ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΕΧΝΙΚΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΠΑΡΥΦΕΣ ΤΟΥ ΔΙΚΤΥΟΥ

ΕΥΑΓΓΕΛΙΔΟΥ ΓΕΣΘΗΜΑΝΗ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Κολομβάτσος Κωνσταντίνος
Επίκουρος Καθηγητής

Λαμία 4 Ιουλίου έτος 2022

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΕΧΝΙΚΕΣ ΚΥΒΕΡΝΟΑΦΑΛΕΙΑΣ ΣΤΙΣ ΠΑΡΥΦΕΣ ΤΟΥ ΔΙΚΤΥΟΥ

ΕΥΑΓΓΕΛΙΔΟΥ ΓΕΣΘΗΜΑΝΗ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Κολομβάτσος Κωνσταντίνος
Επίκουρος Καθηγητής

Λαμία 4 Ιουλίου έτος 2022

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

CYBER SECURITY TECHNIQUES AT THE EDGE OF THE NETWORK

EVANGELIDOU GESTHIMANI

FINAL THESIS

ADVISOR

Kolomvatsos Konstaninos
Assistant Professor

Lamia 4 July year 2022

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια .

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 04/07/2022

Ο – Η Δηλ.

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

ΠΕΡΙΛΗΨΗ

Με την πάροδο του χρόνου και τη διαρκή εξέλιξη της τεχνολογίας, το edge computing και το internet of things έχουν μπει για τα καλά στη ζωή μας, προσφέροντας μας δυνατότητες αλλά και απειλές σχετικά με την ασφάλεια των δεδομένων. Σε αυτήν την εργασία αναλύονται τόσο βασικές έννοιες, όσο και απειλές και μετρά ασφαλείας για την **υπολογιστική αιχμή** και το **διαδίκτυο των πραγμάτων**.

Πιο συγκεκριμένα στο πρώτο κεφαλαίο θα δούμε για το edge computing, όπου ουσιαστικά είναι η επεξεργασία και η αποθήκευση των δεδομένων όσο πιο κοντά στην πηγή που παράχθηκαν. Αναπτύχθηκαν διάφορες έννοιες, όπως είναι του cloud και fog computing για την καλύτερη κατανόηση του, άλλα και εφαρμογές στους διάφορους κλάδους όπου χρησιμοποιείται. Αν και έχει πολλά οφέλη, ωστόσο το γεγονός ότι διαχειρίζεται και αποθηκεύει πληροφορίες επιφυλάσσει κινδύνους ασφάλειας. Αφού τρίτα άτομα για δικά τους συμφέροντα μπορεί να θέλουν να επιτεθούν με στόχο να κλέψουν, να υποκλέψουν να τροποποιήσουν ή ακόμα και να διαγράψουν κρίσιμα δεδομένα. Έτσι τονίζεται η ανάγκη για την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων, και αναλύονται βασικά χαρακτηρίστηκα ασφάλειας. Τέλος, στο κεφάλαιο αυτό αναλύονται κάποιοι συγκεκριμένοι τύποι επιθέσεων (όπως είναι κακόβουλες ένεσης λογισμικού/ υλικού, κατανεμημένες επιθέσεις άρνησης εξυπηρετήσεις, επιθέσεις δρομολόγησης πληροφοριών και φυσικές επιθέσεις) αλλά και μετρά για να τις αντιμετωπίσουμε.

Ενώ στο δεύτερο κεφάλαιο που αναφερόμαστε στο Internet of Things (IoT) θα δούμε ότι ουσιαστικά είναι πολλές διασυνδεδεμένες συσκευές όπου συνδέονται στο διαδίκτυο και επικοινωνούν μεταξύ τους. Οι διάφορες αυτές διασυνδεδεμένες συσκευές μπορούν να κάνουν τόσο συλλογή των πληροφοριών, όσο και να δρουν με βάση τα δεδομένα αυτά. Για την καλύτερη κατανόηση του διαδικτύου των πραγμάτων αναλύονται τόσο η ιστορική εξέλιξη των τεχνολογιών για να φτάσει μέχρι το διαδίκτυο των πραγμάτων όπως το ξέρουμε σήμερα, άλλα και τα μοντέλα επικοινωνίας και μερικές από τις αρχιτεκτονικές του IoT. Καθώς το internet of things χρησιμοποιείται σε διάφορες πτυχές της ζωή μας, ίσως και χωρίς να το γνωρίζουμε και εφόσον έχει να κάνει και αυτό με δεδομένα καταλαβαίνουμε πως και εδώ υπάρχει κίνδυνος ασφάλεια από κυβερνοεπιθέσεις. Έτσι στις τελευταίες ενότητες αυτού του κεφαλαίου αναλύονται αρκετές από τις απειλές που υπάρχουν σε κάθε επίπεδο των αρχιτεκτονικών του Internet of things (όπως είναι για παράδειγμα: eavesdropping, node capture, fake node and malicious, timing attack, denial of service attack and distributed denial of service, man - in the middle attack, storage attack, exploit attack, cross-site scripting, malicious code attack, exhaustion, malwares, business logic attack, και zero day attack), αλλά και τεχνικές ανίχνευσης, αντιμετώπισης και πρόληψης των επιθέσεων αυτών.

Τέλος, σημαντικό κρίνεται να αναφέρουμε ότι το edge computing χρησιμοποιείται και σε συσκευές IoT, αν και σε πολλές περιπτώσεις υπάρχει μια σύγχυση στις εννοείς αυτές, ωστόσο δεν είναι το ίδιο. Το διαδίκτυο των πραγμάτων είναι μια τεχνολογία που κάνει χρήση της υπολογιστικής αιχμής.

ABSTRACT

Over time and the evolution of technology, edge computing and the Internet of things have entered our lives for good, offering us opportunities but also threats to data security. This work analyzes both basic concepts as well as threats and security measures for edge computing and the Internet of Things.

More specifically in the first chapter, we will see for Edge Computing where the data is essentially the processing and storage of the data as close to the source produced. Various concepts have been developed, such as cloud and fog computing for better understanding and applications in the various branches where it is used. Although it has many benefits, however, the fact that it manages and stores information reserves risks of security. Since thirds persons in their own interests may want to attack with the aim to stealing, to intercepting, to modify or even delete critical data. This emphasizes the need for confidentiality, integrity and availability of the data, and basic security features are analyzed. Finally, this chapter analyzes some specific types of attacks (such as malicious software/ hardware injection, distributed denial attacks services, information route attacks and physical attacks) but also measures to deal with them.

While in the second chapter we refer to the Internet of Things, we will see that there are essentially many interconnected devices where they are connected to the internet and communicating with each other. These various interconnected devices can both collect the information and act based on these data. For a better understanding of the internet of things, it is analyzed so much the historical evolution of technologies to reach the internet of things as we know it today, but also the different communication models and some of the IoT architects. While the Internet of Things is used in various aspects of our lives, perhaps even without knowing it, and since it has also to do with data, we understand that there is also a risk of cyberattacks. Thus in the latest sections of this chapter, several of the threats that exist at each level of the architectures of the Internet of Things are analyzed (such as: Eavesdropping, Node Capture, Fake Node and Malicious, Timing Attack, Denial of Service Attack and Distributed Denial of Service, Man - in the Middle Attack, Storage Attack, Exploit Attack, Cross -Site Scripting, Malicious Code Attack, Exhaustion, Malwares, Business Logic Attack, Zero Day Attack), as well as techniques for detecting, treating and preventing these attacks.

Finally, it is important to mention that Edge Computing is also used in IoT devices, although in many cases there is a confusion of these concepts, but they are not the same. The Internet of Things is a technology that makes use of edge computing.

Table of Contents

ΚΕΦΑΛΑΙΟ 1 EDGE COMPUTING

1.1 Εισαγωγή

Με τη διαρκή εξέλιξη της τεχνολογίας οι άνθρωποι χρησιμοποιούν ολοένα και περισσότερο συσκευές όπως είναι τα κινητά τηλέφωνα, τα έξυπνα ρολόγια, οι φορητοί και σταθεροί υπολογιστές κλπ. Οι συσκευές αυτές που εντάσσονται στην καθημερινότητα πιθανότατα των περισσότερων ανθρώπων αποτελούν κάποια παραδείγματα υπολογιστικών ακρών.

Με τον όρο υπολογιστική ακρών ή όπως αλλιώς συχνά αναφέρεται υπολογιστική αιχμής (Edge computing) εννοούμε κάθε υπολογιστική διαδικασία που υλοποιείται μέσω μιας συσκευής στην άκρη του δικτύου και όσο γίνεται πιο κοντά στην αρχική πηγή. Τέτοια υπολογιστική διαδικασία αποτελεί η επεξεργασία δεδομένων πελάτη όπου αντί τα δεδομένα να στέλνονται σε κάποιο κεντρικό διακομιστή για να επεξεργαστούν, να επεξεργάζονται σε κάποιο κοντινό σημείο από εκεί που δημιουργήθηκαν. Όπως καταλαβαίνουμε το edge computing είναι μια αρχιτεκτονική κατανεμημένης τεχνολογίας πληροφοριών (Information Technology - IT), στην όποια τα δεδομένα δεν μεταδίδονται ακατέργαστα σε κάποιο κεντρικό κέντρο δεδομένων αλλά αναλύονται ή επεξεργάζονται σε κάποιο σημείο κοντά στην πηγή των δεδομένων.

Εικόνα 1.1: "Υπολογιστική αιχμή"
Πηγή: IPTP Networks

Η εφαρμογή αυτής της αρχιτεκτονικής, της υπολογιστικής αιχμής, δίνει αποτελεσματική λύση σε προβλήματα δικτύου που προκύπτουν λόγω μετακινήσεις μεγάλου όγκου δεδομένων, συνήθως από οργανισμούς κατά την παραγωγή και κατανάλωση των δεδομένων αυτών.

Για να κατανοήσουμε όμως καλύτερα το Edge computing αρκεί να σκεφτούμε την «παραδοσιακή πληροφορική» όπου τα δεδομένα που "δημιουργεί" ο πελάτης με τη χρήση κάποιας εταιρικής εφαρμογής περνάνε μέσω του διαδικτύου και αποθηκεύονται και επεξεργάζονται στο εταιρικό LAN και από εκεί το αποτέλεσμα αποστέλλεται πίσω, πάλι μέσω διαδικτύου, για να φτάσει στη συσκευή του πελάτη. Αυτό έρχεται και καταρρίπτει το

edge computing “φέρνοντας” πιο κοντά το κεντρικό κέντρο δεδομένων στην πηγή που παράγονται τα δεδομένα, καθώς αντί να τα στέλνει σε μια τοποθεσία ίσως και χιλιάδες μιλιά μακριά, τα αποθηκεύει πιο κοντά στη συσκευή όπου δημιουργήθηκαν. Αντιμετωπίζοντας επιτυχώς έτσι τις διάφορες καθυστέρησης στη μεταφορά των δεδομένων που θα μπορούσαν να επηρεάσουν την απόδοση κάποιας εφαρμογής, ποσό μάλλον αν είναι πραγματικού χρόνου.

Ένα άλλο πιο χαρακτηριστικό παράδειγμα θα μπορούσε να ήταν οι κάμερες ασφάλειας που διαθέτουν σύνδεση στο διαδίκτυο για να παρακολουθούν ένα κτήριο. Το να καταγράφουν συνεχεία και να αποστέλλουν όλα τα δεδομένα σε έναν κεντρικό διακομιστή πχ του cloud και εκεί να γίνονται ανάλυση του βίντεο είναι πιο επίπονη διαδικασία για τον διακομιστή, καθώς ασκείτε πίεση να επεξεργαστεί τα διαφορά βίντεο από τις διάφορες κάμερες. Ενώ το edge computing δίνει αποτελεσματική λύση αφού προσφέρει την ικανότητα ανίχνευσης κινήσεις τοπικά σε κάθε κάμερα, για να αποστέλνονται έτσι μόνο σημαντικά τμήματα στον κεντρικό διακομιστή. Η κάμερες φυσικά για να το πετύχουν αυτό διαθέτουν αποθηκευτικό χώρο και επαρκή υπολογιστική ισχύ.

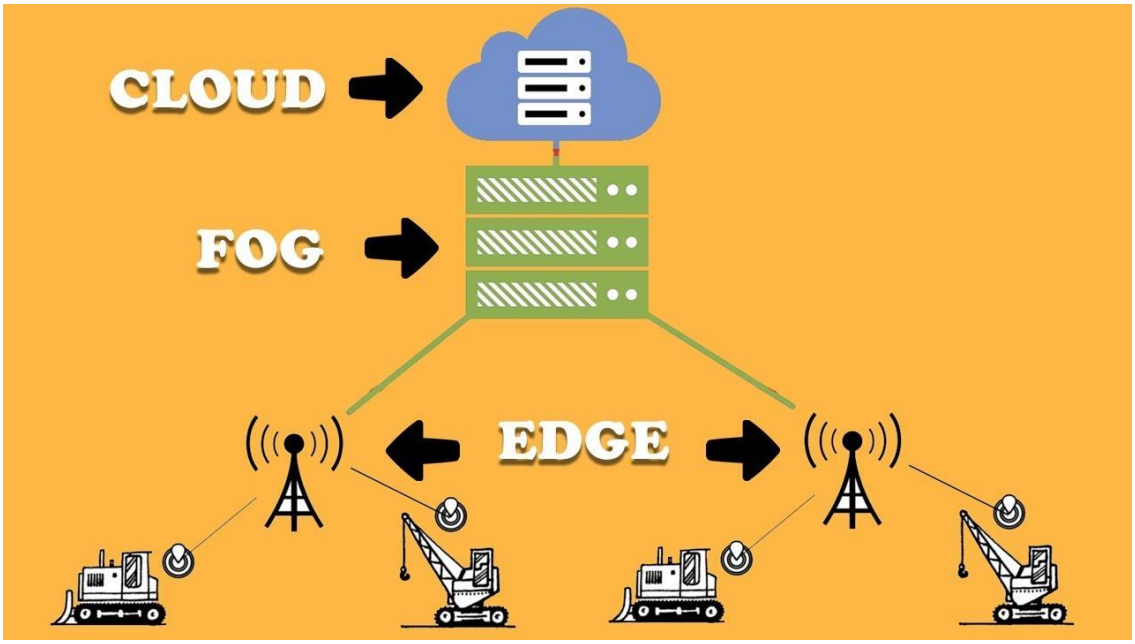
Τα πλεονεκτήματα της χρήσης της υπολογιστικής αιχμής ποικίλουν με το πιο τρανταχτό να είναι η μειώσει του χρόνου απόκρισης, ειδικά αν μιλάμε για παραδείγματα όπου τα δεδομένα πρέπει να σταλούν στην ίδια φυσική τοποθεσία (πχ κάποιο μήνυμα πρέπει να σταλεί από έναν υπάλληλο σε κάποιον άλλον στο ίδιο γραφείο). Προσφέροντας παράλληλα μείωση του κόστους αποδοτικότητας (αφού γίνεται εξοικονόμηση πόρων και εύρος ζώνης του διακομιστή με συνέπεια να υπάρχει και μείωση του κόστους) δίνοντας μεγαλύτερη ασφάλεια για το απόρρητο δεδομένων αλλά και πιο εύκολη συντήρηση των συσκευών και των συστημάτων αιχμής.

Ενώ από την άλλη πλευρά η περιορισμένη εμβέλεια που περιέχει και η ανάγκη για καλή συνδεσιμότητα για τη σωστή επεξεργασία των δεδομένων αποτελούν ένα σημαντικό πρόβλημα του edge computing.

1.2 Edge, cloud και fog computing

Για την καλύτερή κατανόηση του edge computing κρίνεται η ανάγκη της αποσαφηνίσεις των εννοιών του cloud computing (υπολογιστικό σύννεφο) και του fog computing (υπολογιστική ομίχλη), καθώς πολλές φόρες υπάρχει σύγχυση των εννοιών χωρίς όμως να είναι το ίδιο. Αυτό που «ενώνει» τις τρεις έννοιες είναι ότι σχετίζονται τόσο με τον υπολογισμό και τη φυσική ανάπτυξη υπολογιστικών πόρων, όσο και με την αποθήκευση των δεδομένων αυτών.

Αρχικά όπως είδαμε και παραπάνω στο edge computing τα δεδομένα στέλνονται όσο πιο κοντά στην πηγή που παράχθηκαν για να επεξεργαστούν και να αποθηκευτούν. Ουσιαστικά καταργεί την ανάγκη για αποστολή των δεδομένων σε κάποιον κεντρικό κέντρο για την επεξεργασία και την αποθήκευση πληροφοριών, καθώς οι διαδικασίες αυτές γίνονται πλέον σε κάποιο κοντινό σημείο από την πηγή που δημιουργήθηκαν τα δεδομένα. Ενώ σε μια ιδανική περίπτωση του edge computing η επεξεργασία και αποθήκευση δεδομένων θα γινόταν στο ίδιο ακριβώς σημείο από εκεί που παράχθηκαν. Ανεξάρτητα όμως από τον τρόπο επεξεργασίας και αποθήκευσης των δεδομένων, το edge computing δεν περιορίζει τη δυνατότητα αποστολής των δεδομένων που αποθηκευτήκαν σε κάποιο κεντρικό διακομιστή για περαιτέρω ανθρώπινη ανάλυση.

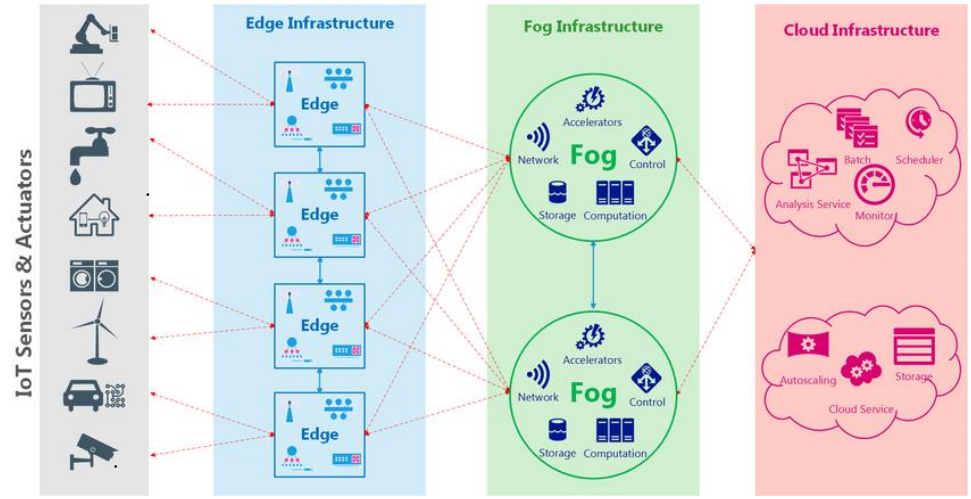


Εικόνα 1.2: "Υπολογιστική άκρη, υπολογιστική ομίχλη και υπολογιστικό σύννεφο"
Πηγή: YouTube

Από την άλλη πλευρά το cloud computing παρέχει υπολογιστικές υπηρεσιών (όπως για παράδειγμα διακομιστές, βάσεις δεδομένων, ανάλυση στοιχείων και μεθόδους τεχνίτης νοημοσύνης κλπ.), για να το πετύχει αυτό χρησιμοποιεί το διαδίκτυο. Έτσι ένα παράδειγμα θα μπορούσε να ήταν μια εταιρία που μπορεί αντί να έχει δικά της κέντρα δεδομένων να νοικιάζει από ένα πάροχο υπηρεσιών, όπως είναι το cloud. Ουσιαστικά το cloud computing αποτελεί μια μεγάλη και επεκτάσιμη ανάπτυξη υπολογιστικών πόρων και φυσικά πόρων αποθήκευσης σε μια από τις κατανεμημένες παγκόσμια τοποθεσία (Distributed global locations). Παρόλο όμως που το cloud computing προσφέρει πολλές υπηρεσίες η πιο κοντινή εγκατάστασή cloud μπορεί να είναι αρκετά μακριά από την πηγή που συλλέχθηκαν τα δεδομένα και αυτός είναι ο λόγος που μπορεί πολλές φορές να αποτελεί μια συμπληρωματική λύση του edge computing.

Εκτός όμως από το edge και cloud computing που είναι πιο διαδεδομένα για την ανάπτυξη υπολογιστικών και αποθηκευτικών πόρων υπάρχει και το fog computing. Στο fog computing οι υπολογιστικοί πόροι (όπως είναι τα δεδομένα, ο αποθηκευτικός χώρος κλπ.) βρίσκονται ανάμεσα στην πηγή που παράχθηκαν τα δεδομένα και του κέντρου δεδομένων του σύννεφου. Αποτελεί μια αποκεντρωμένη υπολογιστική υποδομή, όπου όπως είναι αναμενόμενο έχει να κάνει με διαφορές υπηρεσίες σχετικά με τη διαχείριση και ανάλυση δεδομένων. Αν και σε πολλές περίπτωσης βλέπουμε στενή σύνδεση του ορού το edge με τον fog computing δεν είναι το ίδιο, αφού το edge αποτελεί ένα υποσύνολο της ομίχλης. Ουσιαστικά η υπολογιστική ομίχλη ενσωματώνει τον υπολογισμό στις άκρες αλλά και τις δικτυώσεις για να φτάσουν τα δεδομένα στο τελικό σημείο.

Τέλος, όπως καταλαβαίνουμε ο κάθε όρος έχει τη δικιά του λειτουργία και η χρήση του εξαρτάται από την ανάγκη που έχουμε σε κάθε περίπτωση. Έτσι το edge, cloud και fog computing μπορεί να μην το ίδιο αλλά είναι αλληλένδετα κομμάτια και σε πολλά παραδείγματα συμπληρώνουν το ένα το άλλο για καλύτερα αποτελέσματα.



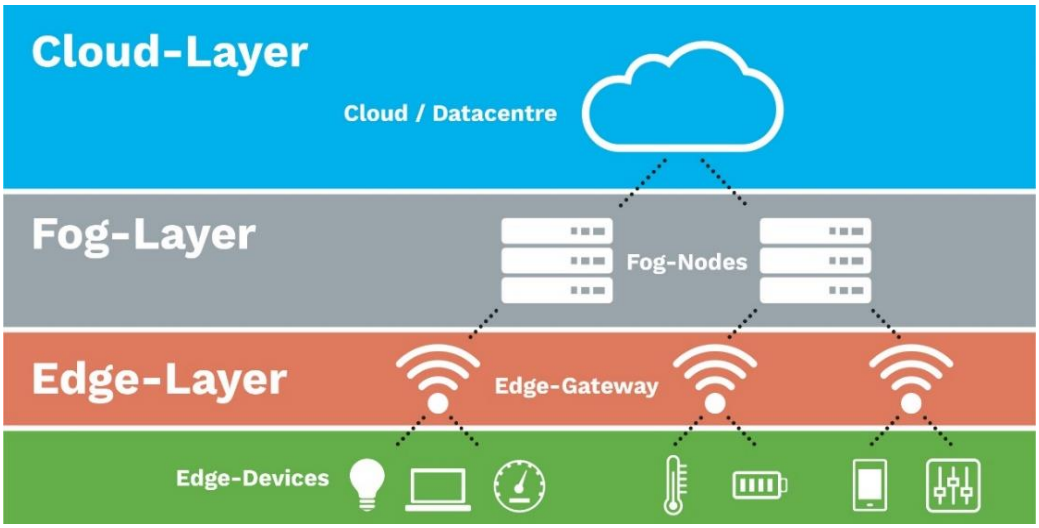
Εικόνα 1.3: "IoT – Edge, Fog and Cloud"
Πηγή: ResearchGate

1.3 Τεχνολογίες του edge computing

Όπως είδαμε και παραπάνω το edge με το cloud και το fog computing συμπληρώνουν το ένα το άλλο. Αυτός είναι κυρίως ο λόγος που σε πολλές περιπτώσεις εφαρμογών της υπολογιστικής αιχμής το υπολογιστικό σύννεφο και υπολογιστική ομίχλη δρουν ως εργαλείο για την υλοποίηση του edge computing και αρά κατά κάποιο τρόπο αποτελούν τεχνολογίες του.

Καθώς σε πολλές περιπτώσεις εφαρμογών που έχουμε σε υπολογίστηκες διαδικασίες στην άκρη μπορούμε να διαλέξουμε την καλύτερο τρόπο επεξεργασίας δεδομένων (δηλαδή cloud ή edge). Και κατά συνέπεια σε πολλά παραδείγματα το cloud computing έρχεται να βοηθήσει στην καλύτερη και αποτελεσματικότερη επεξεργασία δεδομένων στην υπολογιστικής αιχμής.

Παράλληλα ο υπολογισμός ομίχλης, όπου βρίσκεται ανάμεσα στην υπολογιστική αιχμή και στο υπολογιστικό σύννεφο, αποτελεί ένα ακόμα εργαλείο κατά τη διαδικασία της υπολογιστικής αιχμής. Αφού υποδομές που διαθέτει όπως το cloudlets και μικρά κέντρα δεδομένων αποτελούν διακομιστές ακμών και χρησιμοποιούνται για τοπική αποθήκευση ή υπολογιστικές διαδικασίες στο άκρο.



