ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών

&

Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη τεχνικών ασφάλειας φυσικού επιπέδου για εφαρμογές 5G-IoT και υλοποίηση σεναρίων επίθεσης με τη χρήση μηχανικής μάθησης

Δήμος Δ. Γλετζάκος
Α.Μ. 19011

Εισηγητής: Δρ. Αντώνιος Μπόγρης, Καθηγητής

(Κενό φύλλο)

Πανεπιστήμιο Δυτικής Αττικής – University of West Attica

Σχολή: Μηχανικών
Τμήμα: Μηχανικών Πληροφορικής και Υπολογιστών
ΠΜΣ: Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών
Ειδίκευση: Δικτύων και Κατανεμημένων Συστημάτων

Διπλωματική εργασία από το σπουδαστή:

Γλετζάκο Δήμο (mcse19011)

Τίτλος:

Μελέτη τεχνικών ασφαλείας φυσικού επιπέδου για εφαρμογές 5G-IoT και υλοποίηση σεναρίων επίθεσης με τη χρήση μηχανικής μάθησης.

Study of techniques for safety of physical level for applications 5G-IoT and implementation of scenario of attack with the use of mechanical studying.

Εισηγητής:
Δρ. Αντώνιος Μπόγρης, Καθηγητής

Εξεταστική Επιτροπή:

Μπόγρης Αντώνιος
Καντζάβελου Ιωάννα
Ψαρράς Νικόλαος

Antonios Bogris
Digitally signed by Antonios Bogris
Date: 2021.03.09 17:39:13 +02'00'

Ημερομηνία εξέτασης: 03/03/2021

Αιγάλεω, Μάρτιος 2021

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Γλετζάκος Δήμος, του Δημητρίου, με αριθμό μητρώου mcse19011 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών « Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών » του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών, της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία.

Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολο τους με πλήρη αναφορά στους συγγράφεις, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.

Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από εμένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δίκης μου, όσο και του Ιδρύματος. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για ανάκληση του πτυχίου μου.»

Δεν επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου.

Ο Δηλών

Γλετζάκος Δήμος

Ημερομηνία

03-03-2021

(Κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Πρώτα από όλα πρέπει να ευχαριστήσω θερμά τον επιβλέποντα Καθηγητή και υπεύθυνο για το Πρόγραμμα Μεταπτυχιακών Σπουδών που ολοκληρώνετε μετά το πέρας της διπλωματικής αυτής κ. Μπόγρη Αντώνιο, για την πολύ σημαντική βοήθεια και καθοδήγηση στην ολοκλήρωση της παρούσας διπλωματικής αλλά και για την συνολική αδιάληπτη παρουσία του.

Δεν είναι υπερβολή, να τονίσω, ότι ανταποκρίθηκε άμεσα σε όλες τις απορίες μου και μου υπέδειξε με υπομονή και λεπτομέρεια ότι του ζήτησα. Μάλιστα, δεν ήταν λίγες οι φορές που του ζήτησα με email, με βίντεο διάλεξη ακόμα και τηλεφωνικώς να μου διευκρινίσει κάτι. Να με βεβαιώσει για την ορθότητα μιας σκέψεως μου και να μου υποδείξει όποια επιλογή αυτός θεωρούσε καλύτερη από αυτές που του πρότεινα.

Αλλά και αυτή καθ' εαυτή η ανάθεση αυτής της συγκεκριμένης διπλωματικής εργασίας που ήταν μία από τις ωραιότερες που θα μπορούσαν να μου ανατεθούν, με βοήθησε σημαντικά και μου πρόσθεσε αρκετές γνώσεις σε θέματα που μου αρέσουν και που ήθελα να εξειδικευτώ.

Πιστεύω δε, ότι η ωφέλεια αυτής της εργασίας για μένα θα είναι ακόμη μεγαλύτερη στο μέλλον. Έτσι νομίζω ότι οφείλω να εκφράσω, πολλές και θερμές και μέσα από την καρδιά μου ευχαριστίες, στον Καθηγητή μου, γι' αυτήν την προσφορά του.

Εκτός από την οφειλόμενη ευχαριστία προς τον Καθηγητή μου, θα ήθελα να ομολογήσω ότι και η συμπαράσταση της οικογένειάς μου ήταν σημαντική. Μπορεί να μην με βοήθησαν όλοι στην εργασία μου αυτή, αλλά η πολύπλευρη συμμετοχή τους σε ηθική συμπαράσταση, κόστος και κόπο υπήρξε ουσιαστική.

(Κενό φύλλο)

Περίληψη:

Στόχος της εργασίας είναι να μελετήσει τις τεχνικές ασφαλείας φυσικού επιπέδου που εμφανίζονται στη βιβλιογραφία για εφαρμογές 5G-IoT και η υλοποίηση σεναρίων επίθεσης με τη χρήση μηχανικής μάθησης. Στο πρώτο κεφάλαιο της διπλωματικής γίνεται εισαγωγή στον κόσμο της ασφάλειας με ιδιαίτερη έμφαση να αποδίδεται στην ανασκόπηση των θεμελιωδών ιδιοτήτων της πληροφορίας. Στο κεφάλαιο 2 παρουσιάζεται ο κόσμος του IoT. Ο ορισμός, η ιστορική αναδρομή, τα χαρακτηριστικά, οι προκλήσεις ασφαλείας αλλά και τα μοντέλα πιθανών επιθέσεων παρουσιάζονται στο κεφάλαιο αυτό. Στο επόμενο κεφάλαιο, τρίτο κατά σειρά συναντάμε το 5G. Γίνεται μια αναδρομή βήμα - βήμα για την εξέλιξη του κατά μήκος στον χρόνο όπως επίσης παρατίθενται όλα τα απαραίτητα σχετικά στοιχεία ώστε να διαμορφώσει ο αναγνώστης μια πλήρη εικόνα για το δίκτυο αυτό. Ακολουθεί η μηχανική μάθηση που αποτελεί τον πυρήνα της διπλωματικής εργασίας με μια πλήρη ανάλυση να υλοποιείται. Το κεφάλαιο 5ο είναι η πεμπτουσία της διπλωματικής καθώς παρατίθεται η σύνδεση της μηχανικής μάθησης με το IoT-5G. Όλες εκείνες οι λύσεις που μπορούν να μας δώσει η ML σε πιθανές επιθέσεις αλλά και το πως μπορούμε να διασφαλίσουμε τους τρεις πυλώνες της πληροφορίας υπάρχουν στο κεφάλαιο αυτό. Η χρήση παραδειγμάτων που δίνονται μας ισχυροποιούν και μας αποδεικνύουν το πόσο σημαντική εξέλιξη μπορεί να αποτελέσει η εισαγωγή της στο IoT-5G. Το κεφάλαιο 6 ασχολείται με τους περιορισμούς και τις μελλοντικές προκλήσεις, ενώ στο κεφάλαιο 7 υπάρχει η συζήτηση της διπλωματικής ώστε να εξάγουμε τα τελικά μας συμπεράσματα.

Ο Επιβλέπων

Αντώνιος Μπόγρης
Καθηγητής Πανεπιστήμιο Δυτικής Αττικής

Abstract:

The goal of this project is to study the techniques that appear in the bibliography for 5G-Iot applications and the implementation of attack scenarios with the use of machine learning. The first chapter introduces you to the world of security with great emphasis on the review of the fundamental properties of information. The second chapter presents the world of the IoT. It presents the definition, the historical background, the characteristics of it and some of the models of possible attacks too. In the third chapter we meet 5G. We see a step by step review of its evolution over time as well as all the data so that the reader can form a complete picture of this network. Then it introduces you to machine learning which is the center of the diplomatic project with an extended analysis. The fifth chapter is the quintessence of diplomacy as it lists the connection of machine learning to the IoT-5G. This chapter concludes all the solutions that ML can give us in possible attacks and how we can secure the three pillars of information. The use of the examples that are given strengthens us and proves us how important a development can be with the introduction of machine learning into the IoT-5G.The sixth chapter deals with the limitations and possible future challenges, while in the seventh chapter we have the discussion of diplomacy in order to be able to come out with a well rounded correct conclusion.

Supervisor

Antonios Bogris
Professor of University West of Attica

Περιεχόμενα

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Μηχανική Μάθηση, IoT, 5G

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Μηχανική Μάθηση (ML), Internet Of Things (IoT), Φυσικό Επίπεδο (Physical Layer), Σενάρια επίθεσης, Είδη μηχανικής μάθησης, Ασφάλεια πληροφορίας, Δίκτυα 5G.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

1G: First Generation

2G: Third Generation

3G: Third Generation

4G: Fourth Generation

5G: Fifth Generation

AMQP: Advanced Message Queuing Protocol

ARM: Advanced RISC Machines

BLE: Bluetooth Low Energy

CoAP: Constrained Application Protocol

ELM: Extreme Learning Machine

EPC: Electronic Product Code

ESFCM: Edge Based Semi Fuzzy C Means Clustering Method

FCM: Fuzzy C-Means

GSM: Global System for Mobile Communications

HTTP: Hypertext Transfer Protocol

IEEE: Institute of Electrical & Electronics Communications

IoBT: Internet of Battlefield Things

IoT: Internet of Things

IP: Internet Protocol

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

LAN: Local Area Network

LTE: Long Term Evolution

M2M: Machine to Machine

MQTT: Message Queuing Telemetry Transport

OSI: Open Systems Interconnection

POS: Point of Sale terminal

QoS: Quality of Service

RBF: Radial Basis Function

RPL: Routing Protocol for Low-Power and Lossy Networks

RFID: Radio Frequency Identification

SDN: Software Defined Networking

SINR: Signal to Interference Plus Noise Ratio

SOA: Service Oriented Architecture

SVM: Support Vector Machine

TCP: Transfer Control Protocol

XMPP: Extensible Messaging & Presence Protocol

Σημείωση: Στο παραδοτέο οι συντομογραφίες που χρησιμοποιήθηκαν παρουσιάζονται με αλφαβητική σειρά.

ΕΥΡΕΤΗΡΙΟ ΕΙΚΟΝΩΝ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

ΚΕΦΑΛΑΙΟ 1 – Εισαγωγή & Ασφάλεια Πληροφορίας

1.1 Πρόλογος

Μέρος της καθημερινότητας μας αποτελεί πλέον αναμφίβολά το διαδίκτυο. Ο τρόπος χρήσης του ποικίλει από άνθρωπο σε άνθρωπο και από μια γεωγραφική περιοχή σε μια άλλη, ένα όμως είναι το σίγουρο ότι υπάρχουν ολοένα αυξανόμενες απαιτήσεις για βελτίωση των δυνατοτήτων και της απόδοσης του. Σε γενικές γραμμές οι τεχνολογίες της πληροφορίας έχουν γίνει ανυπόστατο κομμάτι της ιδίας της κοινωνίας μας. Στα παλαιοτέρα χρόνια θα μπορούσαμε να ισχυριστούμε ότι η κουλτούρα μας και η νοοτροπία μας είχε διαμορφωθεί μέσω των ερεθισμάτων όπως η οικογένεια, το σχολείο κ.λ.π.

Πλέον μετά βεβαιότητας μπορούμε να αναφέρουμε ότι οι τεχνολογίες αυτές έχουν επιρροή πάνω μας και γενικότερα έχουν βαθιές κοινωνικοοικονομικές επιπτώσεις παρέχοντας μας πληθώρα επιλογών στην παιδεία, την υγεία, τη ψυχαγωγία και σε πολλούς ακόμα τομείς της ζωής μας (Σταματόπουλος 2020). Στην συνέχεια θα εντοπίσουμε και θα μελετηθεί το πως φτάσαμε στο 5G, τι πλεονεκτήματα αποκτάμε τι προβλήματα αντιμετωπίζουμε αλλά και το πως πραγματοποιήθηκε αυτή η εξέλιξη από γενιά σε γενιά.

Όμως, σε αυτό το σημείο οφείλω να προσθέσω ότι έχουμε ξεπεράσει την συμβατική έννοια του διαδικτύου και αυτό γιατί υπάρχει η τεράστια ανάγκη του ανθρώπου για την άμεση διάθεση των δεδομένων και των πληροφοριών της καθημερινότητας με σκοπό την επεξεργασία τους ώστε να φτάσει κάποια στιγμή στην βελτίωση της ποιότητας ζωής του. Εννοείται φυσικά, ότι αυτή η διαδικασία της ανάλυσης και πιθανώς τροποποίησης και χρήσης των δεδομένων γίνεται σε πραγματικό χρόνο. Κάπως έτσι διαπιστώνουμε ότι έχουμε εισαχθεί στον κόσμο των αντικειμένων και των πράγματων γνωστό και ως Internet of Things. Τα οφέλη που αποκομίζουμε από την χρήση του IoT είναι αμέτρητα, υπάρχει διαφοροποίηση στον τρόπο εργασίας μας, στον τρόπο της άθληση μας, στον τρόπο που διασκεδάζουμε και γενικότερα στον τρόπο που ζούμε.

Το μεγαλύτερο ποσοστό των σύγχρονων εταιριών έχουν άμεση εξάρτηση από την πληροφοριακή τους υποδομή καθώς επίσης και τους πόρους των πληροφοριακών συστημάτων τα οποία έχουν στη διάθεσή τους, όχι μονάχα με απώτερο στόχο να λειτουργήσουν σωστά, αλλά και με στόχο να εξελιχτούν και να καταφέρουν εν τέλει να διευρύνουν ακόμα περισσότερο τις δράσεις τους.

