως αποδεικνύουν τα οφέλη του SDN σε εφαρμογές IoT. Ωστόσο, η έρευνα στο συγκεκριμένο επιστημονικό πεδίο βρίσκεται σε φάση διαρκούς εξέλιξης και στο μέλλον αναμένονται περισσότερες και αποδοτικότερες προτάσεις αξιοποίησης του SDN προς όφελος των δικτυακών υποδομών και τεχνολογιών.

Βιβλιογραφία

[1] A. A. Hayajneh, Z. A. Bhuiyan και I. McAndrew, «Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN),» *Computers,* τόμ. 9, αρ. 1 IoT: Security, Privacy and Best Practices, 7 February 2020.

[2] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu και N. Bizon, «State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions,» *ustainability,* τόμ. 13, αρ. 16, p. 9463, Aug 2021.

[3] M. Lombardi, F. Pascale και D. Santaniello, «Internet of Things: A General Overview between Architectures, Protocols and Applications,» *Information,* τόμ. 12, αρ. 2, p. 87, 2021.

[4] Z. Shelby, P. Castellani και C. Borman, «CoAP: An Application Protocol for Billions of Tiny Internet Nodes,» *IEEE Internet Computing,* τόμ. 16, αρ. 02, pp. 62-67, Mar 2012.

[5] S. Cheshire και M. Krochmal, «Multicast DNS,» Feb 2013. [Ηλεκτρονικό]. Available: https://www.rfc-editor.org/info/rfc6762. [Πρόσβαση 17 Apr 2023].

[6] J. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand και C. Chauvenet, «RPL: The IP routing protocol designed for low power and lossy networks,» Apr 2011. [Ηλεκτρονικό]. Available: https://www.cse.chalmers.se/edu/year/2019/course/DAT300/PAPERS/rpl.pdf. [Πρόσβαση 17 Apr 2023].

[7] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis και R. Alexander, «RPL: IPv6 Routing Protocol for Low power and Lossy Networks,» 2012. [Ηλεκτρονικό]. Available: https://www.ietf.org/archive/id/draft-ietf-roll-rpl-13.html. [Πρόσβαση 17 Apr 2023].

[8] I. S. Association, «IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs),» 2011. [Ηλεκτρονικό]. Available: https://standards.ieee.org/ieee/802.15.4/5050/. [Πρόσβαση 18 Apr 2023].

[9] M. Hasan, E. Hossain και D. Niyato, «Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches,» *IEEE Communications Magazine,* τόμ. 51, αρ. 6, pp. 86-93, 10 June 2013.

[10] «IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies,» *IEEE Std 1905.1-2013,* τόμ. ., αρ. ., pp. 1-93, 12 April 2013.

[11] GeeksforGeeks, «User Datagram Protocol (UDP),» GeeksforGeeks, [Ηλεκτρονικό]. Available: https://www.geeksforgeeks.org/user-datagram-protocol-udp/.

[12] w. Iqbal, H. Abbas, M. Daneshmand, B. Rauf και Y. A. Bangash, «An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security,» *in IEEE Internet of Things Journal,* τόμ. 7, αρ. 10, pp. 10250-10276, Οκτ 2020.

[13] A. Mosenia και N. K. Jha, «A Comprehensive Study of Security of Internet-of-Things,» *IEEE Transactions on Emerging Topics in Computing,* τόμ. 5, αρ. 4, pp. 586-602, Oct-Dec 2017.

[14] V. V. S. N. a. U. T. K. K. Karmakar, «SDN Enabled Secure IoT Architecture,» σε *IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, Arlington, VA, USA, 2019.

[15] A. M. Nia, M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan και K. N. Jha, «Energy-efficient long-term continuous personal health monitoring,» *IEEE Transactions on Multi-Scale Computing Systems,* τόμ. 1, αρ. 2, pp. 85-98, 2015.

[16] R.Vilalta και et al, «Improving Security in Internet of Things with Software Defined Networking,» σε *IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, USA, 2016.

[17] F. Meneghello, M. Calore, D. Zucchetto, M. Polese και A. Zanella, «IoT: Internet of Threats? A Survey of Practical,» *IEEE Internet of Things Journal,* τόμ. 6, αρ. 5, pp. 8182- 8201, Οκτώβριος 2019.

[18] Y. Cherdantseva και J. Hilton, «A Reference Model of Information Assurance & Security,» σε *2013 International Conference on Availability*, Regensburg, Germany, 2013.

[19] j. M. Kizza, σε *Guide to Computer Network Security*, Germany, Springer, 2009, pp. 517-529.

[20] K. Dahbur, B. Mohammad και A. B. Tarakji, «A survey of risks, threats and vulnerabilities in cloud computing,» σε *2011 International Conference on Intelligent Semantic Web-Services and Applications (ISWSA '11)*, New York, 2011.

[21] C. Tankard, «Advanced Persistent threats and how to monitor and deter them,» *Network Security,* τόμ. 2011, αρ. 8, pp. 16-19, 2011.

[22] I. Butun, P. Österberg και H. Song, «Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures,» *IEEE Communications Surveys & Tutorials,* τόμ. 22, αρ. 1, pp. 616-644, 2019.

[23] S. Khanam, I. Ahmedy, M. Idris, M. Jaward και A. Sabri, «A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things,» *IEEE Access,* τόμ. 8, 2020.

[24] K. Hamlen, M. Kantarcioglu, L. Khan και B. Thuraisingham, «"Security issues for cloud computing,» *Int. J. Inf. Security Privacy,* τόμ. 4, αρ. 2, pp. 36-48, 2010.