Εικόνα 1.4: "Edge, cloud and fog computing"
Πηγή: riello ups

Τέλος, ένα άλλο εργαλείο της υπολογιστικής αιχμής αποτελεί το Multi-Access Edge Computing (MEC), καθώς το MEC βάζει υπολογιστικούς και αποθηκευτικούς πόρους στο Δίκτυο Πρόσβασης Ραδιοφώνου (Radio Access Networks - RAN) βελτιώνοντας έτσι την αποτελεσματικότητα τόσο του δικτύου αλλά και της σωστής παράδοσης του περιεχομένου. Το RAN είναι ουσιαστικά το τμήμα που χρησιμοποιούν ραδιοφωνικούς και ασύρματους πόρους για επικοινωνία.

1.4 Εφαρμογές edge computing

Το edge computing αν και σαν όρος δεν ακούγεται τόσο συχνά ωστόσο χρησιμοποιείται σε διάφορους κλάδους, προσφέροντας αποτελεσματικές λύσεις σε διαφορά προβλήματα που έχει ο καθένας ξεχωριστά. Αφού το edge computing καταφέρνει τόσο να μειώσει την ποσότητα των δεδομένων που χρειάζεται να μετακινηθεί, όσο και την απόσταση που αυτά χρειάζονται να κάνουν.

Ένα σημαντικό παράδειγμα από τους κλάδους αυτούς αποτελεί ο κλάδος της υγείας και περίθαλψης ασθενών, καθώς ο όγκος δεδομένων που παράγεται είναι μεγάλος και το edge computing βοηθάει στον εντοπισμό ασθενών που χρειάζονται άμεση παρακολούθηση από κάποιον γιατρό. Αυτό το επιτυγχάνει με τη χρήση μηχανικής εκμάθησης και αυτοματοποίησης για πρόσβαση σε δεδομένα. Καταλαβαίνουμε ότι όταν έχουμε να κάνουμε με θέματα υγειά και συστήματα ιατρικής παρακολουθήσεις που χρειάζονται να είναι πραγματικού χρόνου για την καλύτερή αντιμετώπιση ιατρικών περιστατικών το edge computing αποτελεί καλύτερή λύση από το να περιμένουμε να ενεργήσει κάποιος διακομιστής cloud.

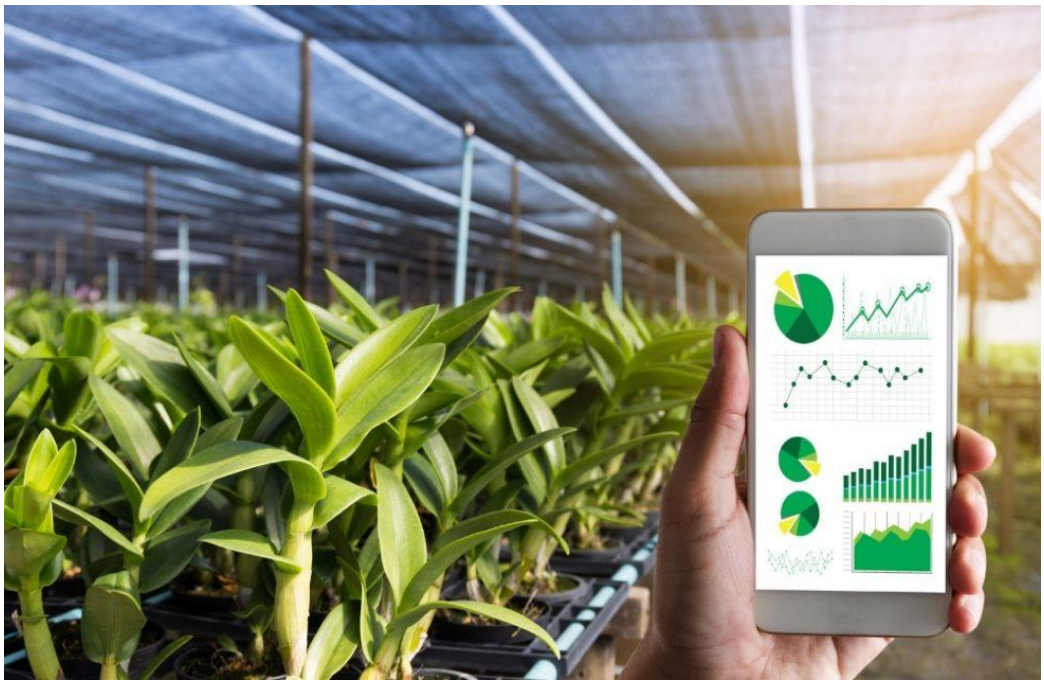
Εικόνα 1.5: "Υπολογιστική αιχμή και υγεία"
Πηγή: STARTUPPER

Εξίσου σημαντικός τομέας είναι ο τομέας της μεταφοράς όπου αν πάρουμε τα αυτόματα οχήματα που χρειάζεται η συλλογή και ανάλυση διαφορών δεδομένων (όπως η κατάσταση οχήματος, η τοποθεσία, οι συνθήκες δρόμου κλπ.) σε πραγματικό χρόνο κατά την κίνηση τους. Ο υπολογισμός αυτών των δεδομένων αποτελεί μια επίπονη διαδικασία αφού η ανταπόκριση σε δεδομένα που συνεχώς αλλάζουν και η λήψη αποφάσεις μέσα από αυτά αποτελεί σημαντικό πρόβλημα. Η επίλυση του προβλήματος έρχεται να δοθεί με το όχημα

να ‘μετατρέπεται’ και σε μηχάνημα υπολογισμού προσφέροντας έτσι ταχύτατη επεξεργασία δεδομένων.

Εικόνα 1.6: “Υπολογιστική αιχμή και οχήματα ”
Πηγή: DIGI

Άλλος κλάδος που έχει επηρεαστεί είναι η γεωργία όπου το edge computing έρχεται να βοηθήσει στη βελτιώσει τις καλλιέργειας και συλλογής των προϊόντων παραγωγής. Αυτό το επιτυγχάνει μέσω ανάλυσης δεδομένων που μαζεύονται από τους αισθητήρες για τις συνθήκες περιβάλλοντος, τη θερμοκρασία αλλά και το έδαφος, έτσι δεδομένα για τις θρεπτικές ουσίες που χρησιμοποιούνται αλλά και την ποσότητα νερού είναι άμεσα διαθέσιμα.



Εικόνα 1.7: “Υπολογιστική αιχμή και γεωργία”
Πηγή: InofA

Μερικοί ακόμα κλάδοι είναι το λιανεμπόριο και ο τομέας της βιομηχανοποίησης όπου και σε αυτές τις περιπτώσεις το edge computing έρχεται να βοηθήσει με τη συλλογή και ανάλυση δεδομένων. Στην πρώτη περίπτωση του λιανικού εμπορίου τα δεδομένα που συλλέγονται και αναλύονται δίνουν επιχειρηματικές ευκαιρίες. Ενώ στη δεύτερη περίπτωση δηλαδή της βιομηχανοποιήσεις τα δεδομένα που συλλέγονται και αναλύονται με το edge computing βελτιώνουν την παραγωγή προϊόντων και εύρεση λαθών κατά την παραγωγή. Για να το επιτύχει αυτό κάνει χρήση τόσο μηχανικής μάθησης όσο και ανάλυση σε πραγματικό χρόνο δεδομένων, όπως είναι τα δεδομένα κατά την παραγωγή και αποθεμάτων.

Εικόνα 1.8: "Υπολογιστική αιχμή, συλλογή δεδομένων"
Πηγή: ergo

Τέλος, το edge computing χρησιμοποιείται και σε συσκευές IoT (Internet of Things), αν και σε πολλές περιπτώσεις υπάρχει μια σύγχυση στις εννοείς αυτές, ωστόσο δεν είναι το ίδιο. Το διαδίκτυο των πραγμάτων είναι μια τεχνολογία που κάνει χρήση της υπολογιστικής αιχμής. Οι διαφορές έξυπνες συσκευές του διαδικτύου των πραγμάτων ωφελούνται από τον κώδικα που υπάρχει και τρέχει σε αυτές από το να περιμένουν το cloud. Περισσότερα για το διαδίκτυο των πραγμάτων αναλύονται στο κεφάλαιο 2 της εργασίας αυτής.

1.5 Κυβερνοασφάλεια και κίνδυνοι ασφαλείας

Η άνοδος του edge computing όπου τα δεδομένα αποθηκεύονταν και επεξεργάζονταν σε μικρά κέντρα κοντά στην πηγή που παράχθηκαν, μας πάει ένα βήμα πίσω, καθώς τον τελευταίο καιρό πρωταρχικό ρόλο στην επεξεργασία και αποθήκευση δεδομένων είχαν τα κέντρα δεδομένων ή οι διακομιστές του cloud. Αυτό αν και συνεπάγεται μια δυναμική προσέγγιση εγκυμονεί κίνδυνους ασφάλειάς. Αφού αν σκεφτόμαστε τον έλεγχο των διαφορετικών συσκευών και κέντρων που μπορούν να επεξεργαστούν και αποθηκευτούν τα δεδομένα, με τη χρήση του edge computing σε σύγκριση με τη διαχείριση και την προστασία τους σε ένα βασικό διακομιστή πχ μιας εταιρίας, αποτελεί πρόβλημα.

Εικόνα 1.9: "Υπολογιστική αιχμή"
Πηγή: NOKIA

Αυτός είναι και ο κύριος λόγος που υπάρχουν κίνδυνοι ασφάλειας στο edge computing, καθώς είναι δύσκολος ο έλεγχος τόσο σε ψηφιακό επίπεδο όσο και σε φυσικό επίπεδο. Έτσι σε φυσικό επίπεδό τα δεδομένα είναι εύκολα πολλές φορές να αντιγραφούν με ένα απλό στικάκι ή ακόμα με μια απλή αφαίρεση του σκληρό δίσκο να πάρει κάποιος τρίτος πρόσβαση στα δεδομένα. Από την άλλη πλευρά σε ψηφιακό επίπεδο η κωδικοί πρόσβασης και έλεγχος ταυτότητας μπορεί να αποτελέσει ένα μειονέκτημα για το edge computing. Καθώς κατά τη διάρκεια του edge computing οι συσκευές όπου συμμετέχουν στη διαδικασία μπορεί να έχουν χαμηλή πειθαρχεία για τους κωδικούς και αν δεν έχουν κάποιο εμπειρογνώμονα που να ασχολείται με την ασφάλεια στις συσκευές αυτές, μπορεί πολύ εύκολα να αποτελέσει τρωτό σημείο για κάποιο χάκερ. Αρά με μια απλή παραβίαση στα πρωτοκολλά κωδικών θα μπορούσαν να πάρει πρόσβαση κάποιος μη εξουσιοδοτημένος χρήστης σε σημαντικές πληροφορίες.

Η παρέμβαση ενός κακόβουλου χρήστη και ουσιαστικά η παρακολούθηση των δεδομένων που παράγονται και αποθηκεύονται κατά το edge computing θα μπορούσε να αποτελέσει σημαντικό κίνδυνο ασφάλειας. Αυτό μπορούμε να το κατανοήσουμε καλύτερα μέσα από ένα απλό παράδειγμα όπως είναι το έξυπνο σπίτι, καθώς αν ο κακόβουλος χρήστης μπορεί και βλέπει τις πληροφορίες σχετικά με το που λειτουργεί το ηλεκτρικό ρεύμα θα μπορούσε να ξέρει κατά ποσό το σπίτι είναι άδειο ή όχι και αρά να χρησιμοποιήσει τις πληροφορίες αυτές για να διαρρήξει το σπίτι την κατάλληλη στιγμή.

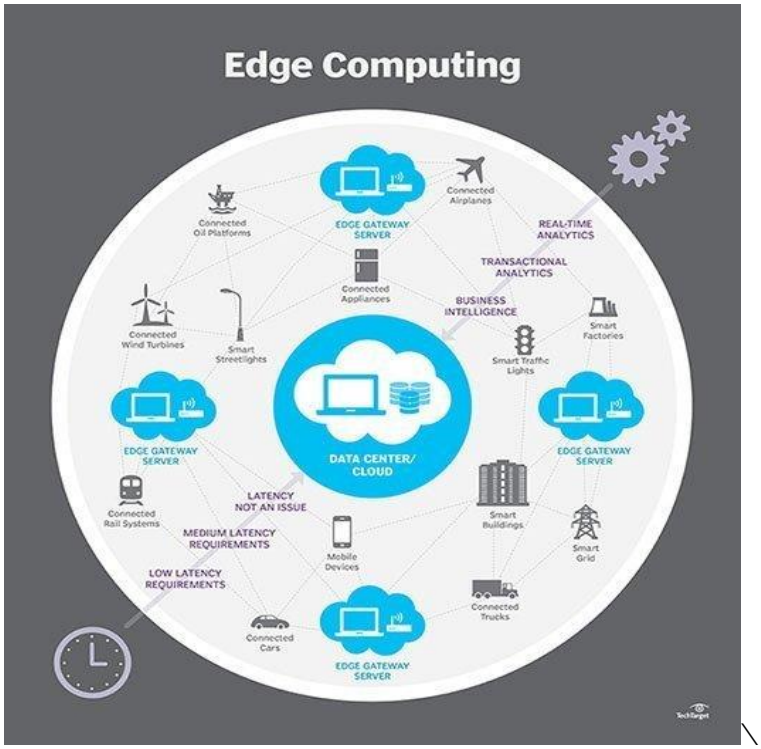
Εικόνα 1.10: "Κυβερνοασφάλεια και υπολογιστική άκρη"
Πηγή: Snowdrop

Έτσι μας γίνεται αντιληπτή η ανάγκη για προστασία κατά τη διάρκεια της υπολογιστικής αιχμής στον κυβερνοχώρο (όπου με τον όρο αυτόν εννοούμε το περιβάλλον που έχει δημιουργηθεί από τα δίκτυα επικοινωνιών με τη χρήση ηλεκτρονικών υπολογιστών), ώστε να αποφύγουμε τυχών ανεπιθύμητες ενέργειες από τρίτα άτομα ή ακόμα και από μια ομάδα ατόμων. Καθώς όταν κάποιος ή κάποιοι προσπαθούν να καταστρέψουν, να τροποποιήσουν, να κλέψουν, να υποκλέψουν ή απλώς να πάρουν πρόσβαση σε μη εξουσιοδοτημένες πληροφορίες μέσω του κυβερνοχώρου τότε μιλάμε για κυβερνοεπιθέσεις (Cyber-attack). Το πρόβλημα των κυβερνοεπιθέσεων έρχεται να λύσει η κυβερνοασφάλεια, όπου με τον όρο αυτό δεν εννοούμε μόνο την προστασία δικτύων και πληροφοριών από τυχόν κυβερνοεπιθέσεις, αλλά και την αντιμετώπιση κάθε παράνομης δραστηριότητας με τη χρήση ψηφιακών τεχνολογιών στον κυβερνοχώρο.

Παρακάτω θα αναλύσουμε κάποιες από τις απειλές και τις επιθέσεις για το edge computing, καθώς και μετρά αντιμετώπισης. Αλλά πριν γίνει αυτό κρίνεται απαραίτητο η εκτενέστερη ανάλυση τόσο της ασφάλεια δεδομένων και απορρήτου (ενότητά 1.3.1), όσο και να ορίσουμε την ασφάλεια που θα έπρεπε να έχουμε για το edge computing (ενότητα 1.3.2).

1.5.α Ασφάλεια δεδομένων και απορρήτου

Στις μέρες μας αναμφίβολα ζούμε στην “κοινωνία της πληροφορίας”, αφού σημαντικό κομμάτι της αποτελεί τόσο η παραγωγή και η χρήση των πληροφοριών, όσο και η διαχείριση τους γενικότερα. Οι πληροφορίες αυτές μπορούν να δώσουν ανταγωνιστικά πλεονεκτήματα αλλά η ασφάλεια τους κατά τη διάρκεια της παραγωγής, διαχείρισης και χρήσης τους αποτελεί ένα σημαντικό πρόβλημα γενικότερα αλλά και ειδικά κατά τη διάρκεια της χρήσης του edge computing. Στο edge computing τα δεδομένα που αποθηκεύονται στα κέντρα δεδομένων κοντά στην άκρη του δικτύου, μπορούν να ανατεθούν σε τρίτους χωρίζοντας έτσι ουσιαστικά την ιδιοκτησία τους και τον έλεγχο τους. Για τον λόγο αυτό, μπορεί να υπάρξει εύκολα τόσο απώλεια των δεδομένων, όσο και άλλες παράνομές δραστηριότητες, όπως διαρροή των πληροφοριών κλπ.



Εικόνα 1.11: "Υπολογιστική άκρη"
Πηγή: TechTarget

Για να εξασφαλιστεί η ασφάλεια των δεδομένων και του απορρήτου κατά τη διάρκεια χρήσης του edge computing, αρχικά θα πρέπει να υπάρχει **εμπιστευτικότητα** των δεδομένων αυτών, δηλαδή να μην επιτρέπει πρόσβαση σε τρίτα άτομα που δεν έχουν εξουσιοδοτηθεί τόσο κατά τη μετάδοση και λήψη των δεδομένων στις άκρες ή στα δίκτυα, όσο και κατά τη διάρκεια της επεξεργασίας και αποθήκευσης στα κέντρα του edge. Εξασφαλίζοντας παράλληλα την **ακεραιότητα** των δεδομένων αυτών σε όλη τη διάρκεια της διαδικασίας, χωρίς να υπάρχει δηλαδή τροποποίηση των πληροφοριών. Όπως επίσης να υπάρχει **διαθεσιμότητα** των δεδομένων αυτών σε όλους τους εξουσιοδοτημένους χρήστες, η ικανότητα δηλαδή της πρόσβασης στις υπηρεσίες αιχμής σύμφωνα πάντα με τις απαιτήσεις των χρηστών.

Ωστόσο, οι απαιτήσεις των δεδομένων και του απορρήτου δε σταματάνε εκεί καθώς ο **έλεγχος ταυτότητας** και **έλεγχος πρόσβασης** είναι απαραίτητος. Όπου με τον έλεγχος της ταυτότητας, εννοούμε να ελέγχει κατά πόσο ένας χρήστης είναι εξουσιοδοτημένος, ουσιαστικά είναι η ταυτοποίηση ενός χρήστη. Ενώ από την άλλη πλευρά ο έλεγχος πρόσβασης αποτελεί σημείο αναφοράς τόσο για την ταυτοποίηση του χρήστη, όσο και για το τι είδους ενέργειες μπορεί να κάνει ο κάθε χρήστης.

Για την εξασφάλιση της ύπαρξης όλων των παραπάνω (εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητα, έλεγχος ταυτότητας και πρόσβασης) υπάρχουν μηχανισμοί ασφάλειας μέσα σε αυτούς είναι και η κρυπτογράφηση όπου διασφαλίζουν την ασφάλεια του απορρήτου στην υπολογιστική αιχμή. Οι μηχανισμοί ασφαλείας αυτοί προσφέρουν ασφάλεια τόσο στα δεδομένα όσο και στον χρήστη εξασφαλίζοντας μυστικότητα για την ταυτότητα του και τοποθεσία του.

1.5.β Βασικά χαρακτηρίστηκα ασφαλείας

Πέρα όμως από την ασφάλεια απορρήτου και δεδομένων, όπου μιλήσαμε παραπάνω, στο edge computing για να μιλήσουμε για ασφάλεια θα πρέπει να πληρούνται κάποια βασικά χαρακτηριστικά, τα όποια θα πρέπει να υπάρχουν σε διάφορες πτυχές της άκρης, έτσι ώστε να εξασφαλίζουν την ασφάλεια σε όλοι τη διαδικασία της υπολογιστικής αιχμής.

Αρχικά για να πούμε ότι το edge είναι ασφαλές θα πρέπει να κάνει τόσο **χρήση κρυπτογράφησης όσο και χρήση των τειχών προστασίας και των ελέγχων προστασίας** πριν δοθεί πρόσβαση σε υπολογιστικούς πόρους. Στόχος, η βασική ασφάλεια και η εξασφάλιση, έως ένα βαθμό, ότι θα δεν υπάρξουν παρεμβάσεις από μη εξουσιοδοτημένα άτομα κατά τη διαδικασία του edge computing. Ωστόσο, εκτός από την κρυπτογράφηση, τη χρήση τειχών και ελέγχων προστασίας δε θα πρέπει να μένει η ασφάλεια εκεί, καθώς η **έγκαιρη ανίχνευση των διάφορων απειλών** μέσω τεχνολογιών είναι απαραίτητη για την πρόβλεψη των απειλών και όπως είναι αναμενόμενο την όσο πιο δυνατόν αποτελεσματική αντιμετώπιση των επιθέσεων.

Εικόνα 1.12: "Ασφάλεια στην υπολογιστική αιχμή"
Πηγή: Schneider Electric

Επιπλέον οι διαφορές εφαρμογές που χρησιμοποιούν οι συσκευές edge θα πρέπει να είναι ασφαλής πέρα από την ασφάλεια του δίκτυο, προσφέροντας έτσι ένα μεγαλύτερο επίπεδο προστασίας.

Τέλος, βασικά κομμάτια ασφαλείας όπως είναι η **συνεχείς συντήρηση** για την ανακάλυψη τρωτών σημείων αλλά και η **αυτόματη ενημέρωση του κώδικα** στις συσκευές για όσο γίνεται καλύτερη προστασία από πιθανών επιθέσεις, ισχύουν και για την ασφάλεια στις άκρες.

1.6 Απειλές στο edge computing και αντίμετρα

Με τη ραγδαία εξάπλωση του edge computing σε διαφόρους τομείς το θέμα της ασφάλειας από τυχόν επιθέσεις κρίνεται ζωτικής σημασίας. Η προστασία πληροφοριών αλλά και η ασφάλεια κατά τη διαχείριση τους είναι απαραίτητη και κατά τη διάρκεια του edge computing. Αφού ευαίσθητες πληροφορίες μπορούν να διαρρεύσουν, να τροποποιηθούν, ακόμα και να διαγράφουν προς όφελος κάποιων αντιπάλων (είτε μιλάμε για επιχειρήσεις, είτε για οργανισμούς που κάνουν χρήστη της υπολογιστικής αιχμής).

Εικόνα 1.13: "Υπολογιστική άκρη και κυβερνοασφάλεια"

Πηγή: Medium

Παρακάτω αναλύονται κάποιοι κίνδυνοι και απειλές ασφάλειας στο edge computing καθώς και μέτρα αντιμετώπισης των επιθέσεων αυτών:

1.6.α Malicious Software/Hardware Injection

Μια από αυτές τις απειλές αποτελεί η κακόβουλη ένεση είτε λογισμικού είτε υλικού (**Malicious Software/Hardware Injection**), ουσιαστικά σε αυτήν την επίθεση εισάγεται κακόβουλο λογισμικό ή υλικό στα επίπεδα της επικοινωνίας ή στους κόμβους του edge computing επιτρέποντας έτσι σε μη εξουσιοδοτημένα άτομα να παρακάμψουν τον έλεγχο ταυτότητας και έτσι να έχουν πρόσβαση στα δεδομένα που μπορούν τόσο να τα κλέψουν όσο και να τα τροποποιήσουν προσθέτοντας ψευδής στοιχεία με αποτέλεσμα η βάση δεδομένων να χάνει την ακεραιότητα της. Οι βάσεις αυτές μπορεί να περιέχουν ευαίσθητες πληροφορίες χρηστών πράγμα που καθιστά εξαιρετικά επικίνδυνο να έχει πρόσβαση κάποιος κακόβουλος χρήστης σε αυτές.

Αρχικά η **ένεση λογισμικού** έχει να κάνει με κάποιο κενό ασφαλείας το όποιο εκμεταλλεύεται ο επιτιθέμενος με σκοπό να πάρει πρόσβαση στα δεδομένα, να τα αλλάξει ή ακόμα και να τα διαγράψει. Χρησιμοποιώντας ουσιαστικά ο δράστης κακόβουλες εντολές - κώδικα με σκοπό να επηρεάσει προκαθορισμένες εντολές κατά τη διάρκεια εκτέλεσης τους.

Εικόνα 1.14: "Ένεση"
Πηγή: simplilearn

Από την άλλη πλευρά οι επιθέσεις με **ένεση υλικού** μπορούν να γίνουν με ποικίλους τρόπους, όπως είναι η «ένεση» ενός νέου κακόβουλου κόμβου edge computing στο δίκτυο, ο οποίος παίρνει το αναγνωριστικό κάποιου εξουσιοδοτημένου κόμβου. Έτσι ο εισαγόμενος κόμβος καθιστά πιστό αντίγραφο κάποιου αλλού, δίνοντας στους κακόβουλους χρηστές τη δυνατότητα να κλέψουν ή να καταστρέψουν τα δεδομένα αλλά και ακόμα να κατευθύνουν λανθασμένα πληροφορίες.