Το θέμα της ασφάλειας όλων αυτών των συστημάτων, τόσο εξαιτίας της σημασίας του, όσο και λόγω του ότι αποτελεί ένα εξαιρετικά πολύπλοκο ζήτημα, χρειάζεται μια συστηματική αλλά και ολοκληρωμένη αντιμετώπιση. Η χρησιμότητα κατά περίπτωση τεχνολογικών μέτρων ασφαλείας, ακόμα και στις περιπτώσεις όπου εκείνες είναι οι βέλτιστες εφικτές, δεν φτάνει, καθώς σημαντικά αγαθά αυτών των συστημάτων, όπως είναι για παράδειγμα τα δεδομένα, είναι δυνατόν να είναι διάσπαρτα μέσα σε μια εταιρία.

Το επίπεδο της ασφαλείας όλων αυτών των συστημάτων κατά κύριο λόγο οριοθετείται από την ασφάλεια του πιο ασθενούς σημείου τους και κατ' επέκταση η εφαρμογή αποσπασματικών τεχνολογικών μέτρων αυτής της μορφής, δεν φτάνει στην περίπτωση στην οποία τα εν λόγω μέτρα δεν περιέχονται σε μια συνολική τακτική και δεν είναι δυνατόν να συνδυαστούν με μια ενιαία καθώς επίσης και ολιστική μέθοδο αντιμετώπισης της επικινδυνότητας αυτών των συστημάτων.

Η ολοκληρωμένη αντιμετώπιση του συγκεκριμένου θέματος πραγματοποιείται με δράσεις, οι οποίες περιέχονται στη διαχείριση της ασφάλειας αυτών των συστημάτων μιας σύγχρονης εταιρίας. Στη συγκεκριμένη δράση καθοριστικό ρόλο είναι εφικτό να παίξει μια σειρά από τεχνικά πρότυπα αλλά και οδηγίες. Σημαντικό ρόλο, για παράδειγμα, διαδραματίζει η οριοθέτηση των κινδύνων, της στρατηγικής που θα εφαρμοστεί για την ασφάλεια αυτών των συστημάτων, η οριοθέτηση των ρόλων και των καθηκόντων κλπ.

Γίνεται εύκολα αντιληπτό, επομένως, πως η ασφάλεια αυτής της μορφής είναι ζωτικής σημασίας και σε ό,τι έχει να κάνει με τη διάδοση των τεχνολογικών και των εφαρμογών του διαδικτύου των πραγμάτων, είτε όπως καλείται εν συντομία του IOT. Η συγκεκριμένη έννοια χρησίμευσε για πρώτη φορά την περίοδο του '99, παρά το γεγονός πως η βασική ιδέα είχε αναπτυχθεί σχεδόν 10 χρόνια πριν από το MIT.

Στη σημερινή εποχή, τα συγκεκριμένα συστήματα παραμένουν ένα πεδίο ευρέως φάσματος για όλες τις σύγχρονες εταιρίες και τους οργανισμούς. Παρά το γεγονός αυτό, όμως, μέχρι και σήμερα πρόκειται για μια νέα τεχνολογία που είναι γεμάτη αβεβαιότητα. Το βασικότερο όραμα το οποίο υφίσταται πίσω από την εν λόγω τεχνολογία έχει άρρηκτη σχέση με την ενεργοποίηση των ενσωματωμένων συσκευών (που ως επί το πλείστον καλούνται έξυπνα αντικείμενα) σαν πρωτόκολλα διαδικτύου σε μια προσπάθεια να κάνουν υπολογισμούς, να οργανώνουν και παράλληλα να επικοινωνούν.

Η τεχνολογία αυτής της μορφής έχει αναπτυχθεί και συντηρηθεί σε οικονομικά και αποδοτικά σε ενέργεια πλαίσια διαμέσου των αισθητήρων που έχουν ενταχθεί στα συγκεκριμένα συστήματα. Αυτό το οποίο είναι στη σύγχρονη εποχή αυτή η τεχνολογία προέρχεται από το συνδυασμό των συνδεδεμένων συσκευών στο internet, των έξυπνων αντικειμένων, των αισθητήρων καθώς επίσης και των υποστηρικτικών υπηρεσιών που εστιάζουν στον παγκόσμιο ιστό.

Εν κατακλείδι, η έννοια του IoT ίσως είναι πολύ δύσκολο να ορισθεί και αυτό γιατί το πεδίο που εμπίπτει είναι αρκετά μεγάλο και αρκετά δαιδαλώδες πάρα ταύτα η πλειοψηφία των ειδικών αναφέρουν ότι με τον όρο IoT ονομάζουμε την απολυτή συνένωση και λειτουργικότητα δικτυών και οντοτήτων τα οποία δέχονται και λαμβάνονται την σχετική αλληλεπίδραση μεταξύ τους σε πραγματικό χρόνο σε οποιοδήποτε γεωγραφικό μέρος (IETF).

1.2 Περιγραφή προσέγγισης – Σκοπός διπλωματικής εργασίας

Ο βασικός σκοπός κάθε εκπαιδευτικής εργασίας είναι προφανής, αφού κάθε είδους εκπαίδευση προσβλέπει στην απόκτηση της απαραίτητης θεωρητικής και πρακτικής εμπειρίας, που βοηθά, σε πιο βελτιωμένες και επαγγελματικές χρήσιμες εφαρμογές τον κάθε φοιτητή ή σπουδαστή μετά το πέρας των σπουδών του. Έτσι δημιουργούνται και υπάρχουν μεσοπρόθεσμοι στόχοι που έχουν να κάνουν με την έρευνα και το σχεδιασμό, αλλά και τη βαθιά εξοικείωση με τις τεχνολογίες που σήμερα είναι απαραίτητες σε πολλούς τομείς της ζωής.

Η βασική αυτή αντίληψη δημιουργεί τις κατάλληλες προϋποθέσεις για να εφαρμοστούν στην πορεία της εργασίας η ευελιξία αλλά και η πειθαρχία σε νόμους και κανόνες που ήδη υπάρχουν μέσα στην κοινωνία και δεν μπορούν να παραλειφθούν. Στην παρούσα εργασία, ισχύουν βεβαίως όλα τα παραπάνω, αλλά και επιπλέον σκέψεις και προθέσεις που απορρέουν από τη «δική μου» την προσωπική μου θέληση και στόχευση για το τι θα ακολουθήσω επαγγελματικά στην ζωή μου (Γλετζάκος 2016).

Στο πρόλογο που ακολούθησε ακριβώς παραπάνω αναφέρθηκε και έγινε απολύτως σαφές ότι το στοιχείο που θα πρέπει να πάρουμε ως δεδομένο είναι ότι οι τεχνολογίες της πληροφορίας βρίσκονται στα βιώματα μας.

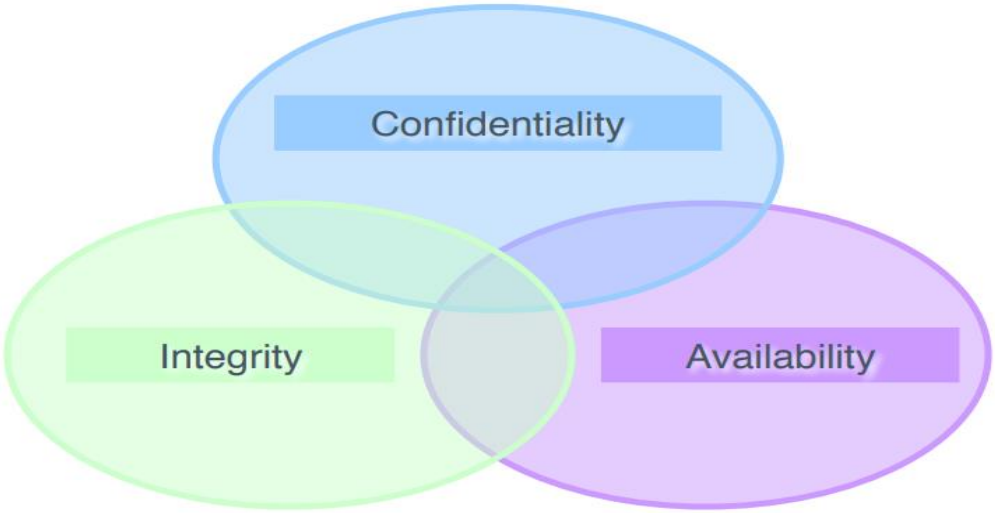
Μέσα από την εργασία αυτή, θα μελετήσουμε τον κόσμο των IoT, του 5G, της μηχανικής μάθησης και το πως αυτή μπορεί να αποτελέσει το κλειδί για να διασφαλίσουμε την πληροφορία που ανήκει μόνο σε εμάς. Αφού, πρώτα γίνουν γνωστοί οι 2 αυτοί κλάδοι η τόσο διαφορετική αλλά όμοιοι επίσης, σε δεύτερη φάση θα μάθουμε πως μέσω της μηχανικής μάθησης μπορούμε να «προστατεύουμε» σε ορισμένες περιπτώσεις.

1.3 Θεμελιώδεις ιδιότητες της ασφάλειας για την πληροφορία

Αφού λοιπόν έχουμε διασφαλίσει ότι η πληροφορία θα μεταδοθεί σε αυτήν την υπόενότητα θα εξετάσουμε ποιοι είναι οι βασικοί πυλώνες στην πληροφορική που μας δίνουν την αξιοπιστία που απαιτούν οι καιρό όσον αφορά την πληροφορία αυτή.

Η ασφάλεια πληροφοριών αποσκοπεί στην προστασία των δεδομένων και των πόρων ενός πληροφοριακού συστήματος, από ζημίες που θα μειώσουν η θα καταστρέψουν ολοσχερώς την αξία τους. Στην ουσία έχουμε στα χέρια μας ένα αγαθό (asset) το οποίο συνήθως είναι κάποιος πόρος ή κάποιο αντικείμενο που έχει αξία για τον ιδιόκτητη του. Αυτό το αγαθό οφείλετε να προστατεύετε. Για να μπορέσει κάποιος να ισχυριστεί ότι όντως το αγαθό του είναι προστατευμένο πρέπει να διασφαλίσει ότι δεν έχουν παραβιαστεί οι 3 βασικοί πυλώνες της πληροφορικής όσον αφορά την ασφάλεια και είναι τα ακόλουθα (Κάτσικα et al. 2004; Πάγκαλου και Μαυρίδη 2002):

α) Εμπιστευτικότητα β) Ακεραιότητα γ) Διαθεσιμότητα.



Εικόνα 1 - Θεμελιώδεις ιδιότητες

Με τον όρο «Εμπιστευτικότητα» εννοούμε την δυνατότητα πρόσβασης στα αγαθά μόνο από όσους έχουν δικαίωμα (εξουσιοδοτημένα μέρη – authorized parties). Δηλαδή, η πρόσβαση προσδιορίζεται ως τύπου ανάγνωσης.

Στην περίπτωση τώρα της ακεραιότητα ορίζεται η δυνατότητα τροποποίησης των αγαθών μόνο από εξουσιοδοτημένα μέρη η μόνο με εξουσιοδοτημένο τρόπο. Μια τροποποίηση μπορεί να περιλαμβάνει αλλαγή κατάστασης, διαγραφή ή ακόμα και μια νέα δημιουργία (Κάτσικα et al. 2004).

Τέλος, ως ορισμό της διαθεσιμότητας στον τομέα της πληροφορικής λαμβάνουμε την εξασφαλισμένη πρόσβαση στα αγαθά, μόνο από τα εξουσιοδοτημένα μέρη όποτε απαιτείται. Με λίγα λόγια η έγκαιρη απόκριση, η δίκαιη κατανομή, η ανεκτικότητα στα λάθη και γενικότερα η ελεγχόμενη σύμπτωση είναι ο στόχος σε κάποιον που θέλει να εξασφαλίσει ότι το σύστημα του παρέχει διαθεσιμότητα (Καντζάβελου 2018; Πάγκαλου και Μαυρίδη 2002)

Με μια γρήγορη σκέψη θα μπορέσουμε να καταλάβουμε ότι γενικά οι τρεις αυτοί πυλώνες είναι ανεξάρτητα κομμάτια αλλά μπορεί μερικώς να επικαλύπτονται ή και να αποκλείει το ένα το άλλο. Για παράδειγμα η εμπιστευτικότητα μπορεί να περιορίζει την διαθεσιμότητα (Κάτσικα et al. 2004).

Όλα τα παραπάνω μπορούμε να τα διασφαλίσουμε εάν έχουμε μια έγκαιρη

πρόληψη, μια βαθιά ανίχνευση και μετέπειτα αντίδραση καθώς οι «ζημίες» που προκαλούνται από τις επιθέσεις είναι ποικίλες και διαφέρουν. Η ουσία βέβαια παραμένει η ίδια η οποία δεν είναι άλλη από την εκμετάλλευση μια ευπάθειας ώστε να προκληθεί μια επίθεση. Χαρακτηριστικά αναφέρονται ορισμένες επιθέσεις που μπορούν να πραγματοποιηθούν στα πληροφοριακά συστήματα και στην συνέχεια των κεφαλαίων θα γίνει μια πιο στοχευμένη επισκόπηση κάποιων εκ των κατηγοριών (Πάγκαλου και Μαυρίδη 2002; Κάτσικα et al. 2004).