[25] D. Puthal, S. Nepal, R. Ranjan και J. Chen, «Threats to networking cloud and edge datacenters in the Internet of Things,» *IEEE Cloud Comput.,* τόμ. 3, αρ. 3, pp. 64-71, May/Jun 2016.

[26] S. A. Kumar, T. Vealey και H. Srivastava, «Security in Internet of Things challenges solutions and future directions,» IEEE, Hawaii, 2016.

[27] J. Wurm, K. Hoang, O. Arias, A. -R. Sadeghi και Y. Jin, «Security analysis on consumer and industrial IoT devices,» Asia South Pac, 2016.

[28] P. Paganini, «securityaffairs,» 2014. [Ηλεκτρονικό]. Available: https://securityaffairs.co/wordpress/30320/security/microsoft-patch-kerberos-bug.html.

[Πρόσβαση Δεκεμβριος 2022].

[29] j. Wurm, O. Arias, K. Hoang και Y. Jin, «Privacy and security in Internet of Things and wearable devices,» *IEEE Trans. Multi-Scale Comput. Syst,* τόμ. 1, αρ. 2, pp. 99-109, Apr.–Jun 2015.

[30] B. Fowler, «Some top baby monitors lack basic security features report finds,» *nbc new york,* 2015.

[31] L. Qian, Z. Zhu, J. Hu και S. Liu, «Research of SQL injection attack and prevention technology,» σε *2015 International Conference on Estimation, Detection and Information Fusion (ICEDIF)*, Harbin, China, 2015.

[32] D. Miller, «Blockchain and the Internet of Things in the Industrial Sector,» *IT Professional,* τόμ. 20, αρ. 3, pp. 15-18, May/June 2018.

[33] A. Dastjerdi και R. Buyya, «Fog Computing: Helping the Internet of Things Realize Its Potential,» *Computer,* τόμ. 49, αρ. 8, pp. 112-116, Aug 2016.

[34] V. K. Sehgal, A. Patrick, A. Soni και L. Rajput, «Smart Human Security Framework Using Internet of Things, Cloud and Fog Computing,» σε *Intelligent Distributed Computing*, 2015.

[35] A. Alwaris, A. Alhothaily, C. Hu και X. Cheng, «Fog Computing for the Internet of Things: Security and Privacy Issues,» *IEEE Internet Computing,* τόμ. 21, αρ. 2, pp. 34-42, 2017.

[36] M. Mollah, M. Azad και A. Vasilakos, «Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things,» *IEEE Cloud Computing,* τόμ. 4, αρ. 1, pp. 34-42, Jan-Feb 2017.

[37] P. P. Ariza-Colpas, E. C. Ayala-Mantila, M.-A. Pineras-Melo, D. Villate-Daza, R. C. Morales-Oretega, E. De-la-Hoz-Franco, H. Sanchez-Moreno, S. B. Aziz και C. Collazos-Morales, «Multilayer Perception Applied to the IoT Systems for Identification of Saline Wedge in the Magdalena Estuary-Colombia,» *Computer Information Systems and Industrial Management,* pp. 235-244, 2021.

[38] L. Xiao, Y. Li, G. Han, G. Liu και W. Zhuang, «PHY-Layer Spoofing Detection With Reinforcement Learning in Wireless Networks,» *IEEE Transactions on Vehicular Technology,* τόμ. 65, αρ. 12, pp. 10037-10047, 2016.

[39] W. Yang, S. Wang, M. N. Sahri, N. M. Karie, M. Ahmed και C. Valli, «Biometrics for Internet-of-Things Security: A Review,» *Sensors,* τόμ. 21, αρ. 18, p. 6163, 2021.

[40] Open Networking Foundation, «https://opennetworking.org/,» Open Networking Foundation, 13 April 2012. [Ηλεκτρονικό]. Available: https://opennetworking.org/sdn-resources/whitepapers/software-defined-networking-the-new-norm-for-networks/. [Πρόσβαση 17 March 2023].

[41] I. Farris, T. Taleb, Y. Khettab και J. Song, «A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems,» *IEEE Communications Surveys & Tutorials,* τόμ. 21, αρ. 1, pp. 812-, 2018.

[42] S. M. a. A. V. V. S. Bera, «Software-Defined Networking for Internet of Things: A Survey,» *IEEE*

Internet of Things Journal, τόμ. 4, αρ. 6, pp. 1994-2008, 2017.

[43] F. G. e. al., «Software defined and virtualized wireless access in future wireless networks: scenarios and standards,» *IEEE Communications Magazine,* τόμ. 53, αρ. 6, pp. 26-34, 2015.

[44] C. Yoon et al, «Enabling security functions with SDN: A feasibility study,» *Computer Networks,* τόμ. 85, pp. 19-35, 2015.

[45] M. D. D. F. L. C. E. d. B. a. M. M. C. Trois, «A survey on SDN programming languages: Toward a taxonomy,» *IEEE Commun. Surveys Tuts,* τόμ. 18, αρ. 4, pp. 2687-2712, 2016.

[46] N. C. J. H. K. M. K. a. S. M. A. Singh, «Energy efficient and side-channel secure cryptographic hardware for IoT-edge nodes,» *IEEE Internet Things J.,* τόμ. 6, αρ. 1, pp. 421-434, Φεβρουαριος 2019.

[47] S. Bunia και M. S. Hsiao, «Hardware Trojan Attacks: Threat Analysis and Countermeasures,» σε *Proceedings of the IEEE*, 2014.

[48] T. D. Nadeau και G. Ken, SDN: Doftware Defined Networks, O'Reilly Media, Inc, 2013.

[49] O. Berthold και H. Langos, «Dummy traffic against long term intersection attacks,» σε *Proceedings of the 2nd international conference on Privacy enhancing technologies*, 2002.