Παρόμοια θα μπορούσαν να επιτύχουν κάποια επίθεση υλικού εισάγοντας έναν πλαστό κακόβουλο υπολογιστικό κόμβο, όμως αυτήν τη φορά να μην αποτελεί αντίγραφο κάποιου

αλλού, αλλά να λειτουργεί όπως οι εξουσιοδοτημένη κόμβοι έχοντας δηλαδή δυνατότητες αποθήκευσης, επεξεργασίας, ανακατεύθυνσης και μετάδοσης δεδομένων.

Επιπλέον, ένας κακόβουλος χρήστης θα μπορούσε να πάρει τον έλεγχο κάποιου υπάρχοντα κόμβου edge computing και έτσι να επιτύχει την επίθεση ένεση υλικού. Όπου με την πρόσβαση που παίρνει μπορεί να παρεμποδίζει την παράδοση των δεδομένων ή ακόμα και να τα τροποποιεί στέλνοντας ψεύτικα πακέτα δεδομένων.

Τέλος, θα μπορούσε να πάρει κάποιος εισβολέας μη εξουσιοδοτημένη πρόσβαση σε ολοκληρωμένα κυκλώματα μέσω του Hardware Trojan, όπου ουσιαστικά είναι κακόβουλη τροποποίηση του κυκλώματος η όποια γίνεται κατά τη διάρκεια σχεδιασμού ή κατασκευής πχ κάποιου τσιπ (συνήθως χωρίς ο σχεδιαστής - κατασκευαστής να γνωρίζει). Η επίθεση trojan υλικού μπορεί να ενεργοποιηθεί είτε υπό την προϋπόθεση ότι θα εκτελεστεί κάποια συνθήκη, είτε μέσω αισθητήρων ή των κεραιών και ανάλογα με της αλληλεπίδρασης που έχουν με τον εξωτερικό κόσμο. Σε κάθε περίπτωση όμως μπορεί να δώσει σε μη εξουσιοδοτημένο άτομο την πρόσβαση σε δεδομένα και αρά αποτελεί σημαντική απειλεί στο edge computing.

ΑΝΤΙΜΕΤΡΑ:

Υπάρχουν διάφοροι τρόποι για την αντιμετώπιση των κακόβουλων ενέσεων υλικού/ λογισμικού και αντίμετρα για την προστασία, τη διάγνωση και την αντιμετώπιση από τις παραπάνω απειλές μερικά από αυτά αναλύονται παρακάτω.

Για την εύρεση και αντιμετώπιση τόσο Trojan Hardware όσο και άλλον κακόβουλων εγκαταστάσεων υλικό/ λογισμικό σε κόμβους ή και συσκευές edge computing, εφαρμόζεται τακτικές όπως η ανάλυση σημάτων πλευρικού καναλιού. Με κύριο σκοπό να ανιχνεύουν οποιαδήποτε περίεργη δραστηριότητα όπως για παράδειγμα σε ένα εγκατεστημένο κακόβουλο λογισμικό ή υλικό σε κάποιο κόμβο του edge computing ή κάποια υπολογιστική συσκευή, θα μπορούσε να ήταν μια αύξηση στους χρόνους εκτέλεσης ή ακόμα και στη θερμοκρασία. Αυτό επιτυγχάνεται με μελέτη και ανάλυση σε εφαρμογών με βάση τους χρόνους, την ενέργεια που καταναλώνεται και τις διακυμάνσεις της θερμοκρασίας.

Πιο συγκεκριμένα στο Hardware Trojan για να γίνει καλύτερα η ανίχνευση μπορούμε να κάνουμε σύγκριση κυκλωμάτων που έχουν κολλήσει Trojan υλικού και κυκλωμάτων που δεν έχουν, με αποτέλεσμα να μπορούμε τόσο να εντοπίσουμε πιο εύκολα τον κίνδυνο, όσο και να φτιάξουμε μοντέλα για τέτοιες επιθέσεις με κύριο σκοπό την πιο γρήγορη διάγνωση και κατά συνέπεια αντιμετώπιση τους. Αυτό επιτυγχάνεται με μεθόδους που ενεργοποιούν Trojan σε κυκλώματα και έτσι δίνεται η δυνατότητα της σύγκρισης στις διαφορετικές συμπεριφορές των δυο κυκλωμάτων.

Τέλος, μια αποτελεσματική λύση σε κυκλώματα που έχουν προσβληθεί όντως από Trojan ή γενικά που έχουν υποβληθεί σε κακόβουλες ενέσεις λογισμικού/υλικού είναι η τροποποίηση ή αντικατάσταση κυκλώματος. Το μετρό αυτό περιλαμβάνει σε αρχικό στάδιο την αποτροπή της εισβολής όπου κάθε κόμβος edge computing διαθέτει υλικό τόσο για την πρόληψη έναντι στις επιθέσεις, όσο και για την αυτοκαταστροφή τυχών προσβεβλημένου κόμβων και αυτόματη διαγραφή των δεδομένων τους για την καλύτερη ασφάλεια. Ακόμα περιλαμβάνει την εξασφάλιση των όσο γίνεται λιγότερων δεδομένων που ξεφεύγουν από την εξουσιοδοτημένη πρόσβαση με διάφορες τεχνικές όπως με την εκούσια καθυστέρηση δεδομένων, επιλογή σταθερής διαδρομής κλπ. Τέλος, το μετρό αυτό περιέχει στο υλικό του κυκλώματος το Physically Unclonable Function (PUF) για τον έλεγχο της ταυτότητας και αναγνώριση των συσκευών για τη διάγνωση και αποτροπή επιθέσεων.

1.6.β Distributed Denial of Service Attack

Οι κατανεμημένες επιθέσεις άρνησης υπηρεσίας **(Distributed Denial of Service Attacks – DDoS Attack)** έχουν σαν κύριο σκοπό να μην μπορεί ένα πληροφοριακό

σύστημα να ανταποκριθεί λόγο εξάντληση των πόρων του. Στο edge computing μια επίθεση DDoS επιτυγχάνεται με την παρεμπόδιση, είτε αυτή είναι διακοπτόμενη είτε είναι συνεχόμενη, του σήματος κατά τη μετάδοση και λήψη πακέτων στους υπολογιστικούς κόμβους.

Εικόνα 1.15: "Κατανεμημένη επίθεση άρνησης εξυπηρέτησης"
Πηγή: iGuRu

Στο edge computing υπάρχουν τρεις διαφορετικές επιθέσεις κατανεμημένης άρνησης υπηρεσιών που μπορούν να γίνουν και αφορούν κυρίως τους κόμβους. Οι τρεις βασικοί αυτοί τρόποι σύμφωνα με την ερευνά που έγινε από την IEEE είναι:

- Οι <u>επιθέσεις διακοπής λειτουργίας</u> όπου ουσιαστικά οι κόμβοι σταματούν να λειτουργούν εντελώς και αυτό εξαιτίας μη εξουσιοδοτημένης πρόσβασης κάποιου ατόμου.
- Οι <u>επιθέσεις στέρησης ύπνου</u> που στην ουσία εξαντλεί το σύστημα αφού ο κακόβουλος χρήστης αποστέλλει μεγάλο αριθμό αιτημάτων στους κόμβους του edge computing.
- Οι <u>επιθέσεις αποστράγγισης της μπαταρίας</u> όπου στην ουσία εξαντλούν τους κόμβους ή τους αισθητήρες που χρησιμοποιούνται. Αφού στην επίθεση αυτήν εκτελούνται συνεχώς προγράμματα και εφαρμογές που καταναλώνουν ενέργεια με κύριο σκοπό τη μείωση των κόμβων ή των αισθητήρων, επιτυγχάνοντας έτσι διακοπή λειτουργίας.

<u>ΑΝΤΙΜΕΤΡΑ</u>:

Για την αντιμετώπιση των κατανεμημένων επιθέσεων άρνησης υπηρεσιών, οι ερευνητές τις IEEE στην ερευνά που έκανα θέτουν ως πρωταρχικό στοιχείο ασφάλειας τη μελέτη πολίτικων που είναι για ανίχνευση οποιασδήποτε παραβιάσεις. Ουσιαστικά να γίνεται έλεγχος δικτύου για οποιαδήποτε ασυνήθιστη δραστηριότητα μέσου του ελέγχου για τυχόν παραβιάσεις των τυπικών κανόνων δικτύου. Έτσι για την εξάντληση της μπαταρίας ή τη στέρηση ύπνου που προαναφέραμε για την εύρεση επιθέσεων θα μπορούσαν να ελέγχουν για τυχόν περίεργα αιτήματα στους διάφορους υπολογιστικούς κόμβους.

1.6.γ Routing Information Attack

Φυσικά, αφού μιλάμε για μετάδοση και διαχείριση δεδομένων οι επιθέσεις πληροφοριών δρομολόγησης **(Routing Information Attack)** δε θα μπορούσαν να λείπουν. Στις επιθέσεις αυτές οι επιτιθέμενοι «παίζουν» με τη δρομολόγηση των πληροφοριών, αλλάζοντας τη δρομολόγηση των δεδομένων. Η αλλαγή της δρομολόγησης μπορεί τόσο να αλλάξει τις καθυστερήσεις στη μετάδοση των πληροφοριών αφού αλλάζουν οι διαδρομές όπου θα χρησιμοποίησαν κανονικά για τη μετάβαση ενός πακέτου δεδομένων αλλά και πολλές φορές κρίνεται κίνδυνος για τη σωστή διαπεραίωση τις μετάδοσης των δεδομένων μέσα στο δίκτυο. Στην έρευνα που έγινε από την IEEE, αναφέρονται σε τέσσερις επιθέσεις τέτοιου τύπου τις black holes, τις grey holes, τις wormholes και το Hello Flood.

Στην πρώτη επίθεση των μαύρων τρυπών (**Black holes**) εξασφαλίζει ότι τα πακέτα δεδομένων δε θα φτάσουν ποτέ στον τελικό προορισμό του διαγράφοντας τα όλα. Παρόμοια με τις μαύρες και οι γκρι τρύπες (**Grey holes**) διαγράφουν πακέτα δεδομένων με τη διαφορά ότι εδώ επιλέγονται συγκεκριμένα πακέτα δεδομένων για διαγραφή, πράγμα που καθιστά πιο δύσκολο τον εντοπισμό τις επιθέσεις ενώ από την άλλη πλευρά η επίθεση των τρυπών των σκουληκιών (**Wormholes**) ο επιτιθέμενος καταγραφεί όλα τα δεδομένα σε μια διαδικτυακή τοποθεσία και στη συνεχεία τα μεταφέρει σε μια άλλη τοποθεσία. Από την άλλη πλευρά η επίθεση **HELLO Flood** είναι ουσιαστικά η πλημμύρα πακέτων «HELLO» από τον κακόβουλο κόμβο του edge computing προς όλους του γειτονικούς κόμβους.

Τέλος, αξίζει να αναφερθεί, ότι αυτές οι επιθέσεις επιτυγχάνονται με τη χρήση κακόβουλου υπολογιστικού κόμβου, ο όποιος βοηθάει τον εισβολέα τόσο στη διαγραφή πληροφοριών και την αντιγράφει των διάφορων πακέτων πληροφοριών που φτάνουν σε αυτόν τον κόμβο, όσο και την αποστολή των διάφορων πακέτων «HELLO» στους γειτονικούς. Το πιο τύπο θα χρησιμοποιήσει ο επιτιθέμενος όταν έχει τον έλεγχο κάποιου κόμβου εξαρτάται πάντα με τι θέλει να πετύχει.

ΑΝΤΙΜΕΤΡΑ:

Φυσικά η ύπαρξη αξιόπιστων πρωτοκόλλων δρομολόγησης (Reliable Routing Protocols) όπου θα έχουν ένα πίνακα με αξιόπιστους κόμβους για να μεταδίδονται τα διαφορά πακέτα δεδομένων είναι σημαντικό για την προστασία από επιθέσεις δρομολόγησης πληροφοριών. Ο πίνακας αυτός δημιουργείται από τους διάφορους υπολογιστικούς κόμβους, και εξασφαλίζει ότι ευαίσθητα δεδομένα δε θα διαρρεύσουν σε μη εξουσιοδοτημένα πρόσωπα. Περεταίρω μέτρα ασφάλειας για την επίθεση στη δρομολόγησης πληροφοριών είναι η χρήση του συστήματος ανίχνευσης εισβολής (Intrusion Detection System - IDS), το οποίο όχι μόνο ελέγχει το δίκτυο και αν τυπικές πολιτικές τηρούνται, αλλά αναφέρει τις ύποπτες δραστηριότητες που ανιχνεύει.

1.6.δ Physical Tempering and Attack

Το edge computing φέροντας τα δεδομένα πιο κοντά στην πηγή που παράχθηκαν δημιουργεί αυτόματα μεγαλύτερο ευρέως για να κάλυψη από φυσικές επιθέσεις.

Οι φυσικές παρεμβάσεις ή επιθέσεις (**Physical Tampering and Attacks**) συμβαίνει όταν κάποιος κακόβουλο άτομο μπορεί να πάρει φυσική πρόσβαση σε υπολογιστικούς κόμβους ή σε συσκευές edge computing. Το αποτέλεσμα τις επιθέσεις αυτής είναι η έκθεση ευαίσθητων δεδομένων σε άτομα που δε θα έπρεπε και που δεν έχουν εξουσιοδοτημένη πρόσβαση. Η σημαντικότητα τον φυσικών επιθέσεων φαίνεται αν σκεφτούμε ότι ο επιτιθέμενος πέρα από την εξαγωγή πληροφοριών μπορεί ακόμα να τροποποιήσει μέχρι και το λειτουργικό σύστημα.

Τέλος, το γεγονός ότι υπάρχουν μεγάλος αριθμός συσκευών edge computing σε διαφορετικές τοποθεσίες δε βοηθάει την προστασία του σε σχέση με τις φυσικές επιθέσεις.

ΑΝΤΙΜΕΤΡΑ:

Οι φυσικές επιθέσεις μπορούμε να τις αντιμετωπίσουμε με μεθόδους που ήδη αναφέραμε στην κακόβουλη ένεση υλικού/λογισμικού. Μεθόδους όπως της τροποποίησης ή και αυτοκαταστροφής κυκλώματος όπου περιλαμβάνει τόσο τεχνικές για αποφυγή της επίθεσης ενσωματωμένα στο υλικό των κόμβων, όσο και αυτοκαταστροφή κόμβων για τη χειρότερη περίπτωση. Εκτός από αυτές τις μεθόδους όμως η αυξήσει της ασφάλειας στις φυσικές επιθέσεις μπορεί να περιλαμβάνει και αλλά μετρά όπως προσθήκη επιπλέον τεχνικών ακεραιότητας κατά την κατασκευή ή την εφαρμογή μηχανισμών ασφάλειας.

ΚΕΦΑΛΑΙΟ 2 INTERNET OF THINGS

2.1 Εισαγωγή

Στις μέρες μας ολοένα και περισσότερο γίνεται λόγος για το διαδίκτυο των πραγμάτων (Internet of Things – IoT) και τις δυνατότητες που μπορεί να προσφέρει σε διάφορους τομείς και όχι άδικα, καθώς αποτελεί μια από τις κορυφαίες τεχνολογίες της δεκαετίας μας. Καταφέρνοντας να συνδέει ένα σύνολο συσκευών (τόσο μηχανικών όσο και ψηφιακών) μεταξύ τους σε ένα δίκτυο επικοινωνιών, με σκοπό την ανταλλαγή δεδομένων με άλλες συσκευές και συστήματα. Οι συσκευές αυτές περιέχουν ενσωματωμένα ηλεκτρονικά μέσα, λογισμικά, αισθητήρες και σύνδεση στο δίκτυο (τοπικό δίκτυο ή παγκόσμιο δίκτυο) δίνοντας τους έτσι δυνατότητα συλλογή και ανταλλαγή δεδομένων χωρίς απαραίτητα την αλληλεπίδραση του ανθρώπου με άνθρωπο ή με κάποια συσκευή.

Εικόνα 2.1: "Διαδίκτυο των πραγμάτων"
Πηγή : ΕΛΛΑΚ

Ουσιαστικά ένα σύστημα Internet of things αποτελείτε από διάφορες συσκευές με δυνατότητα σύνδεσης στο διαδίκτυο, οι οποίες έχουν αισθητήρες, λογισμικά και υλικό για να επικοινωνούν μεταξύ τους. Με αυτόν τον τρόπο μπορούν να κάνουν συλλογή, ανταλλαγή και ακόμα δράση πάνω σε διαφορά δεδομένα. Χαρακτηριστικό παράδειγμα αποτελούν τα ημιαυτόνομα αυτοκίνητα όπου διαθέτουν κάμερες, αισθητήρες και σύστημα Internet of Things για να μπορούν να λαμβάνουν αποφάσεις αυτόνομα οποιαδήποτε στιγμή, αποφεύγοντας κάποια ανθρωπινά λάθη κατά τη διάρκεια της οδήγησης. Εκτός από τα ημιαυτόματα αυτοκίνητα, οι κατασκευαστές δημιούργησαν πλήρως αυτόνομα οχήματα, όπου αναλαμβάνουν όλες τις λειτουργίες οδήγησης και μπορούν να σε πάνε στον προορισμό σου. Ωστόσο, τα οχήματα τέτοιου τύπου είναι ακόμα σε πειραματικό στάδιο και αυτός είναι ο κύριος λόγος που διαθέτουν τα εξαρτήματα ενός μη αυτονόμου οχήματος (όπως τιμόνι, φρένα κλπ.) για να μπορέσει οποιαδήποτε στιγμή να υπάρξει ανθρώπινη παρέμβαση.

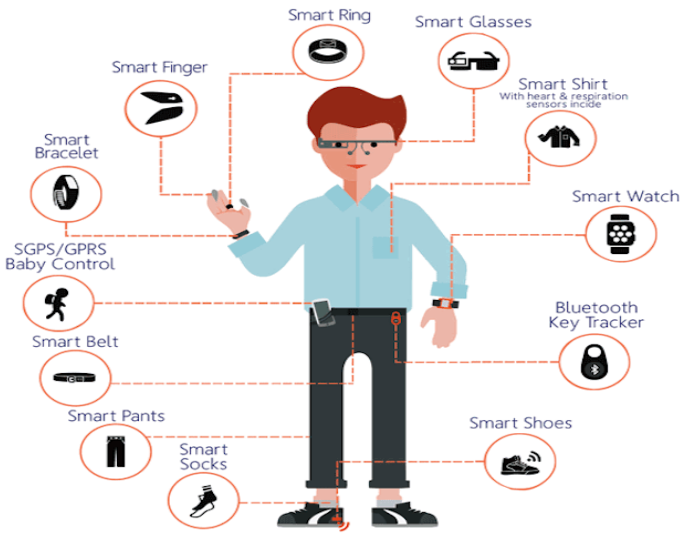
Πέρα όμως από τις αυτοκινητοβιομηχανίες και τα οχήματα που διαθέτουν συστήματα IoT, το διαδίκτυο των πραγμάτων χρησιμοποιείται και σε διάφορες άλλες πτυχές της καθημερινότητα μας, όπως για παράδειγμα είναι τα έξυπνα ρολόγια, έξυπνα συστήματα ασφάλειας, έξυπνα ψυγεία κλπ. Στόχος είναι διευκόλυνση των ανθρώπων καθώς αυτοματοποιεί τις εργασίες και μειώνει την ανθρώπινες παρεμβάσεις, δίνοντας πάντα την ικανότητα προσβάσεις σε δεδομένα από οπουδήποτε σε οποιαδήποτε χρονική στιγμή!

Επιπλέον η εξέλιξη του Internet of things όπως είναι σήμερα έχει βελτιώσει κατά πολύ την επικοινωνία μεταξύ των συνδεδεμένων συσκευών. Ανεξαρτήτως όμως από ποιες συσκευές και συστήματά IoT χρησιμοποιούμε, το διαδίκτυο των πραγμάτων έχει κάποια βασικά χαρακτηριστικά, αναλύονται μερικά παρακάτω:

- ✓ **Συνδεσιμότητα (Connectivity)**: Βασικό χαρακτηριστικό αποτελεί η συνδεσιμότητα, χωρίς αυτήν δε θα μπορούσαν να υπάρξει το διαδίκτυο των πραγμάτων. Αφού η συνδεσιμότητα δίνει τη δυνατότητα πρόσβασης στο δίκτυο και τη συμβατότητα που χρειάζεται για την κατανάλωση και παραγωγή δεδομένων.
- ✓ **Ετερογένεια (Heterogeneity)**: Η ετερογένεια που υπάρχει στο IoT φαίνεται από της διαφορετικές διασυνδεδεμένες συσκευές που το αποτελούν.
- ✓ **Επεκτασιμότητα (Scalability)**: Τα συστήματα IoT παράγουν μεγάλο όγκο δεδομένων και για την καλύτερη αντιμετώπιση των δεδομένων αυτών μπορεί μεταγενέστερα να χρειαστεί μαζική επέκταση.
- ✓ **Ασφάλεια (Safety)**: Σε μια τεχνολογία που έχει να κάνει με τα δεδομένα, όπως είναι το διαδίκτυο των πραγμάτων, η ασφάλεια αποτελεί σημαντικό χαρακτηριστικό που πρέπει να έχει.
- ✓ **Νοημοσύνη (Intelligence)**: Η πληροφορίες όπου συλλέγονται από τα συνδεδεμένα πράγματα στις περισσότερες περιπτώσεις έχουν σκοπό να βοηθήσουν στη λήψη αποφάσεων. Έτσι η ανάγκη για την εξαγωγή γνώσεων μέσα από αυτά τα δεδομένα και η σωστή ερμηνεία είναι πολύ σημαντική, για αυτόν τον λόγο αναπτύσσουμε μοντέλα μηχανικής μάθησης πάνω στα δεδομένα αυτά.
- ✓ **Δυναμική και αυτοπροσαρμόσιμη (Dynamic and self-adapting)**: Οι συσκευές IoT θα πρέπει να προσαρμόζονται αυτόματα και δυναμικά στις μεταβολές του περιβάλλοντος. Αυτό μπορούμε να το κατανοήσουμε αν πάρουμε σαν παράδειγμα μια κάμερα παρακολούθησης το να μπορεί να προσαρμόζεται αυτόματα ανάλογα π.χ. με τον φωτισμό (Πρωί - Βραδύ) είναι απαραίτητο.

2.2 Καθημερινότητα και Διαδίκτυο των Πραγμάτων

Το Διαδίκτυο των πραγμάτων, όπως αναφερθήκαμε παραπάνω, έχει καταφέρει να επηρεάσει πολλές πτυχές της ζωής μας. Μπαίνοντας μερικές φορές ασυνείδητα στην καθημερινότητα μας και αυτό μπορούμε να το συνειδητοποιήσουμε από τις διαφορές **φορητές συσκευές** που χρησιμοποιούμε και διαθέτουν Internet of Things.

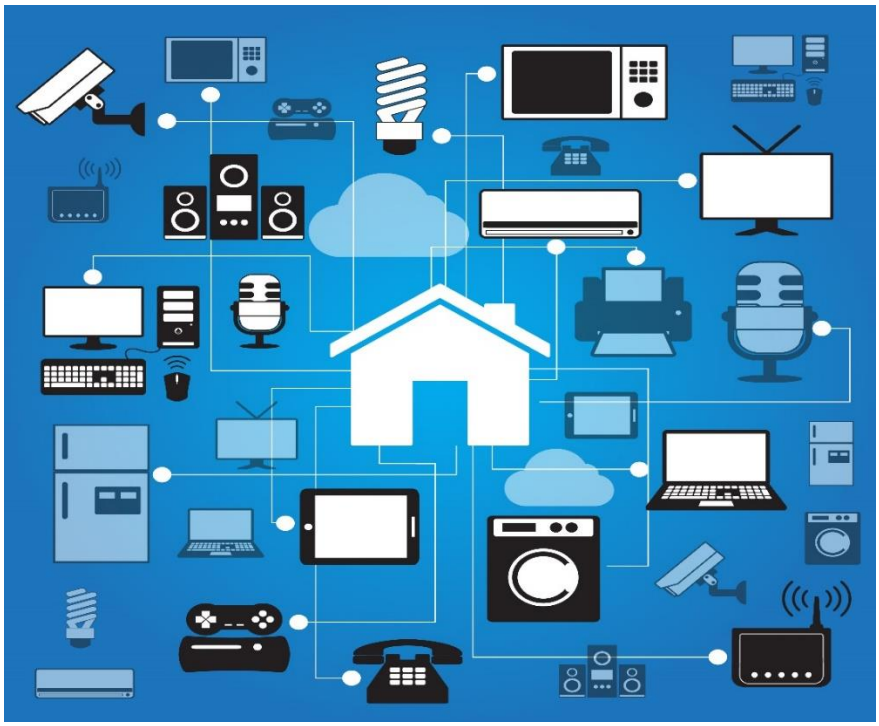


Εικόνα 2.2: "Διαδίκτυο των πραγμάτων και φορητές συσκευές"
Πηγή: Embedded COMPUTING DESIGN

Το πιο γνωστό τέτοιο παράδειγμα είναι τα **έξυπνα ρολόγια (smart watch)** τα περισσότερα από αυτά μπορούν να συνδεθούν με το κινητό τηλέφωνο και να του στέλνουν τα διάφορα δεδομένα που συλλέγουν. Κάποιες πληροφορίες χρήστη που μπορούν να μετρήσουν και κατά συνεπεία να συλλέξουν είναι τα βήματα, οι απόστασής, οι παλμοί της καρδιάς, ο τρόπο ύπνου (ελαφρύ ή βαρύ) κλπ. Κάποια smart watch έχουν και επιπλέον δυνατότητες όπως να σηκώνουν κλήση του κινητού τηλεφώνου ή να δέχονται υποστήριξη φωνής που του επιτρέπει την αλληλεπίδραση με την Siri, την Alexa και τη βοηθό της Google.