- Ανθρώπινες ευπάθειες
- Ευπάθειες υλικού & λογισμικού
- Ευπάθειες μέσων
- Φυσικές ευπάθειες
- Εκ φύσεως ευπάθειες.

Εικόνα 2 - Ηλεκτρονικός Υπολογιστής

ΚΕΦΑΛΑΙΟ 2 – IoT

2.1 Ιστορική Αναδρομή

Το Διαδίκτυο των πραγμάτων (IoT) είναι μια ραγδαίως αναπτυσσόμενη τεχνολογία που εντάσσεται ολοένα και περισσότερο στις ζωές μας. Η βασική ιδέα του IoT είναι η ενσωμάτωση συσκευών καθημερινής χρήσης ή μη, με σκοπό την βελτίωση της ποιότητάς ζωής μας (Press 2014; Σολδάτος 2017)

Αν και έχουμε την εντύπωση ότι πρόκειται για κάτι εντελώς καινούργιο που από μια όψη δεν είναι και τελείως λάθος, σαν αόριστη σκέψη το IoT υπάρχει από το 1950 κιόλας.

Οι μηχανικοί της IBM είχαν την απαίτηση να οριοθετήσουν ταυτότητες σε όλα τα αντικείμενα και τα συστήματα τα οποία χρησιμοποιούσαν στην εν λόγω εταιρία. Η συνεχής ενασχόληση και οι δοκιμές με γραμμικούς σχηματισμούς σταδιακά οδήγησαν στη δημιουργία των barcodes. Η πρώτη δημιουργία αυτής της μορφής ήρθε 5 χρόνια αργότερα με την ανάπτυξη ενός ρολογιού που πρόβλεπε τους κύκλους που έκαναν οι ρουλέτες στα καζίνα (Βελλισάρης, 2017). Ήταν ολοένα και πιο ξεκάθαρο σαν εικόνα ότι σιγά σιγά όλες οι εταιρείες έπρεπε να έχουν ταυτότητα στα πάντα που εμπορευόντουσαν (Press 2014; Σολδάτος 2017).

Κατά καιρούς υπάρχουν πειραματισμοί από επιστήμονες ώστε να ακολουθήσουν σε επίπεδο hardware και κινητών φορητών συσκευών την ίδια νοοτροπία.

Σχεδόν 15 χρόνια αργότερα αναπτύχθηκε το 1ο σύστημα σε σχήμα μυωπικών γυαλιών που έπαιξε καθοριστικό ρόλο για τους ανθρώπους με ειδικές ανάγκες, προκειμένου να διαβάζουν τα χείλια ων ανθρώπων (σύμφωνα με αυτή την ιδέα ανακαλύφθηκε πριν μερικά χρόνια το Google Glass) (Press 2014; Σολδάτος 2017). Την περίοδο του ’70 αναπτύχθηκε το δίκτυο ARPANET με στόχο την επικοινωνιακή ανταλλαγή πληροφοριών ανάμεσα σε διάφορες στρατιωτικές βάσεις ενώ την περίοδο του ’82 ανακαλύφθηκε το TCP/IP, διαμέσου του οποίου ξεκίνησε μια καινούρια εποχή (Hassan 2018).

Πλησιάζοντας το 1973 δημιουργήθηκε η τεχνολογία των RFID που θα αποτελέσει και τον κορμό στην εποχή του IoT και πρόκειται για την τεχνολογία που επιτρέψει την ασύρματη επικοινωνία μέσω των RFID Tags με παθητική ανάγνωση δεδομένων αλλά και εγγραφή σε άλλες συσκευές. Πάρα ταύτα, τα RFID στον επιχειρησιακό κλάδο άργησαν πολύ να ενταχθούν καθώς η επικρατούσα μέχρι τότε χρήση των barcode είχε αποδεκτή πολύ φιλική (Press 2014; Σολδάτος 2017). Σχεδόν 10 χρόνια αργότερα ανακαλύφθηκε πρωτόκολλο Machine to Machine. Το συγκεκριμένο πρωτόκολλο το οποίο θα το συναντήσουμε και στην συνέχεια δεν ήταν άλλο από το MQTT και αποτέλεσε ένα από τα πιο σημαντικά βήματα για την ενίσχυση προς την επικράτηση του Internet of Things (Αποστολόπουλος 2020; Lawton 2004; Κουλουβάκης 2019; Σολδάτος 2017) ενώ την περίοδο του ’95 υπήρξε το πρώτο τσιπ που διαμέσου

δικτύου GSM από την Siemens. Αυτό παρείχε την ευχέρεια σε διάφορα βιομηχανικά συστήματα να επικοινωνούν μεταξύ τους ασύρματα όπως επίσης υπάρχει η δυνατότητα εκτέλεσης εντολών (Boulogeorgos et al. 2017).

Την περίοδο του ’99 αναπτύχθηκε το 1^{ο} κέντρο ερευνών για παρόμοιας μορφής συστήματα ενώ ένα χρόνο αργότερα αναπτύχθηκε το πρώτο πρωτόκολλο επικοινωνίας αυτής της μορφής.

Στην πορεία υπήρξαν ομάδες που είχαν σκοπό την διαδώσει του IP σε όλα τα μελλοντικά σχέδια και προτάσεις που αφορούσαν το IoT. Οπότε το 2010 αναβαθμίστηκε η τεχνολογία του Bluetooth και δημιουργήθηκε το έξυπνο Bluetooth. Η εξέλιξη αυτή ονομάζεται BLE (Bluetooth Low Energy) και παρείχε καινούριες εφαρμογές και διασυνδεδεμένα συστήματα σε μια σειρά από κλάδους όπως η υγεία, η άθληση, το Smart Home κλπ. Την ίδια χρονιά δημιουργήθηκε η υπηρεσία της Google, με street view από φωτογραφίες 360 μοιρών (Tsiatsis et al. 2018).

Εξασφαλίζοντας επί της ουσίας ότι το IoT θα μας απασχολεί για πολλά χρόνια ακόμα το 2005 κατασκευάστηκε το Arduino που αποτελούσε μια οικονομική λύση μικροελεγκτή που προοριζόταν για φοιτητές (Αποστολόπουλος 2020; Lawton 2004; Κουλουβάκης 2019; Σολδάτος 2017). Στα επόμενα χρόνια έγιναν μεγάλες επενδύσεις από εταιρείες όπως η Apple, η Google και άλλες αφού είχε προεξοφλήσει ότι το IoT είναι το παρόν μας.

Εκείνη την περίοδο ξεκίνησε να υφίσταται τεράστιο ερευνητικό ενδιαφέρον για αυτή την τεχνολογία. Στα τέλη της περιόδου του 2013, η IDC δημοσίευσε μια αναφορά η οποία τόνιζε πως η συγκεκριμένη τεχνολογία θα στοίχιζε 8.900 δις δολάρια στην αγορά μέχρι την περίοδο του 2020 και με αυτόν τον τρόπο η έννοια του IOT άρχισε να διαδίδετε παντού σε παγκόσμιο επίπεδο. Σε αυτή τη διάδοση καθοριστικό ρόλο έπαιξε η αγορά της Nest από την Google αντί 3,2 δισεκατομμυρίων δολαρίων.

Τέλος, την επόμενη χρονιά η APPLE ανακοίνωσε το HealthKit & HomeKit. Πρόκειται για 2 πλατφόρμες ανάπτυξης υλοποιήσεων ενώ καθοριστικό ρόλο διαδραματίζει και η υποστήριξη της πλατφόρμας από διάφορα καινούρια συστήματα που στόχο είχαν την εξέλιξη της ιδέας των έξυπνων σπιτιών και της καθημερινότητας των ανθρώπων (Greengard 2015).

Με την ενσωμάτωση του πρωτοκόλλου IPv6 επιτράπηκε σε κάθε αντικείμενο να έχει την δικιά του ξεχωριστή διεύθυνση IP με αποτέλεσμά τα πάντα πλέον να δραστηριοποιούνται στο κόσμο του IoT (Αποστολόπουλος 2020; Lawton 2004; Κουλουβάκης 2019; Σολδάτος 2017).

2.2 Ορισμός του IoT

Για να είμαστε απολύτως αντικειμενικοί, ο ορισμός του Internet of Things δεν είναι τόσο εύκολο να διατυπωθεί σε μια πρόταση. Με τη συγκεκριμένη ορολογία καλούμε ένα δίκτυο φυσικών αντικειμένων, συστημάτων, οχημάτων, κτιρίων καθώς επίσης και διάφορων άλλων αντικειμένων που περιλαμβάνουν ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικά, αισθητήρες αλλά και διάφορες διαδικτυακές ικανότητες διασύνδεσης, κάτι το οποίο προσφέρει την ευχέρεια στα εν λόγω αντικείμενα να συλλέγουν είτε ακόμα και να ανταλλάσσουν πληροφορίες (Βελλισάρης 2017)

Η τεχνολογία αυτής της μορφής προσφέρει την ευχέρεια στα παραπάνω αντικείμενα να παρακολουθούνται απομακρυσμένα διαμέσου μιας δικτυακής υποδομής, αναπτύσσοντας σημαντικές δυνατότητες αλληλεπίδρασης του φυσικού κόσμου με διάφορα υπολογιστικά συστήματα της σημερινής εποχής. Όλο αυτό έχει σαν κυριότερη συνέπεια την αισθητή βελτίωση της αποδοτικότητας των συγκεκριμένων συστημάτων, την ακρίβεια καθώς επίσης και τη σημαντική ελάττωση του κόστους (Tsiatsis et al. 2018).

Ακόμα, η τεχνολογία αυτού του είδους βασίζεται στην τεχνολογία η οποία περιέχει διάφορους αισθητήρες και ενεργοποιητές που αποτελούν ένα καθοριστικό κομμάτι των καθημερινών έξυπνων συστημάτων, όπως είναι για παράδειγμα τα έξυπνα σπίτια, τα έξυπνα οχήματα κλπ. Όλα τα αντικείμενα αυτής της μορφής αναγνωρίζονται ξεχωριστά από το ενσωματωμένο υπολογιστικό σύστημα και υφίσταται η δυνατότητα να δράσει τόσο αυτόνομα όσο και σε συνεργασία με όλη την άλλη διαδικτυακή υποδομή (Boulogeorgos et al. 2017).

Ολοκληρωμένα σύστημα που έχουν στόχο να φέρουν εις πέρας μια συγκεκριμένη αποστολή έως μέχρι και οι πιο απλές wearables συσκευές που χρησιμοποιούνται για την συλλογή δεδομένων μέσω των ενσωματωμένων αισθητήρων που υπάρχουν σε αυτά καλούνται ως IoT Devices. Με λίγα λόγια οποιαδήποτε ηλεκτρονική συσκευή έχει σύνδεση μεταξύ άλλων και διαδικτύου θα μπορούσε να θεωρηθεί ως κομμάτι του Internet of things. Μην ξεχνάμε ότι όπως προκύπτει και από την ιστορική αναδρομή ο ορός είναι κάτι το πρόσφατο. Σε αυτό μπορούμε να αναλογιστούμε ότι ο ορός προστέθηκε στο λεξικό Oxford μόλις τον Αύγουστο του 2013. Πρέπει να γίνει κατανοητό απόλυτα ότι το Internet όπως το ξέραμε τα προηγούμενα χρόνια δεν υπάρχει πια και αποτελεί τη ραχοκοκαλιά του σημερινού μας Internet of Things.

Επί της ουσίας το Διαδίκτυο των πραγμάτων είναι μια από τις πιο ακμάζουσες τεχνολογίες της τρέχουσας εποχής. Σήμερα, πολλές συσκευές που άνοιξαν το δρόμο για την ανάπτυξη έξυπνων σπιτιών σε έξυπνα αυτοκίνητα συνδέονται μέσω δικτύων IoT ενώ πλέον χρησιμοποιούνται και διάφορες ιατρικές συσκευές όπως βηματοδότες και νευροδιεγέρτες που επιτρέπουν την παρακολούθηση ασθενών από μακριά και συνδέονται μέσω IoT (Korenda et al. 2019).

Στον αντίποδα με τον ορισμό που διατυπώθηκε παραπάνω, υπάρχουν εκείνοι που ισχυρίζονται ότι για να χαρακτηριστεί κάτι ως κομμάτι του Internet of Things δεν

χρειάζεται να έχει άμεση πρόσβαση στο δίκτυο τουλάχιστον την στιγμή που συλλεγεί τα δεδομένα αλλά αρκεί ακόμα και μια έμμεση επικοινωνία. Ένα χαρακτηριστικό παράδειγμα είναι το γνωστό σε όλους μας smartwatch που παρακολουθεί την φυσική μας κατάσταση και την υγεία μας γενικότερα μέσω των ενσωματωμένων αισθητήρων που διαθέτει, τα μεταδίδει στην αντίστοιχη εφαρμογή μέσω της τεχνολογίας Bluetooth και εν συνεχεία καταγράφονται. Η καταγραφή αυτή μπορεί για παράδειγμα να γίνει σε μια online cloud υπηρεσία (Σολδάτος 2017; Vohra & Srivastava 2015).

Αφού γνωστοποιήθηκε η δυσκολία και οι διαφωνίες που υπάρχουν στην κοινότητα της πληροφορικής ως προς τον ορισμό της έννοιας Internet of Things παρακάτω παρουσιάζονται οι ορισμοί όπως έχουν δοθεί από μεγάλους οργανισμούς του κλάδου.