Πέρα όμως από τα έξυπνα ρολόγια υπάρχουν και αλλά παραδείγματα φορητών συσκευών με σύστημα Internet of things όπως είναι τα **έξυπνα ρούχα (smart clothes)** για αθλητές. Τα οποία χάρης τις μετρήσεις που μπορούν να κάνουν (καύσης θερμίδων, καρδιακοί ρυθμοί κλπ.) βοηθούν τους αθλητές να έχουν καλύτερη απόδοση. Όπως και στα έξυπνα ρολόγια έτσι και τα έξυπνα ρούχα μπορούν να συνδεθούν με το τηλέφωνο και να καταγράψουν τις διάφορες πληροφορίες εκεί. Τα παραπάνω παραδείγματα αποτελούν μερικές από τις πολλές φορητές συσκευές που ο άνθρωπος μπορεί να χρησιμοποιεί και να διαθέτουν συστήματα Internet of things. Κάποια αλλά παραδείγματα ενδεικτικά είναι έξυπνα παπούτσια, έξυπνες κάλτσες, έξυπνα γυαλιά, έξυπνη ζώνη κλπ.

Ωστόσο δε θα αναφερθούμε εκτενέστερα σε αυτές τις φορητές συσκευές, καθώς πέρα από τις συσκευές που μπορούμε να έχουμε πάνω μας υπάρχουν και διάφορες **οικιακές συσκευές** που χάρης την εξέλιξη της τεχνολογίας και του IoT κάνουν τα σπίτια μας πιο "έξυπνα" και τη ζωή των ανθρώπων πιο εύκολη.



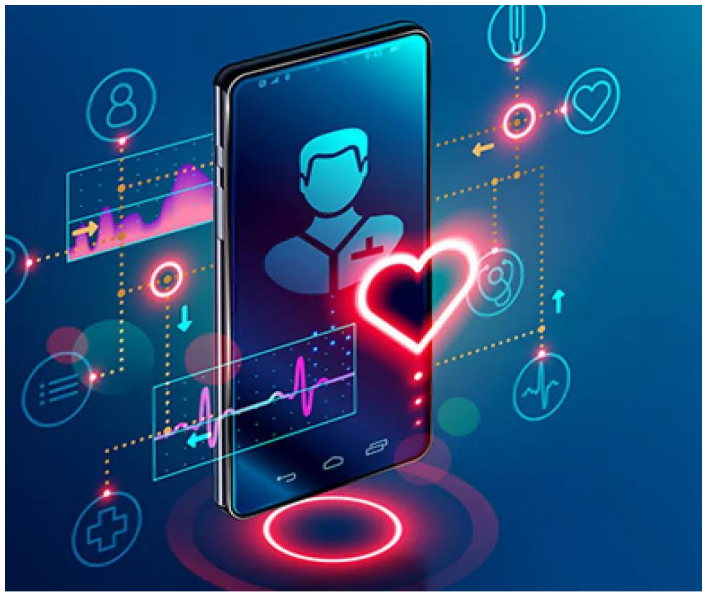
Εικόνα 2.3: "Διαδίκτυο των πραγμάτων και έξυπνο σπίτι"
Πηγή: speciale IoT

Τέτοιες έξυπνες οικιακές συσκευές μπορεί να είναι σκούπες, στεγνωτήρια, πλυντήρια, και οτιδήποτε άλλο μπορούμε να φανταστούμε. Ενδεικτικά αναφέρουμε τα έξυπνα ψυγεία

όπου μπορούν να σε ενημερώσουν ανά πάσα στιγμή για τα προϊόντα που καταναλώνονται ή για τα άδεια μπουκάλια που υπάρχουν στο ψυγείο εκείνη τη στιγμή. Επιπλέον, χαρακτηριστικό παράδειγμα που κάνει τα **σπίτια μας έξυπνα (Smart House)** είναι οι κομβόι έξυπνοι σπιτιού (smart house hub) οι οποίοι μπορούν να χειριστούν καθημερινές ανάγκες όπως είναι φωτισμός, θέρμανση, ψύξη κλπ. είτε με φωνητική εντολή ή από κάποια συσκευή όπως είναι το κινητό τηλέφωνο.

Εικόνα 2.4: "Έξυπνά αυτοκίνητα και διαδίκτυο των πραγμάτων"
Πηγή: dreamstime

Ωστόσο, το διαδίκτυο των πραγμάτων έχει επεκταθεί πέρα από αυτά και σε άλλα κομμάτια όπως είναι οι αυτοκινητοβιομηχανίες, που αναφέραμε παραπάνω, δημιουργώντας έτσι τα **έξυπνα αυτοκίνητα (Smart cars)** (Κεφάλαιο 2,0 εισαγωγή) αλλά και στα κομμάτια της υγείας δημιουργώντας έτσι τη **διασυνδεδεμένη υγειά (Connected health)**. Όπου στην ουσία οι διάφορες διασυνδεδεμένες συσκευές του Internet of Things βοηθάνε στη διάγνωση και τη διαχείριση ασθενειών. Ήδη χρησιμοποιούνται τόσο στο σπίτι όσο και στα νοσοκομεία συσκευές Internet of Medical Things (IoMT) για πιο ασφαλής και αποτελεσματική κοινωνική και υγειονομική περίθαλψη.



Εικόνα 2.5: "Υγεία και διαδίκτυό των πραγμάτων"
Πηγή: IoT Business News

Τέλος, αυτά είναι μερικά παραδείγματα καθώς το Διαδίκτυο των πραγμάτων αποτελεί κάτι μεγαλύτερο, που όχι μόνο μπορεί αλλά επηρεάζει και βελτιώνει πολλούς περισσοτέρους κλάδους και πτυχές τις ζωής μας. Ήδη γίνεται λόγος για έξυπνες πόλεις και όχι μόνο, ωστόσο οι έξυπνες πόλεις θα μπορούσαν να αποτελέσουν ξεχωριστή εργασία διότι είναι ένα εξαιρετικά μεγάλο και πολυδιάστατο θέμα. Έτσι προτιμήθηκε η ανάλυση μικρότερων γενικών παραδειγμάτων.

2.3 Ιστορική εξέλιξη

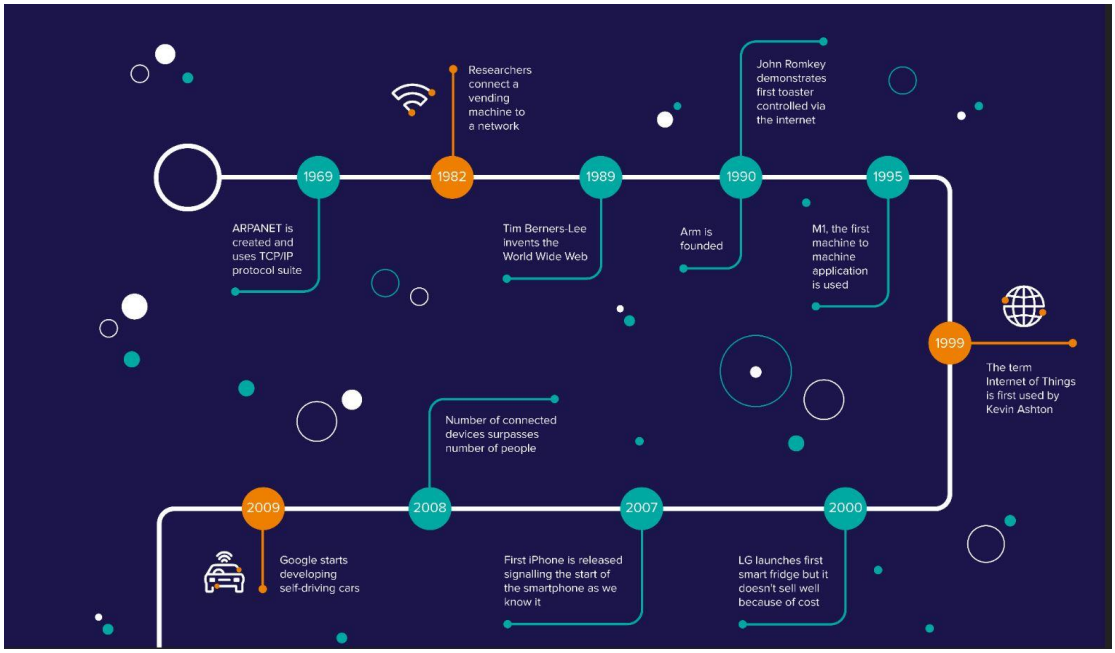
Παρόλα τα όσα αναφερθήκαν παραπάνω το διαδίκτυο των πραγμάτων δεν ήταν πάντα όπως σήμερα, αφού υπήρξε σταδιακή εξέλιξή των τεχνολογιών που οδήγησε στη δημιουργία του. Ωστόσο, αν θέλαμε να ξεκινήσουμε από κάπου σίγουρα αυτό το σημείο θα ήταν η δημιουργία του πρώτου δικτύου το **1969**, αφού το διαδίκτυο αποτελεί βασικό στοιχείο του Internet of Things. Το δίκτυο αυτό ήταν το Advanced Research Project Agency Network (ARPANET) το όποιο δημιουργήθηκε στις ΗΠΑ ήταν το πρώτο δίκτυο μεταγωγή πακέτου που δημιουργήθηκε και είχε ο σκοπός τη διασφάλιση της επικοινωνίας απομακρυσμένων δικτύων ανεξάρτητα αν τα ενδιάμεσα συστήματα βρισκόντουσαν εκτός λειτουργίας εκείνη τη στιγμή. Το ARPANET χρησιμοποιήθηκε κυρίως από την ακαδημαϊκή και ερευνητική κοινότητα ωστόσο αποτελεί τη βάση για τη δημιουργία του διαδικτύου και αυτός είναι ο λόγος που το γράψαμε ως αρχικό σημείο στην ιστορική εξέλιξη του IoT.

Λίγα χρόνια αργότερα το **1973** δημιουργήθηκε το RFID (Radio-Frequency Identification), στο όποιο ουσιαστικά τα ψηφιακά δεδομένα που κωδικοποιούνται σε ετικέτες RFID συλλαμβάνονται μέσω ραδιοκυμάτων από κάποιον αναγνώστη, δίνοντας έτσι τη δυνατότητα ανάγνωσης και εγγραφής δεδομένων σε συσκευές. Αν και το RFID δε δημιουργήθηκε ξαφνικά το 1973, αλλά είχε τις ρίζες του από το Β' Παγκόσμιο πόλεμο και η πρόοδο συνεχίστηκε μετέπειτα ωστόσο το 1973 ο Mario W. Cardullo δημιούργησε ετικέτα RFID με επανεγγράψιμη μνήμη. Σήμερα το RFID αποτελεί βασική τεχνολογία για το διαδίκτυο των πραγμάτων.

Αργότερα το **1984** χρησιμοποιείται το IoT αφού γίνεται χρήση μιας coke machine όπου συνδέθηκε στο διαδίκτυο με σκοπό να αναφέρει τόσο τη διαθεσιμότητα που είχε σε ποτά όσο και τη θερμοκρασία που αυτά είχαν. Ωστόσο, σημαντικό κρίνεται εδώ ότι ο ορός 'Διαδίκτυο των Πραγμάτων' δεν είχε ειπωθεί ακόμα σαν έννοια αλλά μόνο σαν πρακτικό κομμάτι.

Κάπου στα **μέσα της δεκαετίας του 1990** ανάπτυξη γνωρίσαν οι κόμβοι αισθητήρων αφού πλέον ανίχνευαν δεδομένα από μοναδικά αναγνωρισμένες ενσωματωμένες συσκευές και είχαν τη δυνατότητα να ανταλλάσσουν πληροφορίες με στόχο την υλοποίηση της βασικής ιδέας του IoT.

Σημαντική χρονιά αποτέλεσε το **1999** καθώς η επικοινωνία συσκευής με συσκευής εισάγεται από τον Bill Joy. Επιπλέον, την ίδια χρονιά χρησιμοποιείται για πρώτη φορά ο ορός «Διαδίκτυο των πραγμάτων» από τον Kevin Ashton. Αν και το διαδίκτυο των πραγμάτων υπήρχε πολύ πιο πριν απλά δεν είχε ονομασία, για αυτόν τον λόγο ο Ashton αποφάσισε να ονομάσει έτσι τα πράγματα που συλλέγουν, επεξεργάζονται και μεταδίδουν δεδομένα χωρίς την ανθρώπινη παρέμβαση. Σε αυτήν τη διαδικασία η χρήση RFID (Αναγνώριση ραδιοσυχνοτήτων) επιτάχυνε τη διαδικασία μεταφορά δεδομένων απευθείας μεταξύ συσκευών, αλλά η εξέλιξή αυτής της τεχνολογία δε μένει εκεί αφού το 1999 η RFID ενισχύθηκε για την παραγωγή τσιπ από την ίδρυση του κέντρου Auto-ID στο Τεχνολογικό Ινστιτούτο της Μασαχουσέτης. Με σκοπό το τσιπ αυτό να μπορεί να αποθηκεύει πληροφορίες και να χρησιμοποιείται για τη σύνδεση των πραγμάτων στον διαδίκτυο.



Εικόνα 2.6: "Ιστορική εξέλιξη του διαδικτύου των πραγμάτων"
Πηγή: Pelion

Το **2000** βγήκε το πρώτο ψυγείο με σύνδεση στο διαδίκτυο δίνοντας τις δυνατότητες να ψωνίζουν ηλεκτρονικά και να κάνουν βιντεοκλήσεις. Αργότερα το **2005** βγήκε πέρα από το ψυγείο αυτό, και ρομπότ σε σχήμα κουνέλι, δίνοντας τη δυνατότητα να σε ενημερώνει για τα τελευταία νέα, για τον καιρό και αλλαγές στα χρηματιστήρια. Στη **δεκαετία του 2000** το ενδιαφέρον για τις τεχνολογίες του Internet of Things αυξανόταν σταδιακά, έτσι το **2008** αποφάσισαν να κάνουν συμβούλιο σχετικά με το RFID, τις ασύρματες επικοινωνίες και τα δίκτυα αισθητήρων. Το συμβούλιο αυτό πραγματοποιήθηκε στην Ελβετία και συμμετέχοντες από αρκετές χώρες προσήλθαν σε αυτό.

Τέλος, από το **2010 και μετά** οι διασυνδεδεμένες συσκευές έχουν γίνει ευρέως γνωστές και έχουν ενταχθεί στην καθημερινότητα μας. Βάζοντας τόσο το Internet of Things στις ζωές μας όσο και στους κλάδους όπως: μεταφορές, υγειονομική περίθαλψη, λιανικό εμπόριο, γεωργία κλπ. Δεν είναι τυχαίο άλλωστε που πολλές μεγάλες εταιρίες επικεντρώνονται στην παραγωγή τόσο αισθητήρων όσο και συσκευών IoT

2.4 Μοντέλα επικοινωνίας

Όπως είδαμε παραπάνω υπάρχουν αρκετά παραδείγματα για το Internet of Things και το πως αυτά βοηθάνε τον άνθρωπό το καθένα με τον δικό του τρόπο. Ωστόσο, όλα αυτά τα διαφορετικά παραδείγματα αποτελούνται από **«πράγματα»** όπου συλλέγουν διαφορές πληροφορίες με τη βοήθεια των τεχνολογιών RFID, των αισθητήρων και του κώδικα. Τα πράγματα αυτά συνδέονται με το **δίκτυο επικοινωνίας**. Τέλος, για κάθε παράδειγμα IoT χρειάζεται να υπάρχουν **ενσωματωμένα συστήματα και εφαρμογές** για να μπορούν να επεξεργάζονται τα ακατέργαστα δεδομένα που συλλέγονται και ρέουν από και προς τα πράγματα.

Η σύνδεση των παραπάνω μερών, που αποτελούν τα τρία βασικά στοιχεία του Internet of Things, επιτυγχάνεται με τη χρήση μοντέλων επικοινωνίας και για την καλύτερή κατανόηση πως γίνεται η σύνδεση και οι επικοινωνία των συσκευών IoT παρακάτω αναλύουμε τέσσερα μοντέλα επικοινωνίας:

❖ **Μοντέλο επικοινωνίας από συσκευή με συσκευή (Device-to-Device Communication Model) :**

Το μοντέλο αυτό περιλαμβάνει τη σύνδεση δυο ή και περισσοτέρων συσκευών μεταξύ τους, που δε χρειάζονται τη χρήση κάποιου Server για να επικοινωνούν. Αλλά συνδέονται απευθείας και επικοινωνούν μέσω πολλών τύπων δικτύου, μέσα σε αυτούς τους τύπους είναι τα δίκτυά IP και το διαδίκτυο. Οι συσκευές αυτές μπορούν να χρησιμοποιούν πρωτόκολλα για να επιτύχουν την απευθείας επικοινωνία συσκευής με συσκευή, πρωτόκολλα όπως είναι το Bluetooth, Z-wave ή ZigBee.

Όπου το Bluetooth είναι ασύρματη τηλεπικοινωνιακή τεχνολογία για μικρές απόστασης όπου μεταδίδει μικροκύματα σε ψηφιακές συσκευές. Αποτελεί πρότυπο για ασύρματα προσωπικά δίκτυα υπολογιστών (Wireless Personal Area Networks, WPAN). Το Z-wave είναι πρωτόκολλο για ασύρματη επικοινωνία που χρησιμοποιείται για εφαρμογές οικιακού αυτοματισμού. Τέλος, το ZigBee είναι πρωτόκολλο ασύρματης επικοινωνίας συσκευών. Τόσο το Z-Wave όσο και το ZigBee χρησιμοποιούν ραδιοκύματα χαμηλής ενέργειας για την επικοινωνία.

Εικόνα 2.7: "Μοντέλο επικοινωνίας συσκευή με συσκευή"
Πηγή: TechTarget

❖ **Μοντέλο επικοινωνίας συσκευής με νέφος (Device-to-Cloud Communication Model) :**

Σε αυτήν την περίπτωση οι συσκευές Internet of Things επικοινωνούν με τις υπηρεσίες του Cloud μεσώ του διαδικτύου, με σκοπό την ανταλλαγή δεδομένων αλλά και των έλεγχο της κυκλοφορίας μηνυμάτων. Η απευθείας αυτή επικοινωνία επιτυγχάνεται μεσώ ενσύρματων συνδέσεων Ethernet ή Wi-Fi, αφού δημιουργεί έτσι σύνδεση των συσκευών και του δίκτυο IP και το οποίο κατά συνεπεία συνδέεται με την

υπηρεσία cloud. Στην επικοινωνία αυτή φυσικά βοηθάει και η χρήση διάφορων πρωτοκόλλων όπως είναι HTTP, TCP/IP, TLS κλπ.

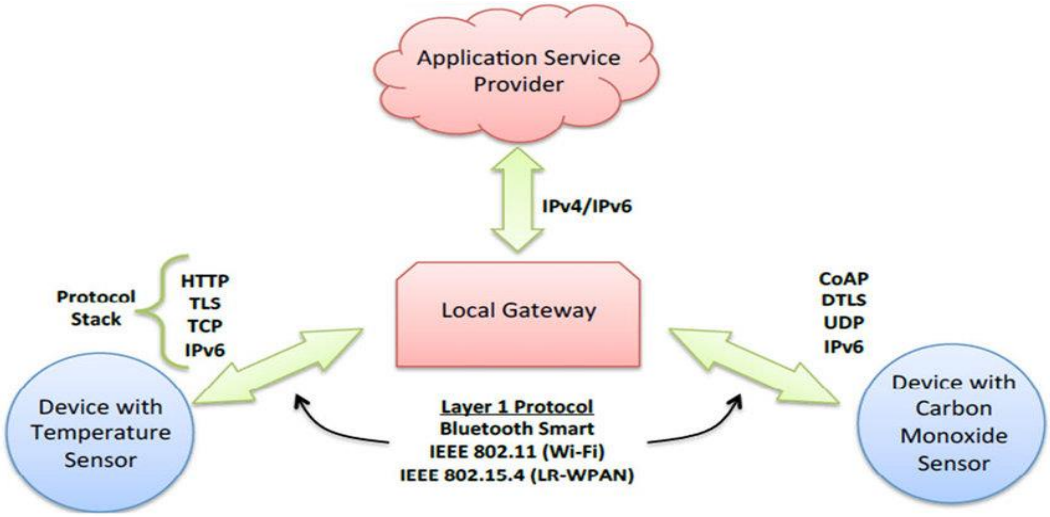
Εικόνα 2.8: "Μοντέλο επικοινωνίας συσκευής με σύννεφό"
Πηγή: Research Gate

- **Μοντέλο επικοινωνίας συσκευής προς πύλης (Device-to-Gateway Communication Model) :**

Η συσκευή gateway διαθέτει λογισμικό εφαρμογών και λειτουργεί σαν ενδιάμεσος στις συσκευές IoT και των υπηρεσιών του cloud, προσφέροντας ασφάλεια και άλλες υπηρεσίες στην επικοινωνία όπως η μεταφορά δεδομένων και η υποστηρίξει πρωτοκόλλων. Έτσι στο μοντέλο αυτό η συσκευή IoT συνδέεται μεσώ μιας υπηρεσίας ALG (Application Layer Gateway) σε μια υπηρεσία του cloud.

Χαρακτηριστικό παράδειγμα που κάνει χρήση αυτού του μοντέλου είναι η εφαρμογή γυμναστικής σε smart phone, η όποια είναι συνδεδεμένη με κάποια συσκευή παρακολούθησης φυσικής κατάστασης. Η συσκευή αυτή εξαρτάται άμεσα από την εφαρμογή του smart phone, αφού χωρίς το smart phone και την εφαρμογή αυτή η συσκευή παρακολούθησης δεν μπορεί από μονή της να συνδεθεί απευθείας με την υπηρεσία cloud.

Το βασικό πλεονέκτημα της εφαρμογής ενός τέτοιου μοντέλου είναι ότι με την ένταξή νέων έξυπνων συσκευές σε ένα παλιού τύπου σύστημα καταφέρνουμε να διευκολύνουμε περισσότερο τη διαλειτουργικότητα μεταξύ συσκευών. Ωστόσο, η προσθήκη λογισμικού εφαρμογής συνεπάγεται τις αύξησης του κόστους και της πολυπλοκότητας στη σχεδίαση του συστήματος.



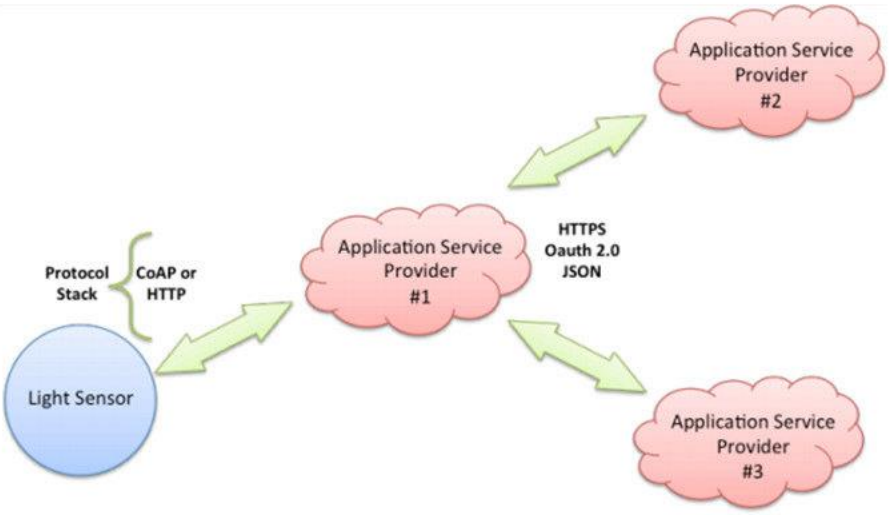
Εικόνα 2.9: "Μοντέλο επικοινωνίας συσκευής προς πύλης"

Πηγή: Research Gate

- **Μοντέλο επικοινωνίας με κοινή χρήση δεδομένων (Back-End-Data-Sharing Communication Model) :**

  Πολλές φορές οι χρήστες επιθυμούν να μοιραστούν δεδομένα αισθητήρων που έχουν αποθηκεύει στο cloud με άλλα άτομα, για να το πραγματοποιήσουν αυτό η χρήση του Back-End-Sharing Communication Model είναι απαραίτητη. Αφού το συγκεκριμένο μοντέλο εξουσιοδοτεί τους χρήστες να μπορούν να βγάλουν τα δεδομένα των συσκευών IoT από τη βάση του cloud που είναι αποθηκευμένα, δίνοντας έτσι και τη δυνατότητα ανάλυσης των δεδομένων.

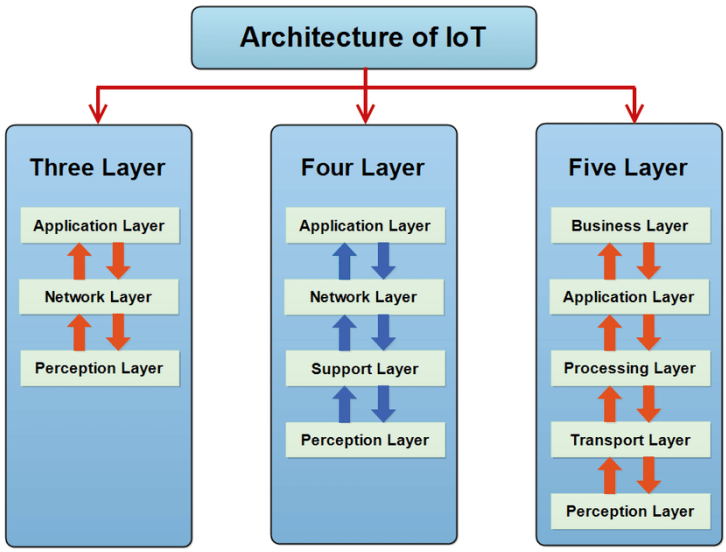
  Το μοντέλο Back-End προσπαθεί να ξεπεράσει περιορισμούς του μοντέλου επικοινωνίας συσκευής με cloud, καθώς επιτρέπει την ανάλυση ροών δεδομένων που συλλέγονται από συσκευές IoT όπου συγκριτικά με το μοντέλο Device-to-cloud communication δεν επιτρέπεται αυτό.



Εικόνα 2.10: "Μοντέλο επικοινωνίας με κοινή χρήση δεδομένων"
Πηγή: Research Gate

2.5 Αρχιτεκτονικές IoT

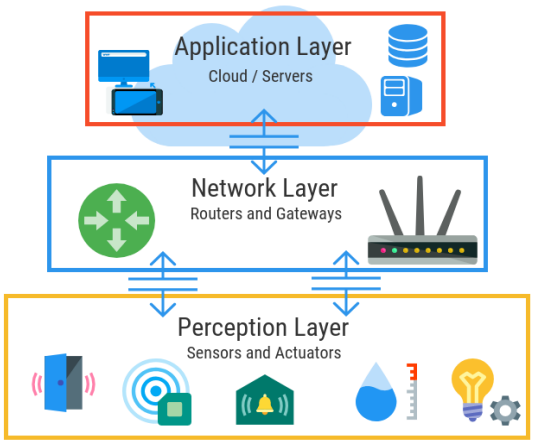
Στο διαδίκτυο των πραγμάτων δεν υπάρχει μια αρχιτεκτονική και ο λόγο είναι ότι υπάρχουν διάφορες εφαρμογές του. Οι διαφορές αυτές αρχιτεκτονικές του IoT επιλέγονται ανάλογα με τη λειτουργικότητα και την εφαρμογή τους στους διάφορους τομείς. Παρακάτω αναλύουμε τα διάφορα επίπεδα των αρχιτεκτονικών τριών, τεσσάρων και πέντε επίπεδων με σκοπό τόσο να καταλάβουμε το διαδίκτυο των πραγμάτων περισσότερο, όσο και να τα χρησιμοποιήσουμε αργότερα. Οι διαφορές αυτές αρχιτεκτονικές είναι ιεραρχικές, όπως φαίνονται στην εικόνα παρακάτω, και αποτελούνται όλες από τρία βασικά επίπεδα, της αντίληψης, του δικτύου και των εφαρμογών. Τα επίπεδα αυτά αποτέλεσαν τη βάση για την ιδέα του Internet of Things και την πρώτη αρχιτεκτονική, ωστόσο μεταγενέστερα αναπτύχθηκαν και άλλες προσπαθώντας να βελτιώσουν την αρχική. Έτσι δημιουργήθηκαν επιπλέον τεσσάρων επίπεδων όπου προσθέτει το επίπεδο υποστήριξης και πέντε επίπεδων όπου βγάζει την υποστήριξη και προσθέτει την επεξεργασία και το επιχειρησιακό.



Εικόνα 2.11: "Αρχιτεκτονικές του IoT"
Πηγή: ResearchGate

❖ Αρχιτεκτονική τριών επιπέδων

Η αρχιτεκτονική των τριών επιπέδων είναι μια βασική αρχιτεκτονική που προτάθηκε στα πρώτα στάδια της εξέλιξης του Internet of Things και υπήρξε η βασική ιδέα του. Αποτελείται από τρία επίπεδα τα οποία είναι της αντίληψης, του δικτύου και της εφαρμογή. Το **επίπεδο αντίληψης (Perception Layer)** έχει την ευθύνη να αναγνωρίζει πράγματα αφού είναι το στρώμα αισθητήρων. Οι αισθητήρες αυτοί επιλέγονται κάθε φορά με τις απαιτήσεις που έχει η κάθε εφαρμογή του IoT για να συλλέγουν τα δεδομένα. Αφού υπάρχουν διάφοροι τύποι αισθητήρων που συνδέονται με τις συσκευές IoT. Επόμενο είναι **το επίπεδο του δικτύου (Network Layer)**, όπως φαίνεται και στην εικόνα, το όποιο μεταφέρει και μεταδίδει (είτε με ενσύρματο είτε με ασύρματο τρόπο) τις πληροφορίες που συλλέγονται. Εκτός από αυτό όμως είναι υπεύθυνο για τη σύνδεση τόσο των έξυπνων πραγμάτων και των συσκευών δικτύου, όσο και δικτύων μεταξύ τους. Τέλος, είναι το **επίπεδο εφαρμογής (Application Layer)** και το όποιο είναι υπεύθυνο για να παρέχει τις υπηρεσίες στις εφαρμογές. Οι υπηρεσίες αυτές διαφέρουν ανάλογα την εφαρμογή αφού έχουν να κάνουν με τους αισθητήρες που χρησιμοποιούνται κάθε φορά και τις πληροφορίες που αυτοί συλλέγουν.

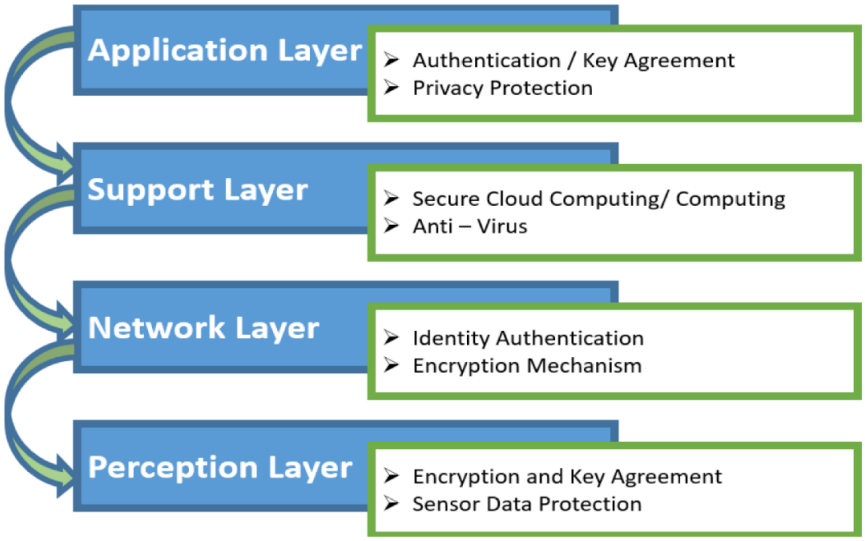


Εικόνα 2.12: "Αρχιτεκτονική τριών επιπέδων"
Πηγή: ResearchGate

❖ Αρχιτεκτονική τεσσάρων επιπέδων

Η αρχιτεκτονική αυτή προσθέτει ένα ακόμα το **επίπεδο υποστήριξης (Support Layer)** ανάμεσα στο επίπεδο του δικτύου και των εφαρμογών. Ο λόγος πίσω από αυτό έγινε για να αποστέλλονται οι πληροφορίες που συλλέγονται εκεί, για να μπορεί ελέγχει αν τα δεδομένα που στέλνονται είναι από αυθεντικούς χρήστες και ότι προστατεύονται από τις απειλές. Καθώς χρησιμοποιεί πολλές μεθόδους επαλήθευσης των χρηστών και των δεδομένων όπως είναι ο έλεγχος ταυτότητας.

Αφού η αποστολή πληροφοριών απευθείας στο επίπεδο του δικτύου αύξανε τους κίνδυνους και λόγο ότι η αρχιτεκτονική με τα τρία επίπεδα είχε ελαττώματα βγήκε η νέα αυτή εκδοχή. Όπου πλέον το επίπεδο υποστήριξης στέλνει (ασύρματα ή ενσύρματα) της πληροφορίες στο επίπεδο δικτύου.



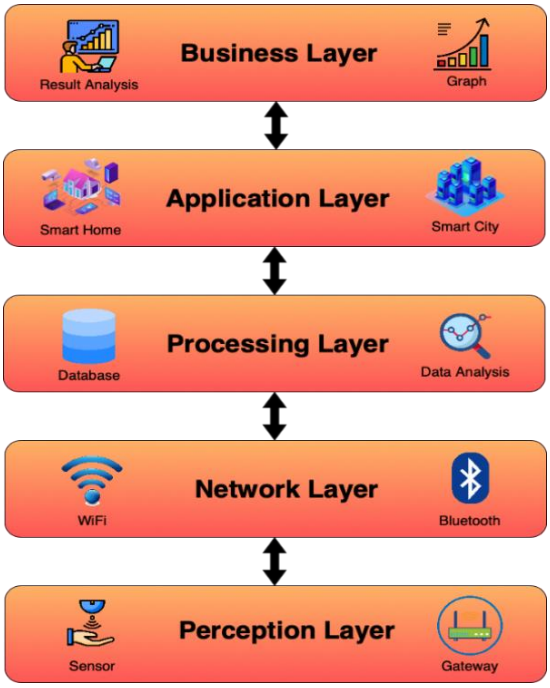
Εικόνα 2.13: "Αρχιτεκτονική τεσσάρων επιπέδων"
Πηγή: MDPI

❖ Αρχιτεκτονική πέντε επιπέδων

Παρόλα που η εφαρμογή με τα τέσσερα βοήθησε στην ανάπτυξη του διαδικτύου των πραγμάτων υπήρχαν ζητήματα ασφαλείας και σε αυτήν την αρχιτεκτονική. Έτσι φτάσαμε στα πέντε επίπεδα όπου κρατάει τα τρία επίπεδα των προηγουμένων αρχιτεκτονικών, δηλαδή το επίπεδο αντίληψης, μεταφοράς και εφαρμογής. Ενώ προσθέτει το επίπεδο επεξεργασίας και επιχειρηματικότητας για να καταφέρει να ολοκληρώσει τις διάφορες απαιτήσεις που έχει το IoT.

Το **επίπεδο επεξεργασίας (Processing Layer)**, όπως φαίνεται στην εικόνα, μπαίνει ανάμεσα στο επίπεδο του δικτύου και των εφαρμογών με σκοπό να επεξεργάζεται τις πληροφορίες που συλλέγονται. Βασική του ευθύνη είναι να εξάγει τις χρήσιμες πληροφορίες και να καταστρέψει τις άχρηστες πληροφορίες.

Ενώ το **επιχειρησιακό επίπεδο (Business Layers)** που προστέθηκε έχει αρμοδιότητες να διαχειρίζεται τις εφαρμογές αλλά και να κάνει τους διάφορους ελέγχους των εφαρμογών αυτών. Επιπλέον, αυτό το επίπεδο έχει και άλλες ευθύνες όπως τη διαχείριση του απορρήτου των χρηστών αλλά και δυνατότητες να ξέρει τον τρόπο δημιουργίας, αποθήκευση και αλλαγών των διάφορων πληροφοριών.



Εικόνα 2.14: "Αρχιτεκτονική πέντε επιπέδων"
Πηγή: TheTechPlatform

2.6 Κυβερνοασφάλεια και θέματα ασφάλειας στο IoT

Σε ένα σύστημα όπως το διαδίκτυο των πραγμάτων όπου παράγει και καταναλώνει μεγάλους όγκους δεδομένων η ασφάλεια τους αποτελεί σημαντικό κομμάτι. Όπως είναι αναμενόμενο για να υπάρξει ασφάλεια στο Internet of Things πρέπει να διασφαλιστεί τόσο στις διάφορες συσκευές που το αποτελούν όσο και στις υπηρεσίες του. Ειδικά αν σκεφτούμε ότι οι συσκευές που το αποτελούν συνδέονται στο διαδίκτυο, το όποιο όμως περιέχει αρκετούς κίνδυνους και πολλά τρωτά σημεία που κάποιος κακόβουλος χρήστη μπορεί να χρησιμοποίηση προς όφελος του.

Έτσι γίνεται αντιληπτή η ανάγκη για τη διαχείριση και την προστασία από τους κίνδυνους αυτούς και σε αυτό έρχεται να βοηθήσει η κυβερνοασφάλεια (Cybersecurity). Αν και είναι δύσκολο να ορίσουμε την κυβερνοασφάλεια, καθώς δεν έχει ευρέως αποδεκτό ορισμό, ωστόσο ο όρος χρησιμοποιείται για να διασφαλίσει ότι θα τηρηθούν τα μέτρα που παίρνονται σχετικά με την προστασία συστημάτων πληροφοριών και των χρηστών τους. Οι ορισμοί που χρησιμοποιούνται για να περιγράψουν την έννοια διαφέρουν και αυτό δείχνει την πολυδιάστατη μορφή της κυβερνοασφάλειας. Για παράδειγμα, στους πολίτικους κύκλους την Ευρωπαϊκή Ένωση ο όρος της κυβερνοασφάλειας δε χρησιμοποιείται μόνο για την ασφάλεια δικτύων και πληροφοριών αλλά και για την αντιμετώπιση κάθε παράνομης δραστηριότητας με τη χρήση ψηφιακών τεχνολογιών στον κυβερνοχώρο. Παρ' όλα αυτά δε διαθέτει κοινό ορισμό, κοινή αντίληψη και συλλογική όραση για την κυβερνοασφάλεια.

Εικόνα 2.15: "Ασφάλεια"
Πηγή: Kloudlearn

Στο κομμάτι του διαδικτύου των πραγμάτων η κυβερνοασφάλειας αποκτάει ακόμα μεγαλύτερο έργο, αφού κάποια χαρακτηρίστηκα του IoT μπορούν να επηρεάσουν τη διαχείριση των κινδύνων στον κυβερνοχώρο σε σύγκριση με τις συμβατικές συσκευές πληροφορικής. Οι λόγοι ποικίλουν ένας από αυτούς θα μπορούσε να ήταν οι τρόποι που οι συσκευές IoT αλληλεπιδρούν με τον φυσικό κόσμο σε σύγκριση με τις συμβατικές συσκευές πληροφορικής. Όπως επίσης δεν είναι το ίδιο εύκολο οι συσκευές IoT να διαχειρίζονται και να παρακολουθούνται σε σύγκριση με τις συμβατικές συσκευές. Αφού μπορεί αυτό να χρειαστεί χειροκίνητη διαχείριση μεγάλων αριθμών συσκευών IoT, περισσότερη εξειδίκευση του προσωπικού και εργαλεία, ώστε να καταφέρουν τη διαχείριση ή παρακολούθηση των συσκευών IoT στις διαφορές ποικιλίες λογισμικών που διαθέτουν και να αντιμετωπίσουν επιτυχώς τους κίνδυνους.

Παρ 'όλα αυτά οι στόχοι ασφαλείας σε IoT συστήματα συμβαδίζουν με τις προκλήσεις στην ασφάλεια των παραδοσιακών Πληροφοριακών Συστημάτων (Information Systems - IS), καθώς και αυτά στοχεύουν στη διαθεσιμότητα των αρχείων, την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Όπου η διαθεσιμότητα αρχείων αφορά την αποθήκευση αρχείων του χρήστη (για παράδειγμα η αποθήκευση προσωπικών φωτογραφιών σε κάποια online εφαρμογή) και κατά πόσο εύκολη είναι η πρόσβαση του σε αυτά. Εξασφαλίζοντας παράλληλα τόσο την εμπιστευτικότητα δηλαδή τα προσωπικά δεδομένα (όπως κωδικοί email, στοιχεία για την ηλεκτρονική είσοδο σε λογαριασμούς τραπεζών κλπ.) να διατηρούνται μη διαθέσιμα σε τρίτα άτομα, όσο και την ακεραιότητα όπου αναφέρεται στην εξασφάλιση ότι τρίτα πρόσωπα δε θα τροποποιήσουν τα δεδομένα του χρήστη. Αν και στις υπηρεσίες και συσκευές IoT η εμπιστευτικότητα αποτελεί ένα βασικό θέμα, καθώς ο χρηστής έχει δυνατότητα πρόσβασης στα δεδομένα αλλά και σε εξουσιοδοτημένα αντικείμενα. Άρα η ανάγκη για σωστό έλεγχο και εξουσιοδότηση αλλά και η ύπαρξή μηχανισμών ελέγχου ταυτότητας και διαχείρισης της είναι σημαντικό κομμάτι της ασφάλειας. Κατά συνέπεια διασυνδεδεμένες συσκευές του IoT θα πρέπει να αναγνωρίζουν άτομα ή και άλλες συσκευές ώστε να μπορεί να γίνεται η επαλήθευση ότι είναι εξουσιοδοτημένα για την πρόσβαση.

Οι προκλήσεις όμως του IoT στο κομμάτι της ασφαλείας δε σταματάνε στους στόχους των παραδοσιακών πληροφοριακών συστημάτων καθώς υπάρχουν και άλλες προκλήσεις όπως για παράδειγμα οι ευπάθειες και τα τρωτά σημεία που δημιουργούνται από την εφαρμογή του cloud και απασχολούν ειδικά την ασφάλεια του Internet of Things, λόγω της συγχώνευσης του με το cloud. Ενώ άλλοι κίνδυνοι ασφαλείας μπορεί να έχουν να κάνουν με υποβαθμισμένα (όπως για παράδειγμα κακώς σχεδιασμένα ή ξεπερασμένα) προϊόντα και υπηρεσίες IoT. Ή ακόμα ένα μη επιδιορθωμένο API (Application Programming Interface)

μπορεί να επηρεάσει και να έκθεση ολόκληρο το σύστημα Internet of Things σε πιθανών κακόβουλες ενέργειες κάποιον χρηστών, καθώς μερικές εφαρμογές του IoT βασίζονται σε ιστό ή και σε κινητά, όπου βασικό κομμάτι στη σχεδίαση τους έχει παίξει το API.

Τέλος, πολλές προκλήσεις της κυβερνοασφάλειας του IoT υπάρχουν λόγω εγγενών ευπαθειών του συστήματος, όπως είδαμε παραπάνω, που εκθέτοντας έτσι όλο το σύστημα σε διάφορες επιθέσεις. Ωστόσο, για να δούμε μετρά ασφάλειας στο κομμάτι αυτό θα πρέπει να αναλύσουμε περαιτέρω πρώτα τις απειλές και τις επιθέσεις που μπορούν να υπάρξουν σε ένα σύστημα IoT.

2.7 Απειλές στις τεχνολογίες IoT στον κυβερνοχώρο

Το internet of things έχει εισχωρήσει τόσο στην καθημερινότητα των ατόμων όσο και σε οργανισμούς, δίνοντας έτσι περισσότερες δυνατότητες αλλά και απειλές. Αφού οι συσκευές και τα συστήματα IoT που χρησιμοποιούμε συνεχώς αυξάνονται και η προστασία τέτοιου όγκου από τις απειλές αυτές δεν είναι συχνά εύκολη αν σκεφτούμε τους διαφορετικούς τύπους ασφάλειας και πρότυπα που υπάρχουν στις συσκευές αυτές.

Οι ψηφιακές αυτές απειλές ονομάζονται κυβερνοαπειλές καθώς βρίσκονται στο κυβερνοχώρο, όπου με τον όρο αυτόν εννοούμε το περιβάλλον που έχει δημιουργηθεί από τα δίκτυα επικοινωνιών. Μία επιτυχημένη μορφή του κυβερνοχώρου θα διέθετε πολλαπλά επίπεδα προστασίας που θα διαδιδόντουσαν σε όλους τους υπολογιστές, τα δίκτυα, τα προγράμματα και τα δεδομένα για να τα διατηρήσει ασφαλή. Ωστόσο, κάτι τέτοιο δεν επιτυγχάνεται σε απόλυτο βαθμό και αυτό γιατί η αύξηση των τεχνολογιών συνεπάγεται τις αύξηση των κυβερνοαπειλών.

Όταν αυτές οι κυβερνοαπειλές παύουν να είναι απλά ψηφιακοί κίνδυνοι αλλά άτομα ή ομάδες ατόμων που στοχεύουν με κακόβουλες ενέργειες για να καταστρέψουν, τροποποιήσουν, κλέψουν, υποκλέψουν ή ακόμα να πάρουν πρόσβαση σε μη εξουσιοδοτημένες πληροφορίες κάποιου ή κάποιων ατόμων μέσω του κυβερνοχώρου τότε λέγονται κυβερνοεπιθέσεις. Ειδικότερα στην περίπτωση του διαδικτύου των πραγμάτων οι κυβερνοεπιθέσεις αποτελούνται από οποιαδήποτε ενεργεία που εκμεταλλεύεται τις αδυναμίες που υπάρχουν στην ασφάλεια ενός συστήματος δημιουργώντας έτσι κάποιο πρόβλημα σε αυτό.

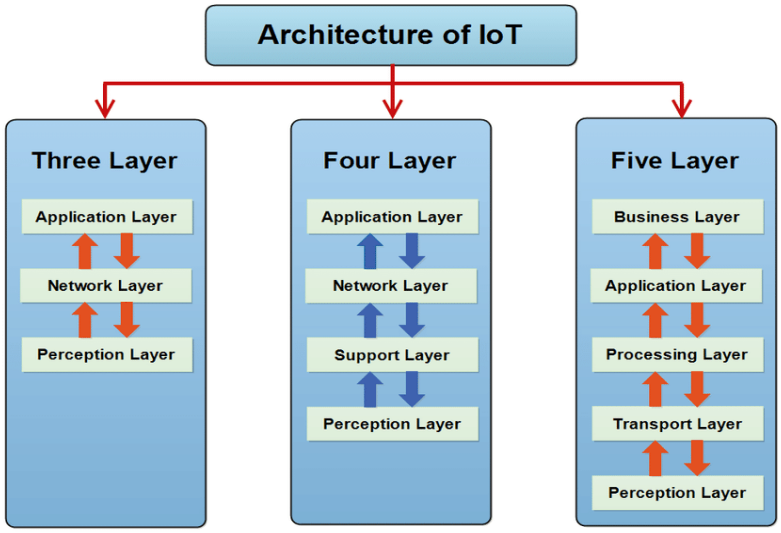
Εικόνα 2.16: "Κυβερνοαπειλές στο διαδίκτυο των πραγμάτων"
Πηγή: Forbes

Οι διαστάσεις του προβλήματος των κυβερνοεπιθέσεων φαίνονται αν συλλογιστούμε ότι άτομα, επιχειρήσεις, οργανισμοί και έθνη αντιμετωπίζουν τις ίδιες απειλές στον κυβερνοχώρο. Ενώ οι τρόποι των κυβερνοεπιθέσεων ποικίλουν και συνεχώς αυξάνονται με την εξέλιξη της τεχνολογίας την αύξηση των διασυνδεδεμένων συσκευών και των συστημάτων IoT. Επίσης, οι μεγάλοι όγκοι δεδομένων που παράγει και καταναλώνει το IoT και ο μεγάλος όγκος συσκευών που το αποτελούν είναι οι κύριοι λόγοι που κακόβουλα λογισμικά μπορούν να κρυφτούν σε αυτά.

Τέλος, οι συσκευές του Internet of Things είναι ευάλωτες απέναντι σε επιθέσεις DoS, DDoS, σε έγχυση κώδικα, επιθέσεις man in the middle και πλαστογράφηση. Μερικές από τις επιθέσεις αναλύονται εκτενέστερα παρακάτω, όπου τις εξηγούμε ανάλογα σε πιο επίπεδα αρχιτεκτονικών (ενότητα 2.4) γίνονται συνήθως οι επιθέσεις αυτές.

2.7.α Επιθέσεις σε επίπεδα αρχιτεκτονικών IoT

Για την καλύτερη κατανόηση του προβλήματος των κυβερνοεπιθέσεων αποφασίσαμε να αναλύσουμε τους διάφορες τύπους επιθέσεων που υπάρχουν ανάλογα με τα επίπεδα των αρχιτεκτονικών που αναλύσαμε παραπάνω (Ενότητα 2.4).