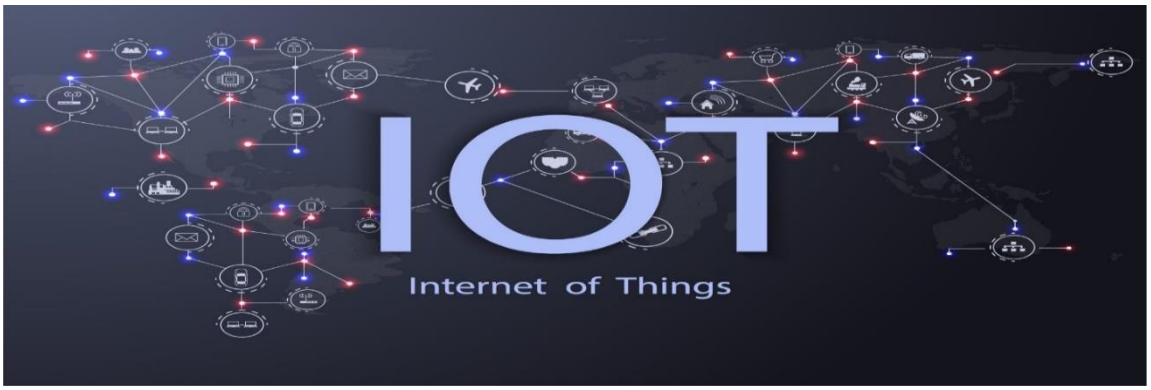
Συγκεκριμένα:

Ο οργανισμός IEEE ορίζει το διαδίκτυο των πράγματων ως ένα δίκτυο των πράγματων όπου το καθένα έχει αισθητήρες ενσωματωμένους και έχουν την δυνατότητα αυτοί να συνδέονται στο διαδίκτυο (Πάντζιου et al. 2020; Παπαζώης 2007).

Η IETF περιγράφει το διαδίκτυο των πράγματων ως μια «υπηρεσία» που συνδέει τα πάντα γύρω μας ηλεκτρικά και μη ηλεκτρικά για την παροχή συνεχούς επικοινωνίας μεταξύ τους (Πάντζιου et al. 2020; Παπαζώης 2007).

Η ITU-T από την άλλη ορίζει το διαδίκτυο των πράγματων ως μια υποδομή από ήδη υπάρχουσες τεχνολογίες που αποτελείται από διασυνδεμένα αντικείμενα. Τα αντικείμενα αυτά τα θέτουν σε λειτουργία προηγμένες υπηρεσίες (Πάντζιου et al. 2020; Παπαζώης 2007).

Οποιοσδήποτε από τους παραπάνω ορισμούς και να είναι πιο κοντά στο να περιγράψει την ουσία του IoT ένα είναι το δεδομένο που σίγουρα εξάγουμε και δεν είναι άλλο από το ότι το δίκτυο πραγμάτων και των αντικειμένων θα αποτελέσει τον τεχνολογικό μας μέλλον τις επόμενες δεκαετίες.



Εικόνα 3 - Internet of Things

2.3 Χαρακτηριστικά των IoT Networks

Ένα από τα κυριότερα γνωρίσματα αυτών των δικτύων είναι η διασυνδεσιμότητα. Κάθε συσκευή είναι εφικτό να συνδεθεί με τη διεθνή υποδομή ενημέρωσης και επικοινωνίας. Εξίσου καθοριστικό γνώρισμα αυτής της μορφής είναι οι υπηρεσίες, οι οποίες έχουν άμεση σχέση με τις συσκευές (πράγματα). Επί της ουσίας η εν λόγω τεχνολογία έχει την ευχέρεια να προσφέρει χρήσιμες υπηρεσίες, οι οποίες ως επί το πλείστον έχουν να κάνουν με τα πράγματα, δίχως όμως να αγνοεί τη σημασιολογική συνοχή, η οποία υφίσταται ανάμεσα στο φυσικό αλλά και εικονικό των πραγμάτων, κάτι το οποίο σταδιακά θα επιφέρει καθοριστικές μεταβολές, τόσο των τεχνολογιών του φυσικού κόσμου όσο και των πληροφοριών (Boulogeorgos et al. 2017).

Εξίσου σημαντικό γνώρισμα λογίζεται πως είναι και η ετερογένεια. Τα συστήματα στο internet είναι ετερογενή, αφού εστιάζουν κατά βάση σε διαφοροποιημένες πλατφόρμες αλλά και δίκτυα. Παρά το γεγονός αυτό, όμως, έχουν την ευχέρεια της αλληλεπίδρασης με διάφορες άλλες συσκευές, συστήματα είτε ακόμα και σύγχρονες πλατφόρμες υπηρεσιών, διαμέσου διαφοροποιημένων δικτύων (Hassan 2018).

Στα κυριότερα γνωρίσματα συμπεριλαμβάνονται, παράλληλα και οι δυναμικές μεταβολές σε συνδυασμό με την μεγάλη κλίμακα χρηστών. Σε ό,τι έχει να κάνει με το πρώτο γνώρισμα εξ αυτών, είναι σημαντικό να τονιστεί πως η κατάσταση των σύγχρονων συστημάτων μεταβάλλεται δυναμικά, για παράδειγμα είναι ενεργές ή όχι, είναι συνδεδεμένες ή όχι, μεταβάλλεται η θέση καθώς επίσης και η ταχύτητά τους. ακόμα, το σύνολο των συνδεδεμένων συστημάτων είναι δυνατόν να μεταβάλλεται και αυτό δυναμικά (Greengard 2015).

Από την άλλη πλευρά, για την μεγάλη κλίμακα χρηστών, θα πρέπει να σημειωθεί πως το σύνολο των συστημάτων, που οι χρήστες διαχειρίζονται και διαμέσου των οποίων έχουν την ευχέρεια να επικοινωνήσουν μεταξύ τους, διαμέσου της συγκεκριμένης τεχνολογίας, θα είναι πιο μεγάλο σε σχέση με το σύνολο των συστημάτων τα οποία είναι διασυνδεδεμένα στο τρέχον internet. Επιπλέον, είναι σημαντικό να γνωρίζουμε πως στο μέλλον θα είναι περισσότερο καθοριστική η αποδοτική διαχείριση καθώς επίσης και η ερμηνεία των δεδομένων που θα παράγονται διαμέσου αυτής της τεχνολογίας και αυτών των συσκευών (Hussain et al. 2020).

Καθοριστικό γνώρισμα, όμως, θεωρείται πως είναι και η ασφάλεια. Στη σημερινή εποχή είναι ζωτικής σημασίας να υφίσταται ασφαλής σχεδιασμός, τόσο για όλους τους δημιουργούς όσο και για τους ίδιους τους παραλήπτες αυτής της τεχνολογίας, όπως επίσης και σε ό,τι έχει να κάνει με την ασφάλεια των προσωπικών δεδομένων και της ιδιωτικότητας όλων των χρηστών. Η ασφάλεια είναι σημαντικό να κλιμακωθεί μεταξύ αυτών των συστημάτων, των δικτύων είτε ακόμα και των διακινούμενων πληροφοριών (Hassan 2018).

Τέλος, εξίσου σημαντικό χαρακτηριστικό αυτής της μορφής είναι η παράμετρος

της συνδεσιμότητας. Αυτό το γνώρισμα στην ουσία έχει να κάνει με την προσβασιμότητα αλλά και τη συμβατότητα την οποία εμφανίζει το εκάστοτε δίκτυο. Για παράδειγμα η παράμετρος της προσβασιμότητας προσφέρει την ευχέρεια για σύνδεση σε ένα δίκτυο, ενώ από την άλλη πλευρά εκείνη της συμβατότητας προσφέρει την κοινή ικανότητα ανάπτυξης καθώς επίσης και χρησιμότητας πληροφοριών του εκάστοτε δικτύου (Greengard 2015).

Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως η εν λόγω τεχνολογία εξυπηρετεί αρκετούς και διαφορετικούς χρήστες. Οι διαφοροποιημένες κατηγορίες χρηστών εμφανίζουν και διαφοροποιημένες απαιτήσεις. Στη σημερινή εποχή υφίστανται 3 καθοριστικές ομάδες χρηστών, που είναι οι μεμονωμένοι χρήστες, η κοινότητα πολιτών (πολίτες μιας πόλης, μιας περιφέρειας κλπ) καθώς επίσης και οι εταιρίες (Tsiatsis et al. 2018).

Συνοπτικά έχουμε λοιπόν τα ακόλουθα:

- Διασυνδεσιμότητα
- Διαλειτουργικότητα – Ετερογένεια
- Δυναμικότητα & Αυτοπροσαρμογή
- Ασφάλεια
- Αυτόδιαμόρφωση
- Επεκτασιμότητα
- Μοναδικό αναγνωριστικό για κάθε IoT συσκευή

Εικόνα 4 - Security Goals for IoT

2.4 Προκλήσεις ασφαλείας στο IoT

Στην αρχή της παρούσας εργασίας αναλύσαμε ποιοι είναι οι τρεις πυλώνες στον τομέα της ασφάλειας για οποιοδήποτε σχεδόν πληροφοριακό σύστημα.

Ομοίως λοιπόν και στον IoT οφείλεται να προστατεύονται οι 3 αυτές βασικές αρχές. Με την παραβίαση ακόμα και ενός εξ αυτών μπορεί να προκληθεί μεγάλη ζημιά σε κάποιο σύστημα IoT (Παπαζώης 2007).

Τα τελευταία χρόνια αρκετές έρευνες αναφέρουν πως σχεδόν το 80% των συγκεκριμένων συσκευών εμφανίζουν τεράστια ανησυχία της ιδιωτικότητας στην περίπτωση στην οποία διασυνδέονται σε υπηρεσίες cloud είτε μεταφέρουν προσωπικά δεδομένα, που δεν έχουν περάσει από την απαιτούμενη κρυπτογράφηση. Τα δεδομένα τα οποία προσφέρονται από τις συγκεκριμένες συσκευές τις περισσότερες φορές συγκεντρώνονται και χρησιμεύουν συνδυαστικά με όλα τα άλλα δεδομένα σε ένα κοινό διαδικτυακό server. (Βελλισάρης 2017 ; Πάγκαλου και Μαυρίδη 2002).

Το παραπάνω γεγονός ως επί το πλείστον σημαίνει πως τα εν λόγω συστήματα έχουν την ευχέρεια να συνδεθούν με μια καθορισμένη ταυτότητα διαμέσου της διευθυνσιοδότησης, που αναπτύσσει την απαίτηση για προστασία των προσωπικών δεδομένων καθώς επίσης και πιο ασφαλή ανταλλαγή δεδομένων. παράλληλα, μελέτες κάνουν λόγο πως σχεδόν το 90% αυτών των συστημάτων συλλέγουν προσωπικά δεδομένα, ενώ το 80% εξ αυτών δεν έχουν κωδικούς πρόσβασης, επομένως, θίγεται η αυθεντικότητά τους ενώ την ίδια ώρα ένα ποσοστό της τάξης του 60 έως και 70% των συγκεκριμένων συστημάτων δεν έχουν την ευχέρεια κρυπτογράφησης και προστασίας, κατεβάζοντας τις σχετικές ενημερώσεις (Hassan 2018; Πάγκαλου και Μαυρίδη 2002).

Γενικότερα, τα κυριότερα ζητήματα τα οποία λογίζονται πως χρήζουν μεγαλύτερης λήψης μέτρων με απώτερο στόχο την βέλτιστη εφικτή ασφάλεια των συνδεδεμένων πραγμάτων είναι οι κόμβοι στους οποίους δεν προσφέρεται η απαιτούμενη επίβλεψη, τα μέτρα με κυριότερο στόχο την αποφυγή φυσικών επιθέσεων, τα μέτρα που συσχετίζονται με την ασύρματη δικτύωση η οποία προσφέρει την ευχέρεια ευκολότερου ελέγχου και καταγραφής είτε αλλοίωσης πληροφοριών, ο διεξοδικός έλεγχος όλων των πόρων και των κόμβων με περιορισμένες προοπτικές, οι οποίοι δεν αφήνουν την εύρυθμη δράση των σύνθετων δομών άμυνας και προστασίας και τέλος τα σημεία στα οποία δεν υφίσταται αξιόπιστη τακτική επικοινωνίας (ασύρματη εκπομπή κλπ) (Boulogeorgos et al. 2017).

Στις κυριότερες προκλήσεις ασφαλείας που καλείται να αντιμετωπίσει η συγκεκριμένη τεχνολογία περιέχονται τα παρακάτω :

- Να προσφέρει αντοχή σε επιθέσεις, αφού είναι ζωτικής σημασίας να αποφεύγονται τα μοναδικά σημεία αστοχίας, ενώ το δίκτυο είναι σημαντικό να έχει τη δυνατότητα να ανακάμψει ύστερα από μια επίθεση

- Να προσφέρει την απαιτούμενη αυθεντικοποίηση των συμμετεχόντων πραγμάτων

- Να προσφέρει την απαιτούμενη εξουσιοδότηση, προκειμένου η εποπτεία πρόσβασης να προσφέρει την ευχέρεια είτε όχι της πρόσβασης στη βάση των δικαιωμάτων της εκάστοτε συσκευής
- Να εξασφαλίζει στο βέλτιστο εφικτό επίπεδο την ιδιωτικότητα, αφού η συγκεκριμένη τεχνολογία στη σημερινή εποχή υφίσταται παντού (Βελλισάρης 2017; Πάγκαλου και Μαυρίδη 2002).

Τέλος, είναι σημαντικό να σημειωθεί πως στους κυριότερους κλάδους της ασφαλείας που είναι χρήσιμο να εστιάσουν την προσοχή τους όλοι οι χρήστες αυτής της τεχνολογίας είναι η ευπάθεια στις επιθέσεις, η κλωνοποίηση ετικετών καθώς επίσης και οι κλοπές ταυτοτήτων, τα δικαιώματα πρόσβασης σε χρήσιμες πληροφορίες, η ποιότητα και η ακεραιότητα, η δέσμευση καθώς επίσης και η συντήρηση των προσωπικών δεδομένων (Hussain et al. 2020)

2.5 Αρχιτεκτονική IoT

Γίνεται ευκολά αντιληπτό ότι ο αυξημένος αριθμός των IoT Devices απαιτεί και την ανάλογη αρχιτεκτονική καθώς ο αριθμός αυτός αυξάνεται εκθετικά και η αρχιτεκτονική είναι απαραίτητη για την κλιμακώσιμη λειτουργία τους. Επίσης, η αρχιτεκτονική είναι εξίσου απαραίτητη για την απομακρυσμένη υποστήριξη και διαχείριση των συσκευών. (Παπαζώης 2007; Πάντζιου et al. 2020).

Λόγω του ότι οι εφαρμογές IoT βασίζονται στην αρχιτεκτονική προσέγγιση του διαδικτύου η οποία φυσικά έχει αναφορά στα 7 επίπεδα OSI μπορούμε να πούμε όλη η αρχιτεκτονική πατάει στα ακόλουθα:

- Application Layer (Στρώμα εφαρμογής)
- Management Service Layer (Στρώμα υπηρεσιών)
- Network Layer (Στρώμα δικτύου)
- Sensor Layer (Στρώμα στοιχείου)

Πάρα ταύτα στην αρχιτεκτονική αναφοράς έχουμε ορισμένα κάθετα επίπεδα και ορισμένα οριζόντια. Συγκεκριμένα έχουμε τα ακόλουθα επίπεδα:

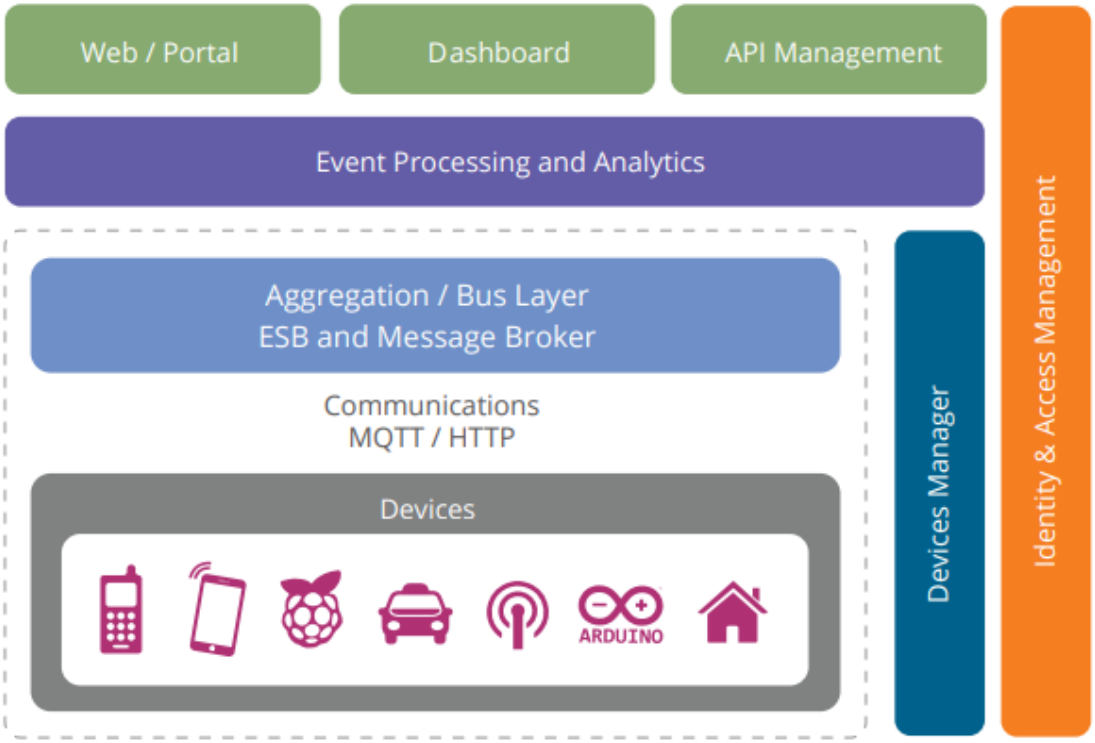
- Εξωτερικές επικοινωνίες – Πίνακας ελέγχου – APIs
- Επεξεργασία συμβάντων & Αναλυτικά στοιχεία
- Επίπεδο συγκέντρωσης / διαύλου – Επίπεδο Μηνυμάτων
- Επίπεδο Μεταφορών μέσω πρωτοκόλλων
  (MQTT / HTTP / XMPP / CoAP / AMQP κλπ)
- Συσκευές – Αισθητήρες

Μια σημαντική σημείωση που δεν πρέπει να την παραλείψουμε είναι ότι στο επίπεδο συμβάντων μπορεί να γίνει και η αποθήκευση των δεδομένων

Ως κάθετα επίπεδα συναντάμε τα ακόλουθα:

- Διαχειριστής συσκευών
- Διαχείριση ταυτότητας & Πρόσβασης

Μια χαρακτηριστική εικόνα που μπορεί να μας αποτυπώσει γλαφυρά όλο αυτό που περίγραψε αναλυτικά μόλις δίνεται στην συνέχεια (Fremantle 2015).



Εικόνα 5 - Αρχιτεκτονική Αναφοράς IoT

DEVICE LAYER

Στο κατώτερο επίπεδο λοιπόν της αρχιτεκτονικής συναντάμε το επίπεδο συσκευής. Υπενθυμίζεται ότι για να θεωρηθεί μια συσκευή ως IoT πρέπει να έχει κάποια επικοινωνία έμμεση η άμεση με το διαδίκτυο. Παραδείγματα άμεσων συσκευών είναι τα εξής:

- Arduino με σύνδεση Arduino Ethernet ή WiFi
- Αισθητήρες
- Raspberry Pi με σύνδεση Ethernet ή WiFi
- Συσκευές ZigBee
- Συσκευές που επικοινωνούν μέσω ραδιοφώνων χαμηλής ισχύος
- Συσκευή UUID που παρέχεται από υποσυστήματα πχ Bluetooth

Ουσιαστική σημείωση και για την συνέχεια της διπλωματικής εργασίας είναι ότι η κάθε συσκευή διαθέτει UUID δηλαδή ένα αμετάβλητο αναγνωριστικό που παρέχεται από τον πυρήνα στο υλικό καθώς και ένα OAuth2 Refresh διακριτικό δηλαδή αποθηκευμένο στην EEPROM. Η προδιαγραφή βασίζεται σε HTTP και οι ροές αυτές γίνονται μέσω MQTT όπου θα τον εξετάσουμε στην συνέχεια (Fremantle 2015).

COMMUNICATION LAYER

Το συγκεκριμένο επίπεδο υποστηρίζει τη συνδεσιμότητα των συσκευών. Υπάρχουν πολλά πρωτόκολλα επικοινωνίας μεταξύ των συσκευών. Τα πιο διαδεδομένα όμως εξ αυτών είναι τα ακόλουθα:

1. HTTP / HTTPS
2. MQTT 3.1
3. CoAP

AGGREGATES & BROKERS

Το συγκεκριμένο στρώμα της αρχιτεκτονικής είναι αρκετά σημαντικό αφού μέσω αυτού υπάρχει η δυνατότητα υποστήριξης ενός διακομιστή HTTP και ενός MQTT ώστε να «μιλήσουν» οι συσκευές μεταξύ τους. Υπάρχει η ικανότητα συγκέντρωσης και συνδυασμού επικοινωνιών από διαφορετικές συσκευές. Η ικανότητα αυτής της γεφύρωσης και του μετασχηματισμού μεταξύ διαφορετικών πρωτοκόλλων είναι από τις πιο ουσιώδες δραστηριότητες του πρωτοκόλλου. Το στρώμα αυτό μπορεί επίσης να παρέχει κάποια απλή συσχετική και χαρτογράφηση από διαφορετικά μοντέλα συσχέτισης για παράδειγμα η αντίστοιχη ενός αναγνωριστικού συσκευής με ένα αναγνωριστικό κατόχου και το ανάποδο.

Τέλος, το επίπεδο αυτό εκτελεί και δυο βασικούς ρόλους ασφαλείας. Είναι ικανό να επικυρώση μέσω του OAuth2 και των πόρων την ζεύξη. Με λίγα λόγια παίζει τον ρόλο του διαμεσολαβητή για να επιτευχθεί μια επικοινωνία σύμφωνα με την πολιτική του Management Layer (Fremantle 2015).

EVENT PROCESSING & ANALYTICS LAYER

Στο επίπεδο αυτό γίνεται η επεξεργασία των γεγονότων που παρουσιάζονται. Μια από τις πιο βασικές ικανότητές είναι η αποθήκευση των δεδομένων σε μια βάση. Υπάρχουν πολλές προσεγγίσεις ώστε να επιτευχθεί το αποτέλεσμα αυτό. Βέβαια η πρώτη και η πιο βασική είναι η χρήση μια μεγάλης πλατφόρμας ανάλυσης δεδομένων σε συνδυασμό με την κλιμάκωση που υποστηρίζεται από τεχνολογίες όπως το Apache Hadopp για την παροχή εξαιρετικά επεκτάσιμων αναλυτικών στοιχείων του mapreduce. Μια δεύτερη προσέγγιση είναι η υποστήριξη επεξεργασιών σε πραγματικό χρόνο βάσει των δεδομένων που αντλούνται απ’ τις συσκευές (Fremantle 2015).

CLIENT COMMUNICATIOS LAYER

Όπως γνωστοποιήθηκε και παραπάνω η αρχιτεκτονική αναφοράς πρέπει να παρέχει έναν τρόπο επικοινωνίας των έξω συσκευών με την συσκευή που βρίσκεται στο σύστημα. Αμέσως, αμέσως γίνεται αντιληπτό ότι χρειαζόμαστε τη δυνατότητα δημιουργίας διαδικτυακών διεπαφών και πυλών να αλληλοεπιδρούν με τις συσκευές και με το επίπεδο επεξεργασίας. Το στρώμα αυτό είναι υπεύθυνο για ακριβώς αυτήν την εργασία. Επιπλέον, το στρώμα αυτό είναι υπεύθυνο για την αλληλεπίδραση των στοιχείων με τα αποκολλόμενα API που και εκείνα ελέγχονται με την σειρά τους από κάποιο κεντρικοποιημένο σύστημα διαχείρισης (API Managemnt).

Στο ίδιο στρώμα υπάρχει όπως φαίνεται εξάλλου και από την εικόνα πιο πάνω και το «Dashboard» που είναι υπεύθυνο για την δημιουργία γραφημάτων και άλλων απεικονίσεων του για τα δεδομένα που προέρχονται από τις συσκευές και το επίπεδο συμβάντων.

Τέλος, το API Management που αναφέρθηκε προηγουμένως έχει τρεις κυρίες λειτουργίες. Πρώτον παρέχει μια πύλη επικεντρωμένη στον προγραμματιστή όπου οι προγραμματιστές μπορούν να εξερευνήσουν το σύστημα , τις διαθέσιμες εκδόσεις και τα γεγονότα των APIs. Δεύτερον, παρέχει μια άλλη πύλη εκτελώντας πολίτικες ελέγχου για περιορισμό και έλεγχό πρόσβασης και τέλος η τελευταία πύλη είναι εκείνη που «δημοσιεύει» τα δεδομένα στο επίπεδο αναλυτικών στοιχείων (Fremantle 2015).

DEVICE MANAGER

Το στρώμα αυτό επικοινωνεί με συσκευές μέσω πρωτοκόλλων και παρέχει μαζικό έλεγχό συσκευών. Επί της ουσίας διαχειρίζεται εξ αποστάσεως το λογισμικό και τις εφαρμογές που αναπτύσσονται στην συσκευή. Μπορεί να κλειδώσει ή και διαγράψει εντελώς μια συσκευή εάν το κρίνει απαραίτητο. Ο Device Manager είναι επίσης ο διαχειριστής της λίστας των ταυτοτήτων των συσκευών όπως επίσης είναι υπεύθυνος για το ποιος άλλος μπορεί να διαχειριστεί την εκάστοτε συσκευή πλην του ιδιοκτήτη. Υπάρχουν τρία είδη, οι μη διαχειριζόμενοι, οι ημιδιαχειροζόμενοι και οι πλήρως διαχειριζόμενοι managers (Fremantle 2015).

IDENTITY & ACCESS MANAGEMENT

Το τελευταίο επίπεδο που θα εξετάσουμε ίσως είναι και εκείνο που για την παρούσα διπλωματική είναι το πιο σημαντικό. Το επίπεδο αυτό δεν είναι άλλο από το επίπεδο διαχείρισης ταυτότητας και πρόσβασης. Στο επίπεδο αυτό παρέχονται οι ακόλουθες υπηρεσίες (Fremantle 2015).