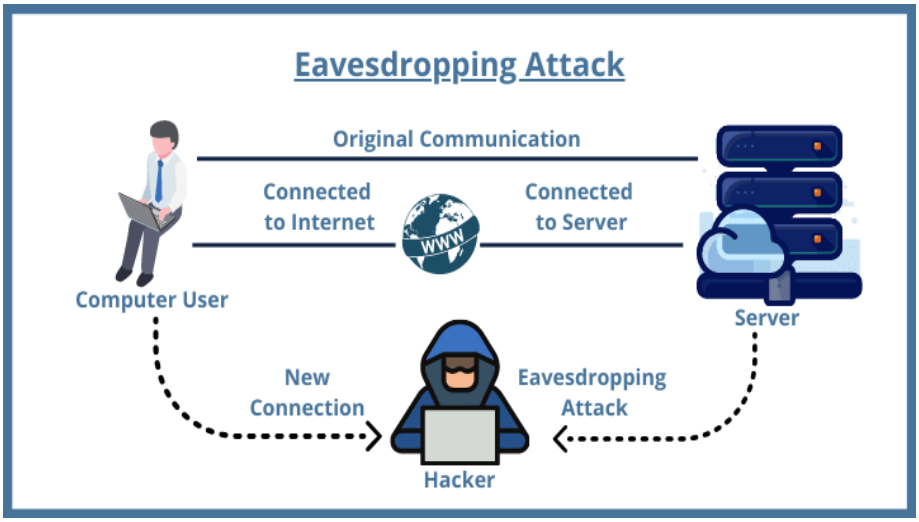


Εικόνα 2.17: "Αρχιτεκτονικές του IoT"
Πηγή: ResearchGate

Το πρώτο επίπεδο που υπάρχει και στις τρεις αρχιτεκτονικές που αναλύσαμε είναι της **αντίληψης** ή όπως συχνά αλλιώς το αναφέρουν το στρώμα αισθητήρων. Είναι απαραίτητο για την ύπαρξη του Internet of Things αφού αποτελείται από τους διάφορους αισθητήρες που συλλέγουν τα δεδομένα. Αυτός είναι ο κυρίως λόγος που αποτελεί στόχο για τους επιτιθέμενους, αφού μπορούν με μια επιτύχει επίθεση να αντλήσουν διάφορες πληροφορίες, κάνοντας αντικατάσταση των αισθητήρων που υπάρχουν με δικούς τους. Μερικές από τις πιο συνηθισμένες απειλές στο επίπεδο αντίληψης είναι οι εξής:

- **Υποκλοπή (Eavesdropping)**

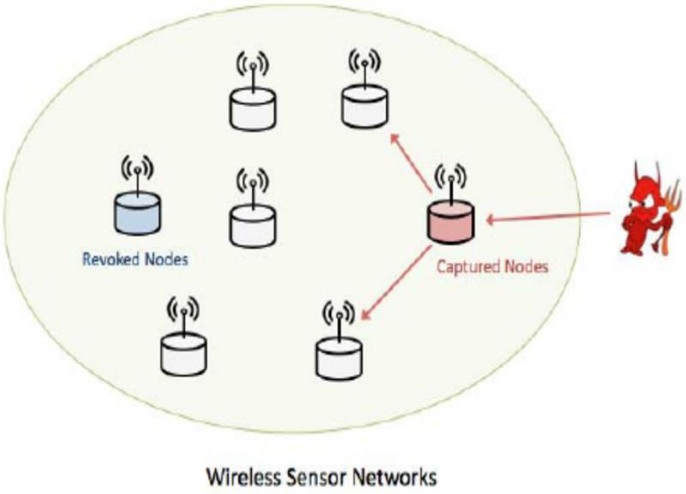
Στην περίπτωση αυτή ο κακόβουλος χρήστης μπαίνει ανάμεσα σε μια συνομιλία και υποκλέπτει πληροφορίες που μεταφέρονται μέσα στο δίκτυο. Η υποκλοπή συνήθως γίνεται σε πραγματικό χρόνο με τις διάφορες δραστηριότητες (πχ μηνύματα, τηλεφωνήματα κλπ.) να παρεμποδίζονται από τον εισβολέας και όπως είναι αναμενόμενο είναι μη εξουσιοδοτημένη επίθεση.



Εικόνα 2.18: "Υποκλοπή"
Πηγή: Huawei

❖ **Καταγραφή κόμβου (Node Capture)**

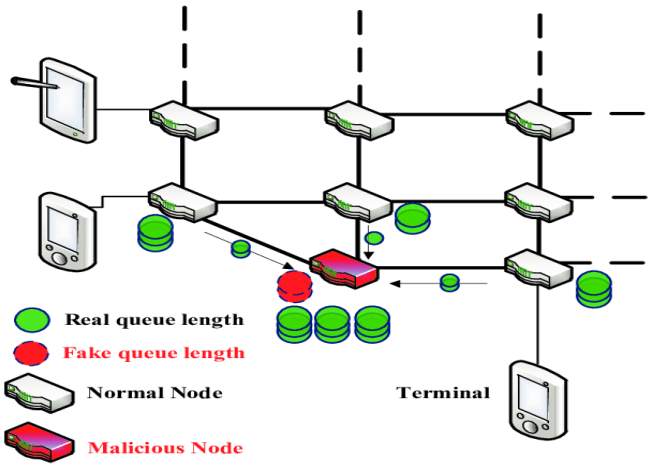
Σε αυτήν την περίπτωση ο κακόβουλος χρήστης παίρνει τον έλεγχο ενός κόμβου κλειδιού, όπως είναι ένας κόμβος πύλης, δίνοντας του τη δυνατότητα να διαρρεύσει όλες την πληροφορίες. Αποτελεί από τις πιο επικίνδυνες επιθέσεις στο επίπεδο του IoT.



Εικόνα 2.19: "Καταγραφή κόμβου"
Πηγή: ResearchGate

❖ **Ψεύτικος και κακόβουλος κόμβος (Fake node and Malicious)**

Σε αυτήν την περίπτωση ο κακόβουλος χρήστη βάζει ένα κόμβο μέσα στο σύστημα, με τον όποιο θα μπορεί να μεταδώσει λανθασμένες πληροφορίες. Ο κόμβος αυτός πέρα από το κομμάτι των πληροφοριών, καταναλώνει αρκετή ενέργεια από τους κανονικούς κόμβους και έχει τη δυνατότητα κάτω από κάποιες προϋποθέσεις να καταστρέψει το δίκτυο!



Εικόνα 2.20: "Fake node and malicious"
Πηγή: ResearchGate

❖ **Timing Attack**

Στην περίπτωση αυτή ο κακόβουλος χρήστης μέσω των τρωτών σημείων μπορεί να πάρει μυστικά για την ασφάλεια ενός συστήματος. Αυτό το επιτυγχάνει με το να κοιτάει ποσό χρόνο χρειάζεται το σύστημα για να ανταποκριθεί σε διαφορετικά ερωτήματα, εισόδους ή κρυπτογραφικούς αλγορίθμους.

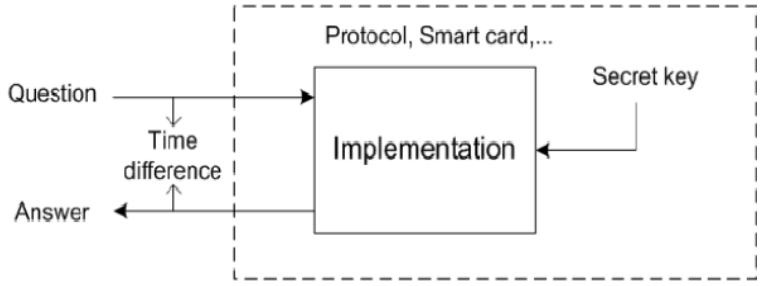


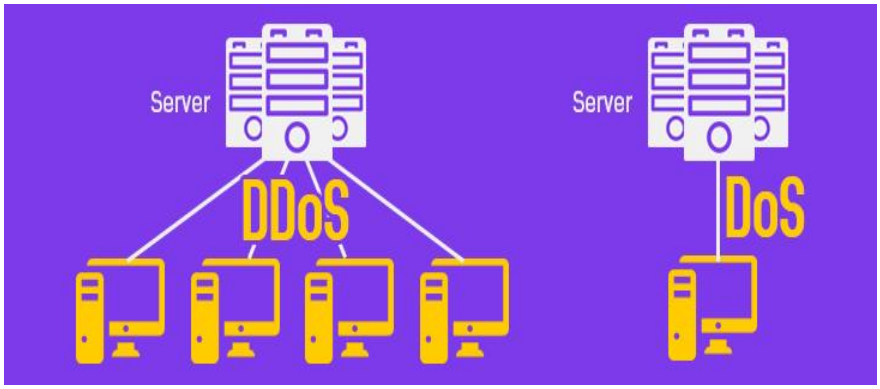
Fig. 1. A conceptual view of the timing attacks.

Εικόνα 2.21: "Timing attack"
Πηγή: SEMANTIC SCHOLAR

Το δεύτερο επίπεδο είναι του **δικτύου** ή όπως αλλιώς ονομάζεται στρώμα μετάδοσης, όπου μεταδίδει τις πληροφορίες και είναι υπεύθυνο για τις συνδέσεις. Έχει αρκετά ζητήματα ασφάλειας όσο αναφορά την ακεραιότητα και τον έλεγχο ταυτότητας των δεδομένων. Τα πιο συνηθισμένα προβλήματα σε θέματα ασφάλειας και επιθέσεις που μπορούμε να συναντήσουμε σε αυτό το επίπεδο φαίνονται παρακάτω:

❖ **Επιθέσεις DoS και DDoS**

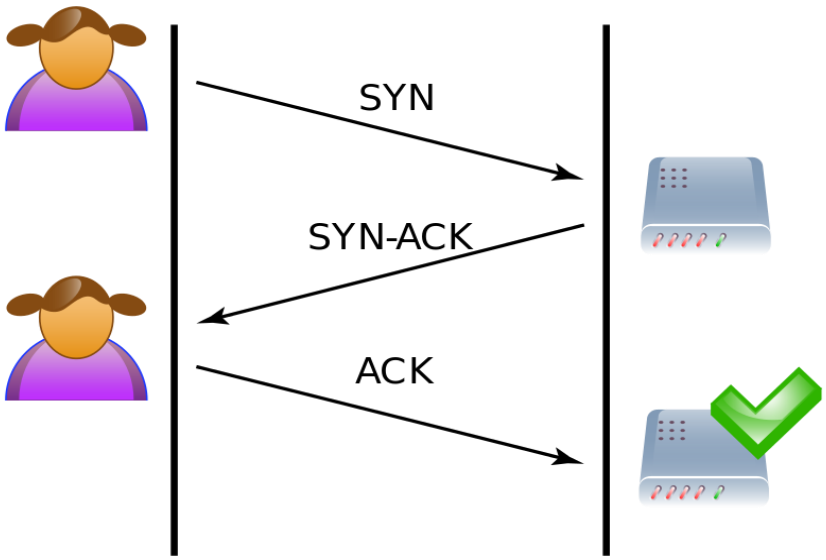
Οι επιθέσεις άρνηση εξυπηρέτησης (**επιθέσεις DoS**–Denial of service) στοχεύουν συνήθως στην εξάντληση των πόρων του συστήματος. Κύριος σκοπός τους είναι να μην μπορεί το σύστημα να ανταποκριθεί σε αιτήματα υπηρεσιών είτε λόγω απενεργοποίησης της υπηρεσίας, είτε λόγω επιβράδυνσης της απόδοσης της. Η επίθεση αυτή επηρεάζει το δίκτυο με στόχο το θύμα να μην μπορεί να έχει πρόσβαση σε αυτό. Από την άλλη πλευρά οι κατανεμημένες επίθεσης άρνησης εξυπηρέτησης (**επιθέσεις DDoS**- Distributed denial of service) ενώ είναι και αυτή μια επίθεση στους πόρους του συστήματος και στοχεύει στην άρνηση της εξυπηρέτησης δρα διαφορετικά. Αποστέλνονται υπερβολικός αριθμός πακέτων με σκοπό να βγάλει την υπηρεσία μη διαθέσιμη.



Εικόνα 2.22: "DDoS and DoS attack"
Πηγή: iplocation

Υπάρχουν δυο τρόποι για να το πετύχει αυτό, ο ένας είναι να στείλει απευθείας πολλά πακέτα στο μηχάνημά του θύματος. Ενώ ο άλλος στέλνει πακέτα σε διαφορετικούς προορισμούς με τη διεύθυνση IP του στόχου να φαίνεται σαν αποστολέας. Για να επιτεθούν, οι δυο αυτοί τρόποι εκμεταλλεύονται τις τυχόν αδυναμίες που έχουν τα πρωτόκολλα TCP/IP μέσω διάφορων τεχνικών όπως για παράδειγμα η **επίθεση TCP SYN flood**. Η επίθεση αυτή είναι μια "πλημμύρα" αιτημάτων TCP SYN από τον κακόβουλο χρήστη προς έναν στόχο.

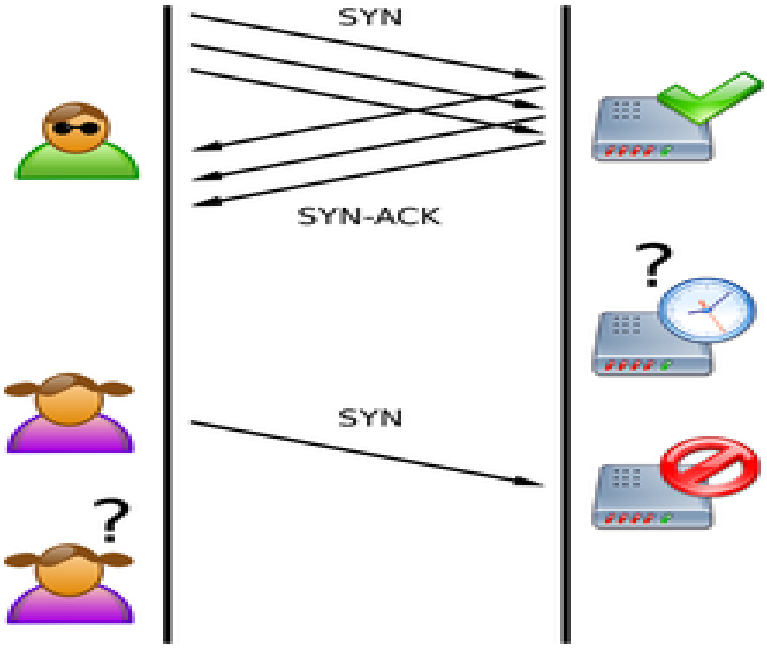
Οι αιτήσεις TCP SYN είναι στην ουσία αίτηση σύνδεση ενός υπολογιστή με έναν διακομιστή. Η διαδικασία δημιουργίας συνδέσεις TCP, ακολουθεί κάποια βήματα του πρωτοκόλλου TCP. Στο πρώτο βήμα ο πελάτης κάνει αίτηση TCP SYN για να συγχρονιστεί με τον διακομιστή (server). Στη συνέχεια ο διακομιστής απαντάει στέλνοντας πακέτα TCP SYN-ACK όπου είναι πακέτα αναγνώρισης – αποδοχής της αίτησης. Τελικό στάδια αποτελεί η απάντηση του πελάτη ότι δέχτηκε και αυτός τη σύνδεση και αρά στέλνει πακέτα TCP ACK.



Εικόνα 2.23: "Syn Flood"
Πηγή: Wikipedia

Έτσι οι επιθέσεις αυτής τις κατηγορίας έχουν να κάνουν με το πρώτο βήμα του πρωτοκόλλου TCP, στέλνοντας ένα σύνολο αιτημάτων, με σκοπό την κατανάλωση πόρων

του συστήματός. Αυτό επιτυγχάνεται αφήνοντας αυτές τις αίτησης που στέλνει ο δράστης ημιτελής, καθώς φτάνουν μέχρι το δεύτερό βήμα και η απάντηση αποδοχής από τον πελάτη - εισβολέα δε φτάνει ποτέ. Προϋπόθεση για να πετύχει αυτή η επίθεση και να καταναλώσει πόρους τους συστήματος είναι ο διακομιστής να δεσμεύει κατευθείαν πόρους μετά το δεύτερο βήμα δηλαδή την απάντηση αποδοχής από τον διακομιστή.



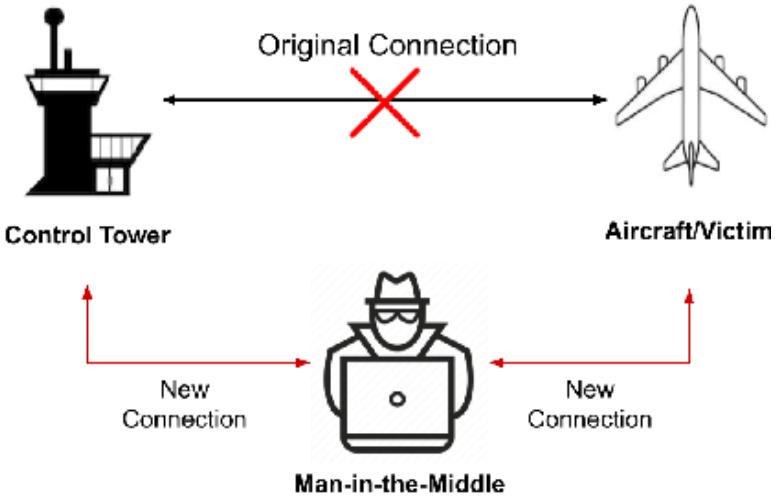
Εικόνα 2.24: " Syn flood attack"
Πηγή: Wikipedia

Η TCP Syn flood είναι μια υποκατηγορία από τους πολλούς τύπους επιθέσεων του DoS και DDoS και μπορούν να βλάψουν το σύστημα IoT. Τέλος, αξίζει να σημειωθεί ότι από αυτές τις δυο οι επιθέσεις οι DDoS είναι μεγαλύτερες, πιο καταστροφικές και σε ορισμένες περιπτώσεις πιο δύσκολο για το θύμα να τις ανιχνεύσει και να τις σταματήσει.

❖ **Man in the middle attack**

Μια επίθεση Man-in-the-Middle (MITM) επιτυγχάνεται με τον δράστη να μπαίνει στη μέση μίας επικοινωνίας, με τον ίδιο να λαμβάνει και να μεταδίδει τα μηνύματα. Έχοντας έτσι τη δυνατότητα να παρακολουθεί παράνομα τη συνομιλία αλλά και να την τροποποίηση. Σε μια τέτοια επίθεση τα δυο μέλη όπου επικοινωνούν μεταξύ του δεν ξέρουν την ενδιάμεση παρέμβαση του δράστη και πιστεύουν ότι η επικοινωνία είναι ασφαλής.

Το Man-in-the-Middle επιτυγχάνεται τόσο με την παρακολούθησης από τον δράστη στα τελικά σημεία της επικοινωνίας όσο και με τη χρήση διάφορων τρόπων ανακατεύθυνσης δεδομένων. Στην πρώτη κατηγορία απαιτείται η εγκατάσταση λογισμικού απευθείας σε κάποιο μέσο επικοινωνίας (όπως είναι η ψηφιακή συσκευή και το Wi-Fi). Ενώ η δεύτερη περίπτωση, δηλαδή η ανακατεύθυνση δεδομένων, μπορεί να επιτευχθεί σε διάφορα επίπεδα όπως είναι στα τοπικά δίκτυα - IPV4 **ARP spoofing** και στο επίπεδο δικτύου - **DNS spoofing**.



Εικόνα 2.25: "Man in the middle attack"
Πηγή: SEMANTIC SCHOLAR

Όπου το **ARP spoofing ή ARP Cache Poisoning** έχει να κάνει με το πρωτόκολλο ανάλυσης διευθύνσεων ARP (Address Resolution Protocol). Στην ουσία κάθε διασυνδεδεμένη συσκευή στο διαδίκτυο έχει μια διεύθυνση IP και μία MAC. Όπου η διεύθυνση IP (Internet Protocol) προσδιορίζει τη θέση μιας συσκευής στο δίκτυο, και το ίδιο το δίκτυο όπου είναι συνδεμένη. Για αυτόν τον λόγο κάθε φορά που συνδέεται σε διαφορετικό δίκτυο αλλάζει η διεύθυνση IP. Από την άλλη πλευρά η MAC (Media Address Control) προσδιορίζει την ίδια τη συσκευή και για αυτό σε αντίθεση με την IP δεν αλλάζει. Όταν θέλει να επικοινωνήσει μια διαδικτυακή συσκευή με μία άλλη το επίπεδο δικτύου ενσωματώνει μια διεύθυνση IP προορισμού, όμως το επίπεδο πρόσβασης του δικτύου ξέρει μόνο τη διεύθυνσης MAC. Έτσι για να επικοινωνήσουν μεταξύ τους δύο διαδικτυακές συσκευές, γίνεται η σύνδεση των διευθύνσεών με τη βοήθεια του ARP. Στην ουσία η συσκευή που θέλει να επικοινωνήσει στέλνει αιτήματα ARP για να μετάφραση μια διεύθυνσή IP σε MAC και η συσκευή όπου διαθέτει τη διεύθυνση απαντάει πίσω (δίνοντας τη MAC διεύθυνση). Έτσι η συσκευή όπου έκανε το αίτημα μπορεί να χρησιμοποιήσει και να αποθήκευση προσωρινά τις πληροφορίες αυτές στη μνήμη του πρωτοκόλλου αυτού. Στην τεχνική ARP Cache Poisoning ή αλλιώς ARP Spoofing ο εισβολέας στην προσπάθεια του να μπει στη μέση μιας επικοινωνίας "δηλητηριάζει" την προσωρινή μνήμη του πρωτοκόλλου ανάλυσης διευθύνσεων ARP. Αυτό το επιτυγχάνει περιμένοντας αρχικά ένα αίτημα ARP στο οποίο δίνει τη διεύθυνση MAC του, "δηλητηριάζοντας" έτσι τη μνήμη του πρωτοκόλλου και αφήνοντας το θύμα να πιστεύει ότι είναι ο σωστός αποστολέας. Για να γίνει κάτι τέτοιο προϋποθέτει ο δράστης να απαντήσει πιο γρήγορα από τον νόμιμο παραλήπτη. Καθώς το πρωτόκολλο ARP δεν απαιτεί έλεγχο ταυτότητας και άρα οι συσκευές μπορούν να προσθέτουν και να ενημερώνουν διευθύνσεις (τόσο IP όσο και MAC) είτε είναι σωστές είτε είναι λανθασμένες.

Ενώ από την άλλη πλευρά το **DNS spoofing ή DNS Cache Poisoning,** όπου αναφέρθηκε παραπάνω έχει να κάνει με τη "δηλητηρίαση" της κρυφής μνήμης του DNS. Το DNS (Domain Naming System) είναι το πρωτόκολλο αυτό όπου μετατρέπει τα ονόματα των διαδικτυακών συσκευών που χρησιμοποιούμε στις αντίστοιχες IP διευθύνσεις. Ουσιαστικά αντιστοιχεί τα ονόματα, για παράδειγμα "www.google.gr" στις IP διευθύνσεις τους, που έχουν τη μορφή για IPv4 X.X.X.X με τα X να περνούν τιμές από 0 έως 255 και για IPv6 τη μορφή X:X:X:X:X:X:X:X με τα X σε αυτήν την περίπτωση να περνούν τιμές από 0000 μέχρι FFFF του δεκαεξαδικού συστήματος. Στη δηλητηρίαση της κρυφής μνήμης DNS (DNS Cache Poisoning) ή αλλιώς Spoofing DNS γίνεται όταν ο δράστης αποθηκεύει στη μνήμη

του DNS λανθασμένες απαντήσεις για κάποιους ιστότοπους στέλνοντας τους χρήστες σε λάθος ιστοσελίδες. Οι ιστοσελίδες αυτές μπορεί να μοιάζουν αρκετά με την κανονική - πραγματική, αλλά να μην είναι και μέσω αυτού ο εισβολέας να καταγράφει τα στοιχεία όπου θα εισάγει ο χρήστης. Ωστόσο, επειδή δεν υπάρχει δυνατότητα επαλήθευσης των αντιστοιχιών αυτών στο DNS, σε περίπτωση παρεμβάσεων οι λανθασμένες αντιστοιχίες των ονομάτων με τις διευθύνσεις IP είτε θα αφαιρεθούν χειροκίνητα, είτε θα παραμείνουν μέχρι να λήξη ο χρόνο ζωής τους (TTL).