- Έκδοση & Επικύρωση του OAuth2
- Άλλες Υπηρεσίες ταυτότητας όπως SAML2 SSO και OpenID Connect για εντοπισμό εισερχομένων αιτημάτων από επίπεδο WEB
- Διαχείριση πολιτικής για έλεγχό
- Κατάλογος Χρηστών

2.6 Βασικές Τεχνολογίες IoT

Σε αυτό το υποκεφάλαιο θα αναλυθούν οι βασικές τεχνολογίες που χρησιμοποιούνται σε ένα διαδίκτυο των αντικειμένων σε συνδυασμό με την αρχιτεκτονική που παρουσιάστηκε στο προηγούμενο

Στο χαμηλότερο στρώμα συναντάμε διαφόρων ειδών κόμβων και αισθητήρων όπως RFID, ενεργοποιητές και έξυπνες συσκευές ανίχνευσης οι οποίοι χρησιμοποιούνται για τον εντοπισμό των αντικειμένων. Οι συσκευές αυτές συλλέγουν τα δεδομένα και τα στέλνουν στο ανώτερο επίπεδο. Στο στρώμα αυτό συναντάμε το πρωτόκολλο IEEE 802.15.4 όπου είναι υπεύθυνο για τον έλεγχο πρόσβασης πολυμέσων για τα ασύρματα δίκτυα. Στόχο του έχει την επικοινωνία χαμηλής ταχύτητας και κατανάλωσης όμως μπορεί να χρησιμοποιηθεί συνδυαστικά με το 6LoWPAN που βασίζεται σε IPv6.

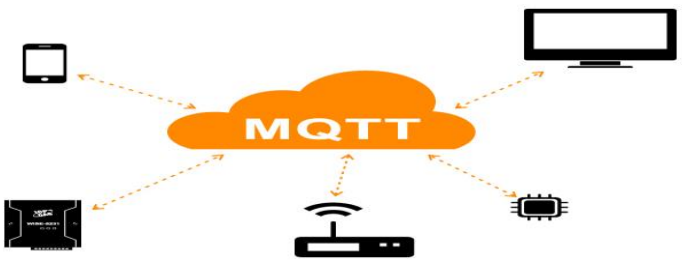
6LoWPAN (Πρωτόκολλο Υπηρεσίας)

Εν συνεχεία, το στρώμα δικτύου μεταδίδει τα δεδομένα στο ανώτερο επίπεδο με το πρωτόκολλο που ήδη αναφέρθηκε το 6LoWPAN που στόχο έχει την χαμηλή κατανάλωση καθώς οι απαιτήσεις των συσκευών είναι αυτές λόγω της περιορισμένης ενεργειακής κατανάλωσης των κόμβων και των αισθητήρων. Μάλιστα αποτελούν και μια μελλοντική πρόκληση η ακόμη μικρότερη κατανάλωση καθώς αμέσως καταλαβαίνουμε ότι δεν είναι εφικτό ένα μικροσκοπικό αισθητήριο το οποίο θα πρέπει να λειτουργήσει για μεγάλο χρονικό διάστημα να διαθέτει μια μεγάλη μπαταριά. (Vohra & Srivastava, 2015)

Στο ανώτερο στρώμα που είναι αυτό των εφαρμογών πριν τα devices συναντάμε πολλά πρωτόκολλα όπως το CoAP, όπως το MQTT, το AMQP αλλά και το XMPP. Όλα τα προαναφερόμενα πρωτόκολλα αποτελούν το στρώμα εφαρμογής. Παρακάτω δίνονται πληροφορίες για τα πρωτόκολλα αυτά.

MQTT (Πρωτόκολλο Εφαρμογής)

Πρόκειται για ένα ελαφρύ πρωτόκολλο επικοινωνίας μεταξύ μηχανής προς μηχανή. Τρέχει πάνω από TCP και είναι ένα ασύγχρονο πρωτόκολλο δημοσίευσης / εγγραφής που μειώνει το εύρος ζώνης του δικτύου. Μεγάλες εφαρμογές όπως το Facebook Massenger χρησιμοποιούν το πρωτόκολλο αυτό καθώς έχει ελάχιστες καθυστερήσεις και εξασφαλίζει τη μικρή χρήση μπαταρίας (Μιχαήλ 2019).



Εικόνα 6 - Πρωτόκολλο MQTT

CoAP (Πρωτόκολλο Εφαρμογής)

Το CoAP εξασφαλίζει παραπάνω αξιοπιστία από το MQTT παρέχοντας ένα δυναμικό QoS. Σχεδιάστηκε βασιζόμενο σε HTTP γεγονός που το καθιστά δια-λειτουργικό. Πρέπει να αναφερθεί ότι το CoAP τρέχει πάνω από UDP υποστηρίζοντας unicast αλλά και multicast (Μιχαήλ 2019).

XMPP (Πρωτόκολλο Εφαρμογής)

Το XMPP (πρωτόκολλο επεκτάσιμων μηνυμάτων & παρουσίας) έχει σχεδιαστεί με την προοπτική να επικοινωνεί σχεδόν σε πραγματικό χρόνο και να λειτουργεί μέσω TCP. Αντιθέτως, με το CoAP δεν υποστηρίζει QoS (Μιχαήλ 2019).

AMQP (Πρωτόκολλο Εφαρμογής)

Το AMQP είναι ένα πρωτόκολλο εφαρμογής στο IoT που έχει ως βασικό γνώμονα τα μηνύματα. Είναι σε θέση να παρέχει αξιόπιστη επικοινωνία μέσω αποστολής μηνυμάτων με διάφορες τεχνικές. Το AMQP μπορεί να συνεργαστεί μόνο με πρωτόκολλα όπως το TCP που είναι φερέγγυα για την ανταλλαγή αυτών των μηνυμάτων. Το πρωτόκολλο υποστηρίζει δυο είδη μηνυμάτων. Αυτά που παρέχονται από τον αποστολέα και δεν υπάρχει κάποιο σχόλιο σαν ετικέτα και αυτά που τα βλέπει ο παραλήπτης που έχουν ετικέτα σχόλιου (Μιχαήλ 2019).

RPL (Πρωτόκολλο Υποδομής)

Το RPL είναι ένα πρωτόκολλο δρομολόγησης για ασύρματα δίκτυα. Το RPL είναι ομολογουμένως αρκετά ευάλωτο σε απώλεια πακέτων αλλά το μεγάλο ατού που έχει, είναι ότι πρόκειται για ένα πρωτόκολλο χαμηλής κατανάλωσης ρεύματος. Είναι βασισμένο στην δομή του IEEE 802.15.4 και χρησιμοποιεί DODAG μηνύματα για να λειτουργήσει (Μιχαήλ 2019).

BLE (Πρωτόκολλο Υποδομής)

Το BLE που ήδη αναφερθήκαμε σε προηγούμενα κεφάλαια είναι ένα «έξυπνο» Bluetooth που χρησιμοποιεί ραδιοσήματα μικρής εμβέλειας και ελάχιστης κατανάλωσης ισχύος για ικανοποιητικό χρονικό διάστημα. Ας αναλογιστούμε ότι μπορεί να λειτουργήσει με ισχύ μετάδοσης από 0,01mW έως 10mW. Αυτό αυτομάτως το καθιστά ιδανικό υποψήφιο για εφαρμογές IoT (Μιχαήλ 2019).

2.7 Μοντέλα επίθεσης στο IoT

Το IoT χρησιμοποιεί στην βάση του πολλές ειδών τεχνολογίες όπως το πρωτόκολλο IPv6, το 6LoWPAN, το Bluetooth, το NFC, το Zigbee και πολλά ακόμα. Τεχνολογίες όπως το SND ή το ICN είναι εκείνες που ορίζουν για το ποτέ το πως θα επιτευχθεί μια επικοινωνία αναμεσά στο device και στην υποδομή.

Μπορούμε αμέσως να φανταστούμε ότι όταν συνδυάζοντας τόσα πολλά εργαλεία μαζί που ναι μεν διευκολύνουν την ζωή μας είναι σαφώς πιο δύσκολο να πέτυχουμε την ασφάλεια που απαιτείται για τα δεδομένα μας. Οι προαναφερθείσες τεχνολογίες έχουν και εκείνες τα τρωτά τους σημεία. Τα τρωτά αυτά σημεία λοιπόν ουσιαστικά κληρονομούνται από το IoT συστήματα εφόσον γίνεται χρήση τους. Δεν πρέπει να ξεχνάμε ότι τα device του IoT διαθέτουν συνήθως μικρούς πόρους όπως πχ ενεργειακή κατανάλωση οπότε δεν είναι εφικτή να χρησιμοποιούνται εξελιγμένη μηχανισμοί ασφάλειας (Chen et al. 2016; Al-Sarawi et al. 2017; Liu et al. 2018)

Έτσι λοιπόν, στα IoT έχουμε απειλές σε φυσικό επίπεδο, στο επίπεδο δικτύου, στο επίπεδο μεταφοράς, στο επίπεδο εφαρμογής αλλά και κρυπτογράφησης (Chen et al. 2016; Al-Sarawi et al. 2017; Liu et al. 2018).

Οι επιθέσεις αφορούν δράσεις οι οποίες υφίστανται με κυριότερο στόχο να καταφέρουν να δημιουργήσουν σημαντικά προβλήματα σε ένα σύστημα είτε με στόχο να διακόψουν τη σχεδιασμένη του δράση, εκμεταλλεύοντας ορισμένες ευπάθειες, κάνοντας χρήση διαφορετικές μεθόδων και μέσων. Οι επιτιθέμενοι υλοποιούν επιθέσεις, προκειμένου να επιτύχουν καθορισμένους σκοπούς είτε ακόμα και για προσωπικό όφελος είτε ακόμα και ευχαρίστηση (Hassan 2018).

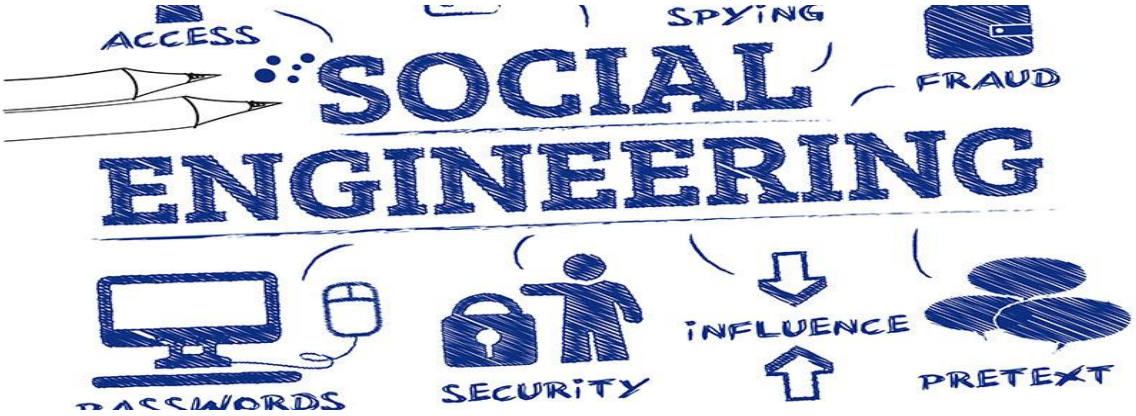
Η ποσότητα της προσπάθειας που καταβάλλεται από τον εκάστοτε επιτιθέμενο έχει άμεση σχέση με την πείρα που έχει, τα μέσα τα οποία χρησιμοποιεί είτε το κίνητρό του. Μια επίθεση είναι δυνατόν να λάβει αρκετές και διαφορετικές μορφές, όπως είναι για παράδειγμα η επίθεση στο δίκτυο με στόχο τον έλεγχο των δεδομένων είτε την αποκρυπτογράφηση των μηνυμάτων, κάνοντας χρήση ορισμένων αδυναμιών κλπ (Greengard 2015).

2.7.1 Φυσική επίθεση

Στην περίπτωση της φυσικής επίθεσης, οι εισβολείς έχουν πιθανότατα άμεση πρόσβαση στις συσκευές. Το «Social Engineering» είναι μια από τις πιο διαδεδομένους μεθόδους για πρόσβαση των επιτιθέμενων στις συσκευές.

Αυτή η πρόσβαση κυμαίνεται από υλική ζημιά στην συσκευή μέχρι κάποια «Slide Attack». Με τον όρο side attack στην ασφάλεια των υπολογιστών εννοούμε μια οποιαδήποτε επίθεση μέσω καναλιού που βασίζεται σε πληροφορίες που αποκτήθηκαν μέσω κάποιων εφαρμογών ενός συστήματος και στην προκείμενη περίπτωση device IoT. Στα side attack συγκαταλέγονται οι επιθέσεις : Cache – Timing – Powe Monitoring – Acoustic – Electromagnetic και άλλες.

Λόγω των τρόπων που υλοποιούνται οι φυσικές επιθέσεις στα IoT είναι δεδομένη η εμπλοκή του χρήστη στο Social Engineering. Με τον όρο Social Engineering εννοούμε την απόσπαση πληροφοριών και την χειραγώγηση των ατόμων που την κατέχουν (Salameh et al. 2018; Sadeghi et al. 2015; Liu et al. 2018).



Εικόνα 7 - Social Engineering

Επιπροσθέτως, οι επιτιθέμενοι συνήθως βρίσκονται σε κοντινή απόσταση με την συσκευή όπου και προκαλούν «βλάβη» σε hardware. Αυτό ισοδυναμεί με μείωση της διάρκειας ζωής της συσκευής ή θέτοντας σε κίνδυνο τον μηχανισμό επικοινωνίας της συσκευής με άλλες.

Άξιο αναφοράς είναι ότι οι φυσικές επιθέσεις μπορεί να μην προκαλέσουν άμεσα ζημιές στα IoT Devices αλλά έμμεσες. Δηλαδή, μια φυσική επίθεση μπορεί να έχει σκοπό την απενεργοποίηση κάποιας δικλίδας ασφαλείας όπως πχ απενεργοποίηση συναγερμού σε περίπτωση ανάγκης που εν τέλη αυτό θα οδηγήσει ίσως και σε χειρότερο αποτέλεσμά. (Patil and Seshadri 2014; Sadeghi et al. 2015; Liu et al. 2018).

Ακόμα χειρότερο όλων μπορεί να εννοηθεί ότι είναι η διασπορά και η διαρροή ευαίσθητων προσωπικών δεδομένων μετά από μια τέτοια επίθεση (Patil and Seshadri 2014; Sadeghi et al. 2015; Liu et al. 2018).

Άλλη περίπτωση ζημίας είναι όταν υπάρχει πρόσβαση στις συσκευές μέσω ενός κακόβουλου κόμβου. Εκεί ο επιτιθέμενος μπορεί να προκαλέσει ζημιά ακόμα και στα ανωτέρα στρώματα αφού θα έχει αποκτήσει έμμεση πρόσβαση και σε αυτά. Εννοείται ότι μπορούν να τροποποιηθούν οι πίνακες δρομολογήσεις και τα κλειδιά ασφαλείας υπερ του επιτιθεμένου σε μια τέτοια περίπτωση (Patil and Seshadri 2014; Sadeghi et al. 2015; Liu et al. 2018).

Η πεμπτουσία της επικοινωνίας αναμεσά σε δυο IoT devices είναι η αυθεντικοποίηση. Μέσω των φυσικών επιθέσεων μπορούν να γίνουν αναταραχές των συχνοτήτων οι οποίες με την σειρά τους μπορεί ακόμα και να αρνηθούν την πρόσβαση σε ένα εξουσιοδοτημένο χρήστη ή την επικοινωνία του με κάποιον τρίτο. Αυτό καλείται ως άρνηση υπηρεσίας (Patil and Seshadri 2014; Sadeghi et al. 2015; Liu et al. 2018).

Τέλος, πρέπει να μην ξεχνάμε ότι τα devices δεν έχουν περιθώριο για σπάταλη και κατακερματισμό της διαθέσιμης ενέργειας. Μέσω της φυσικής επίθεσης οι επιτιθέμενοι μπορούν να διαμορφώσουν τους κόμβους ενός IoT Network και να τους διατηρούν συνεχόμενα «ξύπνιος» αντί να βρίσκονται σε αδράνεια ώστε να εξαντληθεί η μπαταριά. Η επίθεση αυτή αναφέρεται ως «επίθεση στέρησης ύπνου» (Patil and Seshadri 2014; Sadeghi et al. 2015; Liu et al. 2018).

2.7.2 Επίθεση στο Link Layer

Οι παρεμβολές αυτής της μορφής είναι περίπλοκες και δεν είναι ενεργειακά αποδοτικές σε σύγκριση με τους αναστολείς φυσικού στρώματος. Ο στόχος αυτής της επίθεσης είναι πακέτα δεδομένων, ενώ στο φυσικό επίπεδο ο στόχος είναι οποιοδήποτε πακέτο. Όπως περιγράφεται από αυτήν την επίθεση στο επίπεδο σύνδεσης είναι πιο δύσκολο να εντοπιστεί. Σημειώστε ότι, το μπλοκάρισμα του επιπέδου σύνδεσης μπορεί επίσης να εστιάσει στο σήμα ελέγχου, όπως το μήνυμα ACK.

Τα συγκεκριμένα jammers ονομάζονται κατασκευαστές σύγκρουσης. Το jammer layer layer προσπαθεί να μπλοκάρει τα πακέτα δεδομένων. Δεδομένου ότι υπάρχουν διαφορετικοί τύποι πρωτοκόλλου MAC, το jammer πρέπει να εμπλακεί με βάση τον τύπο του πρωτοκόλλου MAC στο WSN. Η πρόκληση για το μπλοκάρισμα επιπέδου συνδέσμου είναι να προβλέψουν την άφιξη των πακέτων δεδομένων (El Mouaatamid et al. 2016).

2.7.3 Επίθεση στο επίπεδο δικτύου

Το εν λόγω επίπεδο, είτε ενσύρματα είτε ενσύρματα εκτίθεται σε αρκετές μορφές επιθέσεων. Εξαιτίας των ασύρματων καναλιών, οι επικοινωνίες είναι δυνατόν να ελέγχονται από κακόβουλους χρήστες. Το επίπεδο αυτής της μορφής διακρίνεται σε 3 είδη, όπως είναι η πιστοποίηση/επαλήθευση, η ασφάλεια δρομολόγησης και η προστασία δεδομένων (Hassan 2018).

Τα δίκτυα σε αυτές τις περιπτώσεις δέχονται επίθεση από Node Capture, Node Subversion, Node Malfunctioning, Message Corruption και από Routing Attacks. Η

λειτουργία του επιπέδου δικτύου δρομολογεί. Το επίπεδο δικτύου αποτελείται από το ασύρματο δίκτυο αισθητήρων (WSN) που μεταδίδει τα δεδομένα από τον αισθητήρα στον προορισμό του. Στα ασύρματα δίκτυα, οι κόμβοι μπορούν να κινούνται ελεύθερα, μπορούν να συμμετέχουν ή να αποχωρούν από το δίκτυο ανά πάσα στιγμή χωρίς καμία προηγούμενη πιστοποίηση (Somasundaram and Selvam 2018).

2.7.4 Επίθεση στο επίπεδο μεταφοράς

Το επίπεδο μεταφοράς είναι υπεύθυνο για τη διεργασία παράδοσης, όπου τα πρωτόκολλα μεταφοράς επιτρέπουν στις διαδικασίες να ανταλλάσσουν δεδομένα. Στο πλαίσιο του IoT, τα παραδοσιακά ζητήματα ασφάλειας επιπέδου μεταφοράς εξακολουθούν να υφίστανται. Η πιο σοβαρή επίθεση σε αυτό το επίπεδο είναι η επίθεση DoS που πνίγει το δίκτυο και οδηγεί σε άρνηση παροχής υπηρεσιών στις εφαρμογές. Αξίζει να σημειωθεί ότι λόγω της φύσης του IoT, τα παραδοσιακά πρωτόκολλα TCP και UDP δεν κλιμακώνονται με συσκευές περιορισμένης χρήσης πόρων, και επομένως στη βιβλιογραφία έχουν προταθεί ελαφρές εκδόσεις πρωτοκόλλων μεταφοράς. Ωστόσο, η ασφάλεια αυτών των πρωτοκόλλων είναι πρωταρχικής σημασίας για την ανακούφιση των DoS και επιθέσεις DDoS στο IoT (Hussain et al. 2020).

Το εν λόγω επίπεδο, είναι εκείνο το οποίο προσφέρει ένα περιβάλλον πρόσβασης για το επίπεδο αντίληψης, τη μετάδοση δηλαδή των δεδομένων είτε την αποθήκευσή τους και με στόχο τη χρησιμοποίησή τους από τις εφαρμογές ανώτερου επιπέδου. Το συγκεκριμένο επίπεδο είναι εφικτό σύμφωνα με τις δράσεις του να διακριθεί σε δίκτυο πρόσβασης, σε δίκτυο κορμού και τοπικά δίκτυα (Boulogeorgos et al. 2017).

2.7.5 Πολύ επίπεδες επιθέσεις

Εκτός από τις παραπάνω επιθέσεις, υπάρχουν και οι πολυεπίπεδες επιθέσεις. Αυτές οι επιθέσεις περιλαμβάνουν ανάλυση κυκλοφορίας, επιθέσεις δευτερεύοντος καναλιού, επιθέσεις επανάληψης, επιθέσεις man-in-the-middle και επιθέσεις πρωτοκόλλου. Οι επιθέσεις ανάλυσης κυκλοφορίας, για παράδειγμα είναι παθητικές επιθέσεις όπου οι εισβολείς ακούνε παθητικά την κίνηση και προσπαθούν να βγάλουν νόημα από αυτήν (Βελλισάρης 2017).

Αυτές οι επιθέσεις είναι πολύ δύσκολο να μετριαστούν, επειδή τα μέρη που επικοινωνούν συνήθως δεν έχουν ιδέα ότι παρακολουθείται η κυκλοφορία τους. Οι εισβολείς αναζητούν ενδιαφέρουσες πληροφορίες στην κίνηση στο Διαδίκτυο, όπως τα προσωπικά στοιχεία των χρηστών, τα στοιχεία της επιχειρηματικής λογικής, τα διαπιστευτήρια και άλλες πληροφορίες που έχουν οποιαδήποτε αξία για τον εισβολέα. Εκτός αυτού, η ασφάλεια μεταφοράς δεδομένων είναι επίσης υψίστης σημασίας στο IoT. Τα δεδομένα που παράγονται στο περιβάλλον IoT χρησιμοποιούνται για σκοπούς λήψης αποφάσεων. Ως εκ τούτου, είναι απαραίτητο να διασφαλιστεί η ποιότητα των δεδομένων (Hussain et al. 2020).

ΚΕΦΑΛΑΙΟ 3 – Δίκτυα 5G

3.1 Ιστορική Αναδρομή δικτύων

Στο προηγούμενο κεφάλαιο εξετάσαμε ενδελεχώς τον κόσμο του IoT. Στο κεφάλαιο 3 της διπλωματικής θα πραγματευτούμε κάτι που είναι αλληλένδετο με το διαδίκτυο των αντικειμένων, το 5G. Πριν απ' αυτό όμως θα γίνει μια ιστορική αναδρομή για το πως έχουμε φτάσει εν έτη 2020 στα δίκτυα 5G (Brain Bridge 2020).

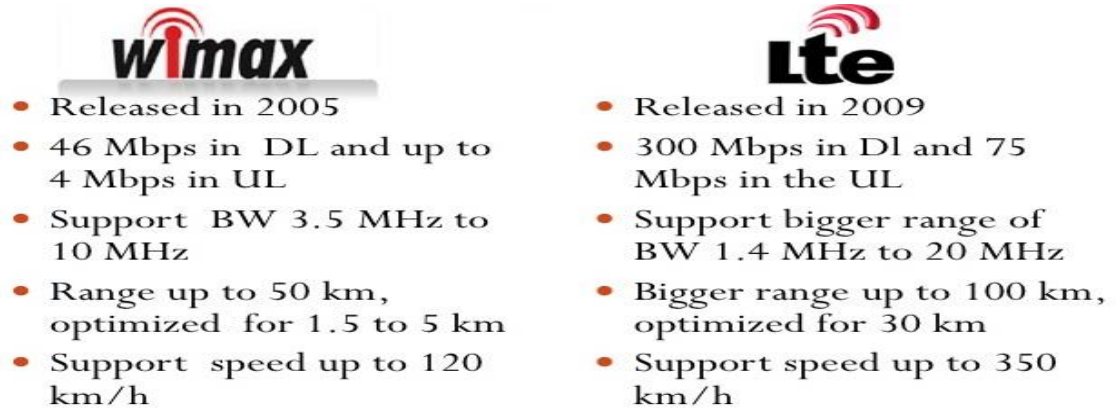
Το 1G δημιουργήθηκε την περίοδο του '83. Εκείνη την περίοδο όλες οι ασύρματες επικοινωνίες ήταν φωνητικές. Την περίοδο του '66, το Bell Labs έλαβε την απόφαση να εφαρμόσει αναλογικά συστήματα για ένα κινητό σύστημα τεράστιας για εκείνη την εποχή χωρητικότητας. Αυτός ήταν και ο βασικότερος λόγος που τα ψηφιακά ραδιοσυστήματα ήταν εξαιρετικά ακριβά. Πριν από την περίοδο εκείνη οι ασύρματες επικοινωνίες ήταν φωνητικές και ως επί το πλείστον γινόταν χρήση αναλογικών συστημάτων με μονοδιάστατη διαμόρφωση (Μίντης 2018). Το 1G κυκλοφόρησε για πρώτη φορά στην Ιαπωνία ενώ η Motorola ήταν εκείνη που λάνσαρε το πρώτο συμβατό κινητό. (Wikipedia 2020; Brain Bridge 2020).

Εικόνα 8 - Κινητό 1G

Πιστεύω ότι είναι απολύτως λογικό να αναλογιστούμε ότι η τεχνολογία της γενιάς αυτής ήταν αρκετά προβληματική αντιμετωπίζοντας προβλήματα κακής ποιότητας. Αλλά προβλήματα στο προσκήνιο ήταν η μη αποδοτικοί αλγόριθμοι κρυπτογράφησης με το σοβαρότερο όμως πρόβλημα να αντιμετωπίζεται στην μη υποστήριξη της περιαγωγής λόγω συχνοτήτων (Brain Bridge 2020).