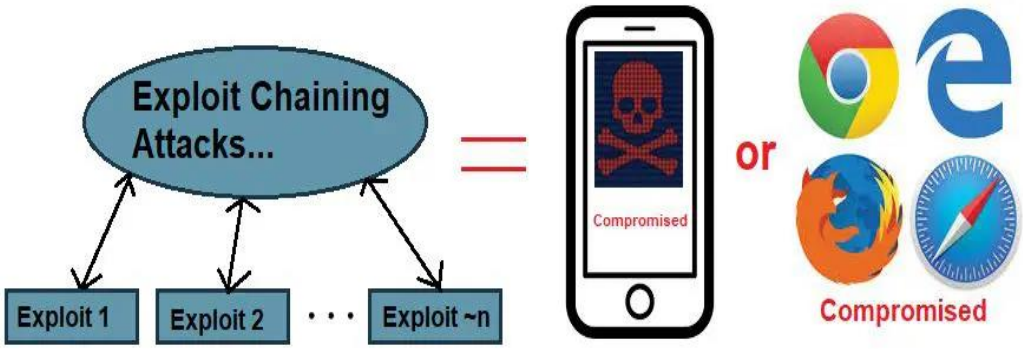
Αυτές είναι δυο από τις πολλές τεχνικές για να κάνει κάποιος επίθεση Man-in-the-Middle!

❖ **Storage attack**

Οι επιθέσεις αυτές γίνονται σε συσκευές αποθήκευσης ή στο cloud όπου οι διάφορες πληροφορίες που συλλέγονται αποθηκεύονται εκεί. Τόσο σε συσκευές αποθηκεύσεις όσο και στο cloud μπορούν να πραγματοποιηθούν διαφορές επιθέσεις με αποτέλεσμα την τροποποίηση των πληροφοριών που αποθηκεύονται και μετατρέπονται σε εσφαλμένες πληροφορίες.

❖ **Exploit attack**

Αυτού του τύπου η επίθεση εκμεταλλεύεται ευπαθή σημεία ασφαλείας (σε εφαρμογές, συστήματα ή υλικά) με απώτερο σκοπό να απόκτηση ελέγχου του συστήματος ή να κλέψει αποθηκευμένες πληροφορίες του δικτύου.

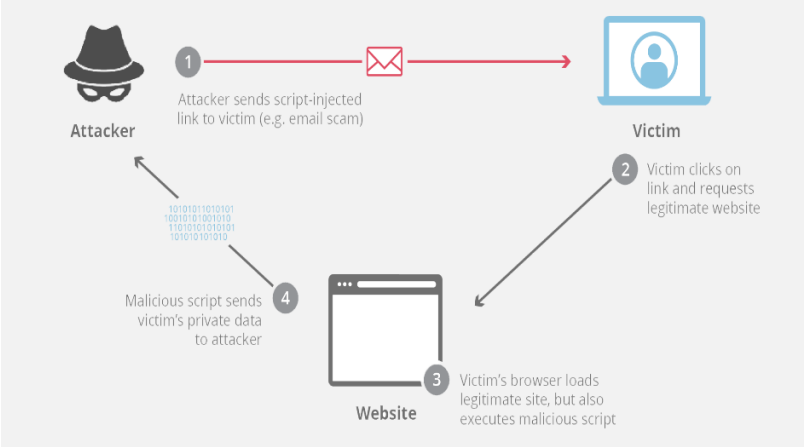


Εικόνα 2.26: "Exploit attack"
Πηγή: CyberHoot

Τρίτο και τελευταίο επίπεδο για τη βασική αρχιτεκτονική IoT είναι το επίπεδο **εφαρμογών** οι συχνές επιθέσεις σε αυτό το επίπεδο είναι:

❖ **Cross-site scripting (XSS) attack**

Η επίθεση Cross-site scripting έχει να κάνει με κάποιο κενό ασφαλείας όπου δίνει τη δυνατότητα στους επιτιθέμενους να εισάγουν scripts (σενάρια) σε μία ασφαλή ιστοσελίδα. Τα σενάρια είναι προγράμματα ή κομμάτια κώδικα που στην περίπτωση μας για να εκτελεστούν χρειάζονται το πρόγραμμα περιήγησης. Έτσι όταν κάποιος μπει σε αυτήν την ιστοσελίδα τα σενάρια όπου έχει τοποθετήσει ο κακόβουλος χρήστης θα εκτελεστούν αυτόματα, χωρίς όμως το πρόγραμμα περιήγησης του να γνωρίζει κάτι, καθώς η ιστοσελίδα θα φαίνεται αξιόπιστη. Ο κακόβουλος κώδικας μπορεί να έχει πρόσβαση σε δεδομένα του χρήστη που αποθηκεύονται προσωρινά κατά την περιήγηση του στην ιστοσελίδα.



Εικόνα 2.27: "Cross site scripting στο διαδίκτυό των πραγμάτων"
Πηγή: CLOUDFLARE

Οι επιθέσεις μπορούν να χωρίζονται σε τρεις κατηγορίες Αποθηκευμένα XSS (Stored XSS), Αντικατοπτριζόμενα XSS (Reflected XSS) και Dom (Document Object Model) based XSS.

Στην πρώτη περίπτωση τα **αποθηκευμένα XSS (Stored XSS)** ο εισβολέας ενσωματώνει κακόβουλα σενάρια στην εφαρμογή ιστού. Αυτά τα σενάρια αποθηκεύονται μονιμά από τον εξυπηρετητή, με σκοπό να εμφανίζονται στην ιστοσελίδα όταν την επισκέπτονται άλλοι χρήστες. Για παράδειγμα, ένα κακόβουλο σενάριο θα μπορούσε να ήταν σε κάποιο πεδίο εισαγωγής στοιχείων του χρήστη. Όταν ο χρήστης ανοίξει την ιστοσελίδα τα κακόβουλα σενάρια αυτά θα φαίνονται ως μέρος τις ιστοσελίδας, με αποτέλεσα να καταλήξει ο χρήστης στην εκτέλεση τους. Με αυτόν το τύπο ο επιτιθέμενος καταφέρνει να διάδοση την επίθεση μέσω της ιστοσελίδας και δε χρειάζεται να στοχεύσει κάποιο συγκεκριμένο χρήστη – θύμα.

Στη δεύτερη περίπτωση τα **αντικατοπτριζόμενα XSS (Reflected XSS)** όπου είναι και από τους πιο συχνούς στις επιθέσεις cross site scripting. Σε αυτήν την περίπτωση η επίθεση λαμβάνει χώρο μέσω του αιτήματος που αποστέλλεται στον διακομιστή και το κακόβουλο σενάριο πρέπει να είναι μέρος αυτού του αιτήματος. Αυτό συμβαίνει όταν κάποιος κακόβουλος χρήστης στέλνει HTTP αιτήματα και αυτό χρησιμοποιείτε αμέσως από τον εξυπηρετητή χωρίς να υπάρχει έλεγχος input sanitization. Η επίθεσή επιτυγχάνεται μέσω το URL που χρησιμοποιείται σαν δόλωμα και είναι η ιστοσελίδα που περιέχει το κακόβουλο σενάριο. Το δόλωμα αποστέλνεται στο θύμα μέσω ηλεκτρονικού ταχυδρομείου ή κάποιου αλλού ιστοτόπου. Βασικό χαρακτηριστικό της επιθέσεις τέτοιου τύπου είναι ότι το σενάριο που χρησιμοποιείται για να γίνει η επίθεση δεν αποθηκεύεται στον εξυπηρετητή που υποστηρίζει την ιστοσελίδα.

Τέλος, το **Dom(Document Object Model) based XSS** έχει να κάνει με τα σενάρια της εφαρμογής του πελάτη όπου γράφουν δεδομένα που δίνονται από τον χρήστης στο μοντέλο αντικειμένου εγγράφου (DOM) και διαβάζονται από την εφαρμογή ιστού με σκοπό τη μετέπειτα εξαγωγή τους στο πρόγραμμα περιηγήσεις. Ουσιαστικά ο εισβολέας μπορεί να εκμεταλλευτεί κάποιο λάθος χειρισμό και μπορεί να βάλει κακόβουλα σενάρια που θα εκτελούνται μετά την ανάγνωση του DOM. Ωστόσο, οι επιθέσεις XSS βασισμένες στον Dom συνήθως είναι δύσκολο να εντοπιστούν καθώς η επιθέσεις γίνονται από την πλευρά του πελάτη και το κακόβουλο σενάριο δε θα φτάσει ποτέ στον διακομιστή.

- **Malicious Code attack**

Η επίθεση **κακόβουλου κώδικα (Malicious Code attack)** έχει ο σκοπό να κάνει ζημιά στο σύστημα, ο κώδικας αυτός μπορεί να μπει σε οποιοδήποτε μέρος του λογισμικού. Ο τύπος αυτός ενεργοποιείται είτε μόνο του είτε να χρειάζεται τη βοήθεια του χρήστη για να εκτελεστεί.

Στο δεύτερο μοντέλο αρχιτεκτονικής εμφανίζεται ένα νέο επίπεδο της **υποστήριξης**, όπου επιβεβαιώνει την αυθεντικότητα του χρήστη που στέλνει τις πληροφορίες και στέλνει τις πληροφορίες στο επίπεδο δικτύου. Αυτό το επίπεδο μπορεί να δεχτεί πολλές επιθέσεις με βασικές να είναι οι DoS και DDoS οπού αναλυθήκαν παραπάνω, με τη διαφορά η επίθεση εδώ σχετίζεται με το δίκτυο. Ο εισβολέας στέλνει τεράστιο όγκο δεδομένων με σκοπό να θέσει την κυκλοφορία του δικτύου μη διαθέσιμη. Απώτερος σκοπός του είναι να μην έχει πρόσβαση ο χρηστής στο σύστημα, λόγω της κατανάλωσης των πόρων του από την επίθεση. Άλλη μια επίθεση είναι κακόβουλη επίθεση σε εσωτερικούς χρήστες (Malicious Insider attack) η οποία ονομάζεται έτσι γιατί συμβαίνει στο εσωτερικό περιβάλλον του IoT για πρόσβαση σε προσωπικές πληροφορίες των χρηστών. Αποτελεί μια πολύπλοκη επίθεση όπου εκτελείται στην ουσία δίνεται εξουσιοδότηση από χρήστη για πρόσβαση σε πληροφορίες αλλού χρήστη.

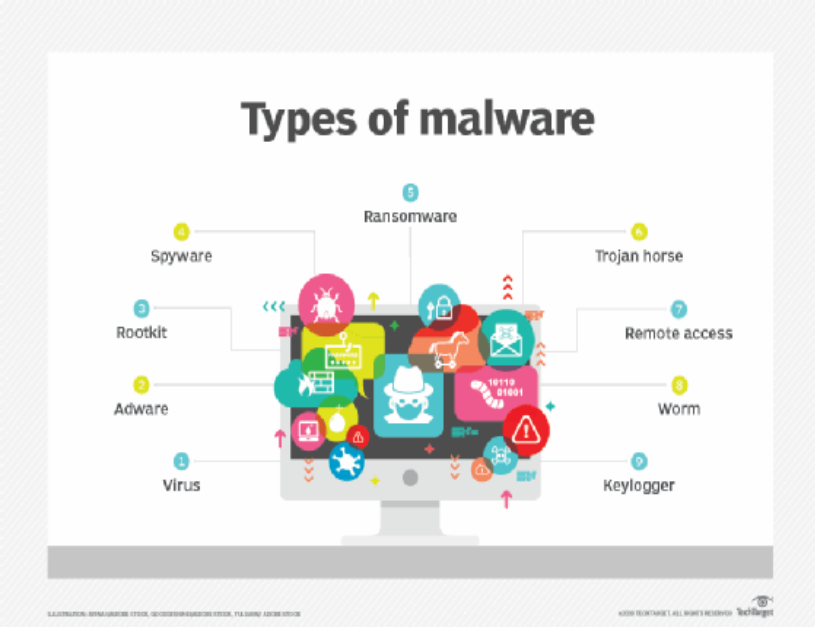
Τέλος, στην αρχιτεκτονική πέντε επίπεδων προθέτονται αλλά δυο επίπεδα το επιχειρησιακό και η επεξεργασία. Αρχικά το **επίπεδο επεξεργασίας** γνωστό και ως στρώμα ενδιάμεσου λογισμικού επεξεργάζεται τις πληροφορίες που φτάνουν σε αυτό, διαγράφοντας τις άχρηστες και κρατώντας τις χρήσιμες. Μερικές από τις επιθέσεις που μπορούν να γίνουν σε αυτό το επίπεδο και μπορούν να επηρεάσουν την απόδοση του είναι:

❖ **Exhaustion**

Η εξάντληση περιλαμβάνει όλους τους τρόπους που κάνει χρήση ο εισβολέας προκειμένου να εξάντληση το IoT όπως για παράδειγμα είδαμε στην επίθεση DoS και DDoS. Ωστόσο, θα μπορούσε να ήταν και αποτέλεσμα άλλων επιθέσεων για εξάντληση στους πόρους του συστήματος (πχ της μνήμης).

❖ **Malware**

Τα **κακόβουλα προγράμματα** (malicious software ή malware) είναι ένας γενικός όρος που συμπεριλαμβάνει κάθε είδους λογισμικό που έχει σχεδιαστεί με σκοπό να βλάψει και εκμεταλλευτεί οποιαδήποτε υπολογιστική συσκευή ή δίκτυο. Τέτοια είδους λογισμικά μπορεί να χρειάζονται ένα πρόγραμμα «ξενιστή» για να εκτελεστούν ή ακόμα και την ανάμειξη του ανθρωπίνου παράγοντα. Αλλά αυτό δεν είναι απαραίτητο καθώς πολλές φόρες μπορούν να εκτελεστούν μόνο τους, όπως κάθε άλλο πρόγραμμα.



Εικόνα 2.28: "Τύποι των κακόβουλων προγραμμάτων "

Πηγή: TechTarget

Υπάρχουν διαφορά ήδη κακόβουλων προγραμμάτων ή αλλιώς κακόβουλων λογισμικών με τον βασικό τύπο οι **ιοί (Virus).** Το συγκεκριμένο κακόβουλο λογισμικό αφού εισβάλει σε κάποια ψηφιακή μηχανή, έχει τη δυνατότητα να αναπαράγεται και να εξαπλώνεται εύκολα σε προγράμματα της. Αφού οι ιοί είναι ικανοί να φτιάξουν τέλεια αντίγραφα τους και κάθε φόρα που ο μολυσμένος υπολογιστής - μηχάνημα έρθει σε επαφή με ένα πρόγραμμα τότε αυτό να μολύνεται με κάποιο από τα αντίτυπα τους. Τα αποτέλεσμα που έχει μια τέτοια επίθεση είναι από το να βλάψει πολλά χρήσιμα αρχεία του χρήστη μέχρι και να οδηγήσει σε κατάρρευση κάποιου συστήματος, καθώς η μόλυνση εξαπλώνεται οπουδήποτε έχει τη δυνατότητα. Ενώ η μετάδοση τους σε κάποιο άλλο μηχάνημα γίνεται εύκολα με τη βοήθεια κάποιας συσκευής (όπως USB) ή μέσω κάποιας εφαρμογής (όπως είναι τα e-mail).

Ένα άλλος τύπος είναι τα **Βακτήρια (Bacteria)** όπου δεν καταστρέφουν εμφανώς αρχεία, καθώς κυρίως σκοπός τους είναι να πολλαπλασιάζονται για να καταλάβουν όλους τους πόρους του συστήματος και να τους στερήσουν από τον χρήστη. Ένα βακτήριο μπορεί να αναπαράγεται και να δημιουργεί δυο αντίγραφα και αυτά με τη σειρά τους να δημιουργούν δυο νέα αντίγραφα του αρχικού βακτηρίου, και η διαδικασία αυτή να συνεχίζεται. Έτσι καταλαβαίνουμε ότι τα βακτήρια πολλαπλασιάζονται εκθετικά με αποτέλεσμα να καταλαμβάνουν τη χωρητικότητα του επεξεργαστή ή του δίσκου ή της μνήμης.

Ενώ από την άλλη πλευρά τα **Σκουλήκια (Worm)** όπου είναι και αυτά διαφορετικός τύπου κακόβουλου λογισμικού μπορεί πολλές φορές να συμπεριφέρεται σαν ιός ή σαν βακτήριο. Μεταδίδεται άμεσα με κάποια διαδικτυακή υποδομή όπως είναι τα τοπικά δίκτυα ή μέσω κάποιου μηνύματος στα ηλεκτρονικά ταχυδρομεία. Όταν μολύνει κάποια ψηφιακή μηχανή έχει τη δυνατότητα να αναπαράγεται και πολλαπλασιάζεται αυτόνομα, με τη χρήση της διαδικτυακής υποδομής. Αυτό έχει σαν αποτέλεσμα να μπορεί να στείλει το κακόβουλο λογισμικό (σκουλήκι) στο άτομο που κάνει την επίθεση προσωπικά δεδομένα, ή κωδικούς και άρα να του δίνει τη δυνατότητα πρόσβασης στο δίκτυο, καθώς και να φορτώνει το δίκτυο με άχρηστες διαδικασίες, και κατά συνέπεια να το επιβαρύνει.

Άλλος τύπος είναι το **rootkit** οπού λειτουργεί στα χαμηλά επίπεδα των λειτουργικών συστημάτων και περιέχει μηχανισμούς απόκρυψης, με σκοπό να παρακάμπτει την πρόληψη και ανίχνευση των κακόβουλων προγραμμάτων. Πέρα από την απόκρυψη τα λογισμικά αυτά χρησιμοποιούνται για να ανοίξουν "πίσω πόρτες" και να επιτρέψουν αργότερα την απομακρυσμένη διαχείριση του ψηφιακού μηχανήματος ή συστήματος από κάποιον τρίτο. Μάλιστα σε κάποιες περιπτώσεις αυτά τα προγράμματα λειτουργούν προστατευτικά προς τα άτομα που κάνουν την επίθεση διαγράφοντας πληροφορίες του εισβολέα.

Άλλοι τύποι σε αυτήν την κατηγορία είναι Bot – zombie, logic bomb, Spyware / Adware, και Trojan Horse. Στην πρώτη περίπτωση του **Bot – zombie,** ο όρος «bot» αναφέρεται σε κάθε είδους αυτοματοποιημένης διαδικασίας, ενώ ο όρος «zombie» αναφέρεται στους υπολογιστές που έχουν μολυνθεί από «bot». Έτσι το bot-zombie προσβάλλει υπολογιστές με κύριο στόχο την ένταξη τους σε ένα δίκτυο υπολογιστών για να πραγματοποιήσουν κατανεμημένες επιθέσεις άρνησης υπηρεσίας (Επίθεση DDoS). Στην ουσία οι μολυσμένοι υπολογιστές προσπαθούν να συνδεθούν στο μηχάνημα – στόχο μέσω του δικτύου για να κατάρρευση το σύστημα, λόγω του φόρτου των αιτημάτων που δέχεται. Η επιθέσεις αυτές πραγματοποιούνται από τον δράστη με την απομακρυσμένη διαχείριση των μολυσμένων υπολογιστών. Στη δεύτερη περίπτωση η **λογική βόμβα (logic bomb)** αποτελεί κομμάτια κώδικα που είναι προσκολλημένα σε κάποιο πρόγραμμα εφαρμογής, και είναι ρυθμισμένο να εκτελέσουν κάποιες ενέργειες όταν εκτελεστούν κάποιες συνθήκες. Παράδειγμα αυτών των συνθηκών μπορεί να είναι να περιμένει μια συγκεκριμένη ημερομηνία και όταν έρθει αυτή να "εκραγεί". Η έκρηξη αυτή μπορεί να περιλαμβάνει από

κάποια τροποποίηση ή διαγραφή δεδομένων μέχρι και να προκαλέσει το σταμάτημα ενός ολόκληρου συστήματος. Από την άλλη πλευρά τα λογισμικά **spyware** και **adware** εντάσσονται ως μέλη της ίδιας κατηγορίας καθώς συνήθως συνεργάζονται για να πετύχουν τον στόχο τους. Τα spyware επικεντρώνεται στην παρακολούθηση και υποκλοπή δεδομένων (όπως είναι κωδικοί πρόσβασης, αριθμοί και λεπτομερείς πιστωτικών συναλλαγών κλπ.) . Ενώ η χειρότερη κατηγορία τους είναι keylogger που υποκλέπτει κάθε χαρακτήρα που πληκτρολογεί ο χρήστης και την προωθεί σε τρίτους. Από την άλλη πλευρά τα adware είναι η αποστολή ανεπιθύμητών διαφημιστικών μηνυμάτων. Για τον λόγο αυτό τα δύο λογισμικά συνεργάζονται με σκοπό τη δημιουργία ενός προφίλ χρήστη και την αποστολή συγκεκριμένων διαφημίσεων. Οι παρενέργειες αυτών των λογισμικών μπορεί να είναι μικρές (όπως για παράδειγμα η εμφάνιση ανεπιθύμητων μηνυμάτων στην επιφάνεια εργασίας) και για αυτό ονομάζονται μερικές φορές απλά ανεπιθύμητα λογισμικά ή μεγάλες και εντάσσονται στην κατηγορία κακόβουλων λογισμικών. Τέλος, ο **Δούρειος Ίππος (Trojan Horse)** όπου η ονομασία του προέρχεται από τον Δούρειο Ίππο της ελληνικής μυθολογίας, και έχει ως στόχο την παραπλάνηση των χρηστών. Καθώς "μεταμφιέζεται" σε χρήσιμη εφαρμογή και με τη βοήθεια κακόβουλο κώδικα που περιέχει δίνει τη δυνατότητα στον δράστη να κλέψει σημαντικά αρχεία ή ακόμα να αποκτήσει τον έλεγχο του συστήματος. Για να το πετύχουν αυτό δημιουργούν μια "πίσω πόρτα" στο σύστημα, όπου ο κακόβουλος χρήστης μπορεί αργότερα να συνδεθεί και να τα εκμεταλλευτεί. Οι δούρειοι ίπποι δεν είναι λογισμικά όπου μολύνουν το σύστημα δηλαδή δεν αναπαράγονται, αλλά χρησιμοποιείται σαν μέσω μεταφοράς για μερικές από τις υπόλοιπες μορφές κακόβουλων λογισμικών.

Οι παραπάνω μορφές μπορούν πολλές φορές να συνδυαστούν, όπως για παράδειγμα ιός μαζί με δούρειο ίππο. Όμως ανεξάρτητα με το τρόπο που εκτελούνται μια επίθεση τέτοιου τύπου, οι τρόποι εξαπλώσεις τους είναι κοινοί και με την πάροδο του χρόνου αυξάνονται εφευρίσκοντας όλο και περισσότερες μεθόδους διαδώσεις, όπως για παράδειγμα συνημμένα email, ή κακόβουλες διαφημίσεις σε δημοφιλής ιστότοπους. Ενώ οι λόγοι χρήσεις μπορεί να είναι η κλοπή ταυτότητας, κλοπή οικονομικών δεδομένων, μόλυνση υπολογιστών και χρήση τους για την εξόρυξη νομισμάτων (όπως είναι τα bitcoins), ακόμα και να πάρουν τον έλεγχο πολλών υπολογιστών για την έναρξη επιθέσεις αρνήσεις υπηρεσιών (Αναλύεται παρακάτω, Επιθέσεις DoS και DDoS).

Εικόνα 2.29: "Κακόβουλα προγράμματα"
Πηγή: BizIntellia

Ενώ στο **επιχειρησιακό επίπεδο** η ευπάθεια αυτού επιτρέπει στον κακόβουλο χρήστη να κάνει κακή χρήση της εφαρμογής IoT. Ενώ τα περισσότερα προβλήματα στο επίπεδο αυτό

ξεκινάνε από πρόβλημα ή κάποια έλλειψη στους ελέγχους ασφαλείας. Συνηθισμένες επιθέσεις είναι στο επιχειρηματικό επίπεδο είναι:

- **Business Logic Attack**

Στην περίπτωση αυτή ο εισβολές μπαίνει ανάμεσα στον χρήστη και τη βάση δεδομένων, αφού μπορεί να ελέγχει και να διαχειρίζεται την ανταλλαγή πληροφοριών. Αυτό μπορεί να τα καταφέρει εκμεταλλευόμενος κάποιο ελάττωμα στο προγραμματιστικό κομμάτι.

- **Zero day**

Αυτή η επίθεση έχει να κάνει με κάποιο κενό ασφαλείας που υπάρχει στο σύστημα και τόσο ο προμηθευτής όσο και ο χρήστης δε γνωρίζουν για αυτό. Ο κακόβουλος χρήστης αφού το εντοπίσει μπορεί να το εκμεταλλευτεί και να πάρει τον έλεγχο χωρίς την άδεια του χρήστη.

2.8 Μετρά ασφαλείας

Η πολυπλοκότητα για την εξασφάλιση της ασφάλειας στο Internet of Things έγκειται στις διαφορετικές διασυνδεδεμένες συσκευές, όπου η προστασία αυτών από τις απειλές αποτελεί μια επίπονη διαδικασία. Για τον λόγο αυτών κρίνονται απαραίτητα η λήψη επιπλέων μέτρων ασφάλειας, πέρα από τη βασική ασφάλεια που έχει κάθε συσκευή και το δίκτυο για να αντιμετωπίσουμε μια επίθεση.

Αρχικά όμως σημαντικό στάδιο στην αντιμετώπιση των επιθέσεων παίζει η ανίχνευση τους, για να γίνει αυτό θα χρειαστούμε ένα σύστημα που να καταγραφεί τις διάφορες δραστηριότητες κατά τη διάρκεια της ταυτοποίησης και διαχείρισης του λογαριασμού αλλά και οποιαδήποτε περίεργης δραστηριότητας σχετικά με τους κανόνες ασφάλειας που θα έπρεπε να πληρούν. Αφού για την ανίχνευση, η παρακολούθηση για τη σωστή λειτουργία των διασυνδεμένων συσκευών του IoT και τη σωστή συμπεριφοράς τους είναι ένας τρόπος, διότι κάθε περίεργη δραστηριότητα θα μπορούσε να αποτελεί μια παραβίαση των συσκευών και αρά μια πιθανή επίθεση που έχει γίνει στο IoT. Έτσι η χρήση συστήματος ανίχνευσης εισβολής (Intrusion Detection System - IDS) είναι απαραίτητη, καθώς οποιαδήποτε απειλή θα αναφερθεί σε κάποιον ατόμου που διαχειρίζεται τέτοιες καταστάσεις ή σε κάποιο σύστημα για την αποτελεσματική διαχείριση των κυβερνοεπιθέσεων.

Ωστόσο, για την αντιμετώπιση των διάφορων κυβερνοεπιθέσεων που μπορούν να συμβούν, μηχανισμοί όπως η αυτοδιάγνωση και η αυτοδιόρθωση είναι απαραίτητη για τη σωστή λειτουργία ενός συστήματος σε περίπτωση εισβολής. Αυτό θα μπορούσε να το επιτύχει με την επαναφορά ασφαλής κατάστασης, έχοντας δηλαδή ορίσει σε ποια κατάσταση ένα σύστημα θεωρείται ασφαλές και έτσι οποιαδήποτε απόκλιση από αυτό (είτε λόγο δυσλειτουργίας του συστήματος, είτε λόγω επίθεσης στο σύστημα) να επανέρχεται στην κατάσταση όπου ορίσαμε ως ασφαλή.

Ενώ σε μερικά από αυτά τα περιστατικά κυβερνοεπιθέσεων, μπορεί να προκληθεί διακοπή λειτουργίας, και έτσι να επιτραπεί σε κακόβουλους χρήστες την υποκλοπή δεδομένο. Σε τέτοιες περίπτωσης μηχανισμοί διαχείρισης της εμπιστευτικότητας των δεδομένων και της ακεραιότητας τους είναι απαραίτητοι, όπως επίσης και η εξασφάλιση ότι το σύστημα θα συνεχίσει να λειτουργεί. Έτσι ανεξάρτητα από το είδος της επίθεσης η ικανότητα της αυτόνομης λειτουργίας βασικών χαρακτηριστικών θα πρέπει να εξασφαλίζεται από τις συσκευές IoT, για την εξασφάλιση της ασφάλειας και της αξιοπιστίας του συστήματος. Αυτό θα μπορούσε να το επιτύχει με την απώλεια της επικοινωνίας της συσκευής όπου έχει παραβιαστεί, και τη συνέχεια των βασικών λειτουργιών από τις υπόλοιπες διασυνδεδεμένες συσκευές. Με τον τρόπο αυτό καταφέρνουμε να συνεχιστεί η λειτουργία ενός συστήματος όπως είναι το IoT, και να αντιμετωπίσουμε τυχόν επιθέσεις

που μπορούν να γίνουν στα δεδομένα και κατά συνέπεια στην εμπιστευτικότητα και ακεραιότητα αυτών.

Από την άλλη πλευρά για την αποφυγή των κυβερνοεπιθέσεων κρίνεται απαραίτητη η ύπαρξη μηχανισμού για εύρεση τυχόν τρωτών σημείων από εξωτερικά άτομα, όπως είναι ένας δημόσιος μηχανισμός για την αναφορά των διαφορών ευπαθειών που υπάρχει σε κάποιο σύστημα. Παρέχοντας έτσι επιπλέον πληροφορίες για τυχόν ευάλωτα σημεία τα οποία μπορεί να μην έβρισκε η ομάδα ασφαλείας, και θα μπορούσαν να αποτελούν μια πιθανή δίοδο για κάποιον κακόβουλο χρήστη. Επιπλέον, η ένταξη σε κοινωνικές ηλεκτρονικές ομάδες με σκοπό την ανταλλαγή χρήσιμων πληροφοριών σχετικά με επίκαιρες απειλές που υπάρχουνε στον κυβερνοχώρο αλλά και τρόποι αντιμετώπισης, είναι απαραίτητο για την αποφυγή των κυβερνοεπιθέσεων. Αφού η γνώση που λαμβάνεται μέσα από την ανταλλαγή των πληροφοριών θα μπορούσε να βοηθήσει τόσο στην πρόληψη των κυβερνοεπιθέσεων με τον εντοπισμό των διαφορών τρωτών σημείων, όσο και στην αντιμετώπιση των τυχόν κυβερνοεπιθέσεων που μπορούν να συμβούν.

Πέρα όμως από την ανταλλαγή γνώσεων η αποφύγει συμβάντων θα μπορούσε να επιτύχει με σύστημα πρόληψης εισβολής (Intrusion Prevention System - IPS) που μοιάζει με το σύστημα ανίχνευσης με τη διαφορά ότι εδώ έχουμε την ικανότητα να πάρει αυτόματα μετρά και να αποκλείσει μια διεύθυνση IP, αν αυτή φαίνεται ύποπτη.

Τέλος, άλλο σημαντικό μετρό για την ασφάλεια του IoT αποτελεί η υποδομή δημοσίου κλειδιού (Public Key Infrastructure - PKI), καθώς η κρυπτογράφηση δε θα μπορούσε να λείπει από την ασφάλεια των συσκευών IoT. Η μέθοδος αυτή, αποτελεί μια καλή λύση για την προστασία των δεδομένων, χρησιμοποιείται πιστοποιητικό γνησιότητας το οποίο αποτελείται από ένα δημόσιο κλειδί (για την αποστολή μηνυμάτων) και ένα ιδιωτικό κλειδί (για την ανάγνωση μηνυμάτων). Η ασφάλεια των συσκευών IoT επιτυγχάνεται στο γεγονός ότι ο κακόβουλος χρήστης δεν μπορεί να πάρει πρόσβαση σε κάποιο από τα ιδιωτικά κλειδιά αλλά ούτε να πλαστογραφήσει τα δημόσια για να μπορέσει να υποκλέψει τις διάφορες πληροφορίες.

ΚΕΦΑΛΑΙΟ 3 Συμπεράσματα

Από την εργασία προκύπτει το συμπέρασμα ότι κάθε τεχνολογία εγκυμονεί κίνδυνους ασφαλείας όταν αυτές συνδέονται με το διαδίκτυο. Πιο συγκεκριμένα το edge computing και το internet of things έχουν να αντιμετωπίσουν αρκετές προκλήσεις και απειλές στον κυβερνοχώρο. Καθώς και οι δυο είναι τεχνολογίες πληροφορίας και σε πολλές περιπτώσεις κρίσιμα δεδομένα μπορούν κλαπούν, τροποποιηθούν ή διαγράφουν, και τα αποτελέσματα αυτών το πράξεων θα μπορούσε να ήταν από αμελητέα μέχρι και ζωτικού χαρακτήρα.

Πέρα από τα παραπάνω όμως, σε αυτήν την εργασία είδαμε ότι το edge computing φέρνει την επεξεργασία και αποθήκευση των δεδομένων πιο κοντά στην πηγή που παράχθηκαν. Έτσι ο βασικός λόγο κινδύνου ασφαλείας προκύπτει από το γεγονός ότι ο έλεγχος είναι δύσκολος να γίνει σε όλα αυτά τα μικρό κέντρα δεδομένων που βρίσκονται στην άκρη. Αλλά το παράδοξο με αυτό είναι, ότι χάρης στο ότι υπάρχουν πολλά κέντρα δεδομένων στην άκρη του δικτύου, η υπολογιστική αιχμή κάνει το δίκτυο λίγο πιο ασφαλές. Αυτό το συμπεραίνουμε από το γεγονός ότι αφού τα δεδομένα επεξεργάζονται και αποθηκεύονται κοντά στην πηγή, δε διανύουν τεράστιες αποστάσεις για να φτάσουν σε κάποιο κέντρο δεδομένων, έτσι οι πιθανότητες για επίθεση κατά τη μεταφορά των δεδομένων μειώνονται. Παράλληλα χάρης το γεγονός ότι η παραμονή πολλών πληροφοριών είναι σε μικρά κέντρα δεδομένων στην άκρη του δικτύου, μειώνει σημαντικά την απειλή επίθεσης σε κάποιο κεντρικό κέντρο δεδομένων που βρίσκεται πέρα από την άκρη του δικτύου.

Από την άλλη πλευρά στο Internet of Things ο κίνδυνος ασφάλειας υπόκειται στο γεγονός της εξασφάλισης της ασφάλειας όλων των διασυνδεδεμένων συσκευών που το απαρτίζουν. Αυτό μπορούμε να το καταλάβουμε καλύτερα αν σκεφτούμε πόσοι διαφορετικοί τύποι συσκευών IoT συνδέονται μεταξύ τους και μπορούν να έχουν διαφορετικά χαρακτηρίστηκα, όπως είναι τα διαφορετικά λειτουργικά συστήματα κλπ.

Για αυτό η τήρηση βασικών μέτρων, όπως είναι για παράδειγμα η σωστή διαχείριση των δεδομένων με έλεγχο των αδειών που δίνουμε, είναι απαραίτητα για τη μεγαλύτερη προστασία και την όσο γίνεται καλύτερη πρόληψη των επιθέσεων αυτών, τόσο στην υπολογιστική αιχμή όσο και στο διαδίκτυο των πραγμάτων. Επιπλέον, είναι αναγκαίο να περνούμε τόσο μετρά πρόληψης των κυβερνοεπιθέσεων, όσο και τεχνικές ανίχνευσης και αντιμετώπισης αυτών των απειλών. Τα μετρά ασφαλείας αυτά, που υπάρχουν και μπορούμε να χρησιμοποιούμε ποικίλουν και πολλές φορές εξαρτώνται από τον τύπο των κυβερνοεπιθέσεων όπου δέχονται η υπολογιστική αιχμή και το διαδίκτυο των πραγμάτων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Abdallah M., Al-Thelaya A. K., Alwarafy A., Hamdi M., & Schneider J. (2020, Αύγουστος, 10). A survey on security and privacy issues in edge computing-assisted internet of things. IEEE Xplore, vol 8 , pp 4004 -4022. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things | IEEE Journals & Magazine | IEEE Xplore

Attack ("*Adversary in the middle: ARP cache poisoning*", 2020, Οκτώβριος, 15). Mitre Att&ck, vol 1.1. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Adversary-in-the-Middle: ARP Cache Poisoning, Sub-technique T1557.002 - Enterprise | MITRE ATT&CK®

Adomhara M. & Koien G. M. (2015, Ιανουάριος). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. River Publishers, vol 4, pp 65-88. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks (riverpublishers.com)

Application IoT ("*Application of IoT in automotive industry | Future of automobiles*", n.d.). BizIntellia. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Application Of IoT In Automotive Industry | Future Of Automobiles (biz4intellia.com)

Baird A., Dole M., Georgiou Y., Glesser D., Humblot N., Larue T., Lisle A., Marshall C., Mercier M., Nasica L., Razafinjatovo A., Sakka Amini K., Silva A. A., Troudi S., Vacher J., Velho P. & Vieillard R. (2020, Οκτώβριος, 15). Edge computing and data security. Ryax technologies. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: Edge computing and data security - Ryax Technologies

Baseline security ("*Baseline security IoT*", 2017). Enisa, pp 9. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: ENISA Good practices for IoT and Smart Infrastructures Tool — ENISA (europa.eu)

Bigelow J. S. (2021, Δεκέμβριος). What is edge computing? Everything you need to know. TechTarget. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: What Is Edge Computing? Everything You Need to Know (techtarget.com)

Bluetooth ("*Bluetooth*", χ.χ.). ΒΙΚΙΠΑΙΔΕΙΑ. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Bluetooth - Βικιπαίδεια (wikipedia.org)

Boeckl K., Fagan M., Fisher W., Lefkovitz N. Megas K. N., Nadeau E., O'Rourke D. G., Piccarreta B. & Scarfone K. (2019, Ιουνίος). Considerations for managing internet of things (IoT) cybersecurity and privacy risks. NIST, pp 44.

Ανακτήθηκε τελευταία φορά στις 26/6/22, από: https://doi.org/10.6028/NIST.IR.8228

Brooks C. (2021, Φεβρουάριος, 7). Cybersecurity threads: The daunting challenge of securing the internet of things. Forbes. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Cybersecurity Threats: The Daunting Challenge Of Securing The Internet Of Things (forbes.com)

Burhan M., Rehman R. A., Khan B. & Kim Byung-Seo (2018). IoT elements, layered architectures and security issues: A comprehensive survey. PubMed Central. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey - PMC (nih.gov)

Characteristics IoT ("*Characteristics of Internet of Things*", 2022, Απριλίου,12). GeeksforGeeks. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Characteristics of Internet of Things - GeeksforGeeks

Chen B., Cheng X., Hu F., Zhang J. & Zhao Y. (2018, Μάρτιος, 28). Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. IEEE Xplore, Vol 6, pp 18209 - 18237. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues | IEEE Journals & Magazine | IEEE Xplore

Cross site scripting attack ("*Cross Site Scripting*", χ.χ.) Βικιπαίδεια. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Cross-site scripting - Βικιπαίδεια (wikipedia.org)

Cross site scripting attack ("*Cross Site Scripting*", χ.χ.). Enisa. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Cross-site scripting (XSS) — ENISA (europa.eu)

Cross site scripting ("*Τι είναι το Cross Site Scripting*", χ.χ.). Quantum. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Επιθέσεις Cross Site Scripting (XSS) | Quantum Software Applications (qsa.gr)

Cyber Security ("*Τι είναι "Cyber Security" – Υπηρεσίες για την Κυβερνοασφάλεια", χ.χ.*). TICTAC. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Cyber Security τι είναι η Κυβερνοασφάλεια; Μιχάλης Μίγγος (tictac.gr)

Daniel B. (2020, Δεκέμβριος, 9). Is edge computing secure? Here are 4 security risks to be aware of. Trenton systems. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: Is Edge Computing Secure? Here Are 4 Security Risks to Be Aware Of (trentonsystems.com)

DDoS ("*DDoS attacks*", χ.χ.). imperna. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: DDoS Attack Types & Mitigation Methods | Imperva

DNS spoofing ("*What is DNS cache poisoning*", χ.χ.). Cloudflare. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: What is DNS cache poisoning? | DNS spoofing | Cloudflare

Drimili K. (2014, Ιανουάριος, 20). MAC - Διευθύνσεις IP. Slideshare. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: MAC - IP διευθύνσεις (slideshare.net)

Dustdar S. & Shi W. (2016, Μάιος, 13). The promise of edge computing. IEEE Xplore, Vol 49, pp 78-81. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: The Promise of Edge Computing | IEEE Journals & Magazine | IEEE Xplore

Edge computing ("*Edge computing*", 2022, Φεβρουάριος, 15). Devopedia, Vol 9. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: Edge Computing (devopedia.org)

Edge computing -Wikipedia ("*Edge computing*", χ.χ.). Wikipedia. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: Edge computing - Wikipedia

Edge computing ("*What is edge security?*", χ.χ.). Forcepoint. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: Edge Security, Edge Computing & Edge IoT Security | Forcepoint

Fog computing ("*What is fog computing*?", χ.χ.). Stackpath. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: What is Fog Computing? (stackpath.com)

Gillis A. S. (2020, Μάρτιος). What is internet of things. IoTAgenda. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: What is IoT (Internet of Things) and How Does it Work? - Definition from TechTarget.com

Hardware trojan ("*Hardware trojan*", 2021, Μάιος, 7). GeeksforGeeks. Ανακτήθηκε τελευταία φορά στις 20/6/22, από : Hardware Trojan - GeeksforGeeks

Harvey C. (2021, Νοέμβριος, 23). What is edge computing? Why it's important and how it works. EBSCOhost. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: https://web.p.ebscohost.com/ehost/detail/detail?vid=5&sid=e2e09dbc-b3d9-4eac-9d44-51bf84fb1742%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=153738837&db=asn

History ("*The History of the Internet of Things*", 2019, Ιουνιος, 27). Perenio. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: The History of the Internet of Things (perenio.com)

IoT ("*What is IoT*", χ.χ.). Oracle. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: What Is the Internet of Things (IoT)? (oracle.com)

Khvoynitskaya S. (2019, Νοέμβριος, 25). The IoT history and future. itransition. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: The IoT history and future - Itransition

Kisten S. (χ.χ.). Cross Site Scripting (XSS). Owasp. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Cross Site Scripting (XSS) Software Attack | OWASP Foundation

Kulkarni Sanjeev & Kulkarni Santosh (2017, Μάιος). Communication model in internet of things. Ijste, vol 3, pp 91. Ανακτήθηκε τελευταία φορά στις 16/6/22, από: Communication Models in Internet of Things: A Survey (ijste.org)

Lakhani A. (2021). Examining top IoT security threads and attacks vectors. Fortinet. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Examining Top IoT Security Threats and Attack Vectors | Fortinet

Man in the middle ("*Man-in-the-Middle*", χ.χ.). Enisa. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Man-in-the-Middle — ENISA (europa.eu)

Melnick J. (2018, Μάιος, 15). Top 10 most common types of cyber attacks. Netweix Blog. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Top 10 Most Common Types of Cyber Attacks (netwrix.com)

Pathak A. (2021, Οκτώβριος, 26). What is edge computing and what are its applications. GEEKFLARE. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: What Is Edge Computing and What Are Its Applications? - Geekflare

Pedamkar P. (χ.χ.). IoT features. EDUCBA. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: IoT Features | 9 Fundamental Characteristics of Internet of Things (educba.com)

Petters J. (2020, Αύγουστος, 10). What is a man-in-the-middle attack: Detection and prevention tips. Varonis. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: What is a Man-in-the-Middle Attack: Detection and Prevention Tips (varonis.com)

Ping of Death ("*Ping of Death*", χ.χ.). Βικιπαίδεια. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Ping Of Death - Βικιπαίδεια (wikipedia.org)

Ping of death attack ("*Ping of Death DDoS attack*", χ.χ.). Cloudflare. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Ping of death DDoS attack | Cloudflare

Ranger S. (2022, Φεβρουάριος, 25). What is cloud computing? Everything you need to know about the cloud explained. ZDNet. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: What is cloud computing? Everything you need to know about the cloud explained | ZDNet /

Rauch S. (2021, Ιούνιος, 2). Edge computing security risk and challenges in 2021, Simplilearn. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: Edge Computing Security Risk And Challenges in 2021 (simplilearn.com)

RFID ("*What is RFID and how does RFID works* ?", χ.χ.). AB&R. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: What is RFID and How Does RFID Work? - AB&R® (abr.com)

Romero B. (χ.χ.). IoT and everyday. FOLDER IT. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: IoT and everyday life (folderit.net)

Satyabrata J. (2020, Ιούνιος, 25). Architecture of internet of things. GeeksforGeeks. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/

Shamkuwar M., Sharma N. & Singh I. (2019, Δεκέμβριος, 31). The history, present and future with IoT. Springer Link, vol 154, pp 27-51. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: https://doi.org/10.1007/978-3-030-04203-5_3

Sreejith (2020, Ιούνιος, 25). What is fog computing and how does it work. Fingent. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: What Is Fog Computing and How Does It Work? - Fingent Technology

Syn flood – βικιπαιδεια ("*SYN flood*", χ.χ.). Βικιπαίδεια. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: SYN flood - Βικιπαίδεια (wikipedia.org)

Tweneboah-Koduah S., Knud Eric Skouby & Tadayoni R. (2017). Cyber Security Threats to IoT Applications and Service Domains. Springer Link. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: https://doi.org/10.1007/s11277-017-4434-6

Types XSS ("*Types of XSS: Stores XSS, Reflected XSS and DOM-based XSS*", χ.χ). Acunetix. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Types of XSS (Cross-site Scripting) (acunetix.com)

Walkowski D. (2019, Ιούνιος, 5). What is a distributed denial-of-service attacks. F5 labs application threat intelligence. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: What Is a Distributed Denial of Service (DDoS) Attack? (f5.com)

Wichers D., Dabirsiaghi A., Paolo S. D., Heiderich M. Wiliams J., & Eduardo Alberto Vela Nava (χ.χ.). Types of XSS. Owasp. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Types of XSS | OWASP Foundation

ZigBee ("*Τι είναι η τεχνολογία Zigbee γιατί είναι σημαντικό για ένα έξυπνο σπίτι και ποια προϊόντα της Xiaomi την υποστηρίζουν;*", 2020, Νοέμβριος, 22). XIAMIPLANET. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Τι είναι η τεχνολογία Zigbee και γιατί είναι σημαντικό για ένα έξυπνο σπίτι; (xiaomiplanet.sk)

Z-Wave ("*Τι είναι το Z-Wave και είναι συμβατό με το έξυπνο σπίτι;*", χ.χ.). Tips and TriCs. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Τι είναι το Z-Wave και είναι συμβατό με το έξυπνο σπίτι σας; (tipsandtrics.com)

Αγγουριδάκη Ε., Αντωνιουδάκη Μ., Βιολάκη Γ., Γκίνη Ε., Κάββαλου Κ. & Κατζαγιαννακη Ε. (χ.χ.). Το κακόβουλο λογισμικό και τα είδη του. Sch. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: ΤΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΚΑΙ ΤΑ ΕΙΔΗ ΤΟΥ (sch.gr)

Αμπατζόγλου Ι. (χ.χ.). Πρωτόκολλα ARP &DHCP. Sch. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Πρωτόκολλα ARP & DHCP | Δίκτυα Υπολογιστών (sch.gr)

Βασικότερα κακόβουλα λογισμικά ("Ποια είναι τα βασικότερα κακόβουλα λογισμικά ", χ.χ.). Wind. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Ποια είναι τα βασικότερα κακόβουλα λογισμικά; | WIND

Βεράτης Χ. (2015, Νοέμβριος, 26). Κυβερνοχώρος-Κυβερνοεπιθέσεις-Κυβερνοάμυνα-Μέρος 1ο. ΚΕΔΙΣΑ KEDISA. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: ΚΥΒΕΡΝΟΧΩΡΟΣ-ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ- ΚΥΒΕΡΝΟΑΜΥΝΑ (kedisa.gr)

Γεωργιάδης Χ. Κ. (2015, Οκτώβριος). Ασφαλής συναλλαγές στον παγκόσμιο ιστό. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: repfiles.kallipos.gr/html_books/9536/Chapter 3/Chapter03.html

Διεύθυνση IP ("Διεύθυνση IP", χ.χ.). Google. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Διεύθυνση IP - Βοήθεια Google Ads

Επιθέσεις ("*Επιθέσεις άρνησης υπηρεσιών*", n.d). Βικιπαίδεια. Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Επιθέσεις άρνησης υπηρεσιών - Βικιπαίδεια (wikipedia.org)

Ευρωπαϊκή Ένωση (2019, Μάρτιος). Προκλήσεις για μια αποτελεσματική πολιτική για την κυβερνοασφάλεια. Europa.eu . Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Challenges to effective EU cybersecurity policy (europa.eu)

Ευρωπαϊκό Συμβούλιο - Συμβούλιο της Ευρωπαϊκής Ένωσης (χ.χ.). *Κυβερνοασφάλεια: Πως αντιμετωπίζει η ΕΕ τις κυβερνοαπειλές*. Europa.eu . Ανακτήθηκε τελευταία φορά στις 18/6/22, από: Κυβερνοασφάλεια: Πώς αντιμετωπίζει η ΕΕ τις κυβερνοαπειλές - Consilium (europa.eu)

Ιστορία (1997, Δεκέμβριος). Ιστορία του Internet. Uth. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Η Ιστορία του Internet (uth.gr)

Κακόβουλα λογισμικά("Κακόβουλα λογισμικά", χ.χ.). Βικιπαίδεια. . Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Κακόβουλο λογισμικό - Βικιπαίδεια (wikipedia.org)

Κακόβουλα λογισμικά("*Τι είναι κακόβουλα λογισμικά*", χ.χ.). McAfee. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: Τι είναι το κακόβουλο λογισμικό; | McAfee

Κοινωνία της πληροφορίας (“*Κοινωνία της πληροφορίας*”, χ.χ.). Βικιπαίδεια. Ανακτήθηκε τελευταία φορά στις 20/6/22, από: Κοινωνία της πληροφορίας - Βικιπαίδεια (wikipedia.org)

Κρουκσάνκ Α. (2019, Ιανουάριος, 25). Ασφάλεια στον κυβερνοχώρο. PlaceTech. Ανακτήθηκε τελευταία φορά στις 26/6/22, από: PlaceTech | Αστυνομικός αστυνομικός: ασφάλεια στον κυβερνοχώρο