Φτάνοντας στο 1991, έχουμε φύγει πλέον από το προβληματικό 1G και έχουμε εισαχθεί σε μια κάπως πιο ψηφιακή κατάσταση. Εκείνη την εποχή, όλες οι ασύρματες επικοινωνίες ήταν φωνητικές. Το διεθνές GMS αποτέλεσε ένα ψηφιακό σύστημα, το οποίο έκανε χρήση πολυπλεξίας TDMA. Δεδομένου πως η AT&T πωλήθηκε σχεδόν μια δεκαετία πριν, κανένας άλλος ερευνητικός οργανισμός δεν είχε την ευχέρεια να αναπτύξει ένα τόσο αναπτυγμένο σύστημα αυτής της γενιάς και για το σύστημα 1G στη Βόρεια Αμερική (Holma et al. 2020). Το IS-54 δεν ήταν επιθυμητό και για αυτό το λόγο δεν προχώρησε. Στη συνέχεια το GSM έλαβε την τελική του ονομασία που ήταν 2G. Η μετάβαση από την προηγούμενη γενιά σε αυτή σήμανε επί της ουσίας τη μετάβαση από τα αναλογικά στα ψηφιακά συστήματα. Σχεδόν 5 χρόνια αργότερα αναπτύχθηκε το 2,5G. Εκείνη την περίοδο όλες οι ασύρματες επικοινωνίες ήταν κατά κύριο λόγο για φωνή υψηλότερης χωρητικότητας με περιορισμένες, όπως υπηρεσίες δεδομένων. Το σύστημα CDMA το οποίο έκανε χρήση 1,25MHZ εύρους ζώνης εφαρμόστηκε στις ΗΠΑ (Penttinen 2019; Brain Bridge 2020).

Αφού πλέον είχε κατοχυρωθεί δια τηλεφώνου μετά βεβαιότητας και δια της ελάχιστης αυτής πλοήγησης που υπήρχε στο διαδίκτυο στις συσκευές 2G δημιουργήθηκε η ανάγκη για την ταχύτερο ρυθμό μετάδοσης. Κάπως έτσι τέθηκε σε εφαρμογή την περίοδο του '99 και αναπτύχθηκε το 3G. Εκείνη την εποχή, οι ασύρματες επικοινωνίες είχαν φωνή αλλά και πληροφορίες. Η γενιά αυτής της μορφής ήταν το 1ο διεθνές τυποποιημένο σύστημα το οποίο κυκλοφόρησε από την ITU. Τα δίκτυα αυτά εκμεταλλεύτηκαν το WCDMA κάνοντας χρήση εύρους ζώνης σχεδόν 5MHz. Το δίκτυο αυτό δρούσε σε FDD αλλά και σε TDD. Επομένως, είναι δυνατόν να τονιστεί πως κατά τη μετάβαση από την προηγούμενη γενιά σε αυτή υλοποιήθηκε η εξέλιξη από φωνητικά συστήματα σε συστήματα που εστίαζαν στα δεδομένα (Greengard, 2015). Είχε ως κύριο μέλημα του την ταχύτερη μεταφορά δεδομένων αλλά και την κάλυψη της οποιαδήποτε εμβελείας επιδιωκόταν. Υπήρχε η δυνατότητα επικοινωνίας με emails και βιντεοκλήσεις αφού η αμφίδρομη επικοινωνία είχε εξασφαλιστεί χωρίς μάλιστα να μειώνει την ικανοποιητική ποιότητα του ρυθμού (Αγγιστριώτης 2020; Brain Bridge 2020).



Εικόνα 9 - Σύγκριση WiMax & LTE

Στη συνέχεια και συγκεκριμένα την περίοδο του 2013 αναπτύχθηκε η επόμενη γενιά. Πρόκειται για συστήματα ταχύτητας δεδομένων υψηλότερων ταχυτήτων και φωνής. Υφίστανται δυο είδη αυτής της γενιάς. Για παράδειγμα, οι ΗΠΑ έχουν δημιουργήσει το WiMAX κάνοντας χρήση ορθογώνιας πολυπλεξίας διαίρεσης συχνότητας ενώ την ίδια ώρα υφίσταται και το σύστημα LTE, το οποίο δημιουργήθηκε μετέπειτα. Το εύρος ζώνης και των δυο παραπάνω συστημάτων είναι 20MHz. (Βελλισάρης 2017). Στην πορεία υπήρξαν συνεχόμενες βελτιώσεις με την βασική να είναι η επέκταση του LTE-A (LTE Advanced) το οποίο παρέχει βασικούς μηχανισμούς για να μεγαλώνει το εύρος του συχνοτικού φάσματος. Το LTE-A αποτελεί ίσως το πρώτο πρωτόκολλο που μπορεί να γίνει αποδεκτό ως ένα αυτούσιο πρωτόκολλο για δίκτυο 4G. Ένα από τα μεγάλα θετικά του 4G είναι ότι δεν εγκαθιδρύει νέες εγκαταστάσεις υλικού αλλά πάτησε στις πάνω ήδη υπάρχουσες. Το 4G όπως ήδη έγινε κατανοητό έχει μεγάλη ταχύτητα πιο ποιοτική αλλά μεταξύ των άλλων ήδη συναντάμε αυξημένη ασφάλεια (Net-informations 2020; Brain Bridge 2020).

3.2 Απαιτήσεις & Υπηρεσίες δικτύων 5G

Εφαρμογές, όπως είναι για παράδειγμα η κινητή τηλεφωνία και το κινητό εύρος ζώνης έχουν σαν βασικότερο σκοπό την παροχή αποδοτικότερων υπηρεσιών επικοινωνίας. Από την άλλη μεριά, αρκετές από τις καινούριες εφαρμογές και περιστατικά χρήσης τα οποία οδηγούν τις ανάγκες και τις δυνατότητες αυτών των δικτύων, είναι από άκρο σε άκρο μεταξύ συστημάτων, με βασικότερη συνέπεια τις περισσότερες φορές να ονομάζονται επικοινωνία τύπου-μηχανής (Ahmad et al. 2019).

Παρά το γεγονός πως εκτείνονται σε ένα μεγάλο φάσμα διαφοροποιημένων εφαρμογών, οι εφαρμογές τύπου μηχανής έχουν την ευχέρεια να διακριθούν σε δυο βασικές ομάδες που είναι η μαζική και η κρίσιμη, σύμφωνα με τα βασικότερα γνωρίσματά τους και τις ανάγκες τους. Η μαζική χρησιμεύει σε περιστατικά κλιμακούμενης αλλά και ευέλικτης προσπέλασης και έχει να κάνει με υπηρεσίες οι οποίες τις περισσότερες φορές έχουν τη δυνατότητα να καλύψουν ένα τεράστιο σύνολο συστημάτων (όπως πχ αισθητήρες κ.λπ.) ενώ η κρίσιμη χρησιμεύει σε περιστατικά στα οποία χρειάζονται μικρότεροι χρόνοι μετάδοσης (Gallardo 2019).

Καθοριστικό ρόλο σε αυτά τα δίκτυα παίζουν οι υπηρεσίες Xmbb (προσφέρει αυξημένες ταχύτητες δεδομένων καθώς επίσης και βελτιωμένη ποιότητα υπηρεσιών), mMTC (προσφέρει συνδεσιμότητα για ένα τεράστιο σύνολο συστημάτων εξοικονόμησης κόστους και ισχύος) και η uMTC (έχει τη δυνατότητα να καλύψει τις απαιτήσεις για υπηρεσίες που είναι αξιόπιστες και χρονικά κρίσιμες) (Penttinen 2019).

Οι παραπάνω υπηρεσίες εμφανίζουν διαφοροποιημένες ανάγκες σε ό,τι έχει να κάνει με τους ελάχιστους ρυθμούς δεδομένων, την βέλτιστη εφικτή κάλυψη, το μέγεθος του πακέτου δεδομένων κλπ. Κατά την ανάπτυξη μιας καινούριας υπηρεσίες, δεν θα χρειάζεται η αγορά καινούριου φάσματος συχνοτήτων και η ανάπτυξη μιας καθορισμένης ασύρματης πρόσβασης, καθώς χρησιμοποιώντας τα δίκτυα που μελετάμε σε αυτό το κεφάλαιο θα έχουμε την ευχέρεια να εισάγουμε καινούριες υπηρεσίες διαμέσου επαναχρησιμοποίησης κοινών συνιστωσών, όπως είναι για παράδειγμα η διαχείριση της φορητότητας, η λειτουργικότητα κ.λπ. (Holma et al. 2020).

3.3 Εργαλεία & Χαρακτηριστικά υπηρεσιών 5G

Τα κυριότερα εργαλεία για την ανάπτυξη αυτών των συστημάτων είναι το λεπτό επίπεδο ελέγχου συστήματος (προσφέρει αποδοτικά καινούρια δεδομένα σηματοδότησης και εποπτείας που είναι καθοριστικές με στόχο να διασφαλιστεί η αξιοπιστία, η ευελιξία κ.λπ.) και το δυναμικό RAN (αποτελεί μια αναθεώρηση των κλασσικών υποδομών ασύρματης πρόσβασης, προκειμένου να περιέχει δυναμικά δεδομένα όπως είναι για παράδειγμα η ραγδαία ανάπτυξη σημείων πρόσβασης κλπ) (Μίντης 2018).

Εξίσου σημαντικά και διαδεδομένα εργαλεία σε αυτές τις περιπτώσεις λογίζονται πως είναι οι τοπικές ροές περιεχομένων και κυκλοφορίας (το εν λόγω εργαλείο προσφέρει την ευχέρεια συγκέντρωσης αλλά και διανομής σε πραγματικό χρόνο των αποθηκευμένων

περιεχομένων) αλλά και η εργαλειοθήκη φάσματος (έχει να κάνει με αρκετές και διαφορετικές τακτικές οι οποίες προσφέρουν τη δυνατότητα σε αυτά τα δίκτυα να δρουν με πρωτοφανή ευελιξία φάσματος σε υφιστάμενες είτε ακόμα και καινούριες μπάντες, με διαφοροποιημένα σενάρια κατανομής φάσματος) (Ahmad et al. 2019).

Από την άλλη πλευρά, σε ό,τι έχει να κάνει με τα κυριότερα γνωρίσματα αυτών των δικτύων, είναι σημαντικό να επισημανθεί πως παρέχουν τεράστια ποσοστά δεδομένων μέχρι και 10bps. Η συγκεκριμένη τεχνολογία προσφέρει την ευχέρεια σε συστήματα τα οποία ταξιδεύουν μέχρι και 500ph να παραμένουν συνδεμένα στο δίκτυο (Μίντης 2018).

Ένα εξίσου καθοριστικό γνώρισμα είναι πως το σύνολο των διασυνδεδεμένων συστημάτων θα είναι σχεδόν τριπλάσιο όπως 1M σε ένα τετραγωνικό χιλιόμετρο. Οι χρήστες σε τοποθεσίες υπερκατανάλωσης, όπως είναι για παράδειγμα σε αεροδρόμια κ.λπ. θα έχουν την ευχέρεια να βιώσουν τις γρηγορότερες ταχύτητες και τη χαμηλότερη καθυστέρηση. Έτσι, τα συγκεκριμένα δίκτυα έχουν κατορθώσει να επεκτείνουν σε τεράστιο επίπεδο τις ευρυζωνικές ασύρματες υπηρεσίες που προσφέρουν στους σύγχρονος χρήστες εκτός από το κινητό διαδίκτυο IoT και σε κρίσιμα τμήματα επικοινωνιών (Penttinen 2019).

3.4 Αξιοπιστία συνδέσεων 5G

Τα εν λόγω συστήματα είναι σημαντικό να πληρούν καθορισμένες ανάγκες σε ό,τι έχει να κάνει με την αξιοπιστία τους, τη διαθεσιμότητά τους καθώς επίσης και την επίτρεψη διαφορετικών εφαρμογών, όπως είναι για παράδειγμα η ασφάλεια της κυκλοφορίας, τα αυτόματα συστήματα εποπτείας των τραίνων αλλά και διάφορες υπηρεσίες ηλεκτρονικής υγείας κλπ (Holma et al. 2020).

Μερικές εφαρμογές οδικής ασφάλειας έχουν ανάγκη από πακέτα δεδομένων τα οποία είναι σημαντικό να παραδοθούν με επιτυχία και με τεράστια πιθανότητα, σε καθορισμένη χρονική περίοδο. Σε περίπτωση αποτυχίας αυτών των πακέτων, υφίσταται η δυνατότητα επηρεασμού της υγείας των χρηστών σε ό,τι έχει να κάνει με την υπηρεσία της οδικής ασφάλειας. Επομένως, είναι ζωτικής σημασίας ο προσεκτικός σχεδιασμός του επιπέδου εφαρμογής καθώς επίσης και της ασύρματης σύνδεσης, με απώτερο στόχο να είναι εγγυημένη η βέλτιστη εφικτή ασφάλεια με ταυτόχρονη συντήρηση αποδεκτού κόστους (Gallardo 2019).

Ένα εξίσου σημαντικό παράδειγμα το οποίο έχει ανάγκη από uMTC είναι η βιομηχανική εποπτεία και έχει την ευχέρεια να διαχειριστεί διαφοροποιημένους τύπους κυκλοφορίας που έχουν σαν βασικό τους γνώρισμα την περιοδικότητα και τα μεμονωμένα στοιχεία αλλά και διάφορα μηνύματα διαμόρφωσης. Με την έννοια περιοδικά καλούμε τα στοιχεία αυτά τα οποία έχουν άμεση σχέση με εισόδους και εξόδους των αλγορίθμων εποπτείας και είναι σημαντικό να παραδοθούν με υψηλότερη αξιοπιστία, μέσα σε καθορισμένο χρονικό διάστημα (Tsiatsis et al. 2018).

Γενικότερα, ένα τυπικό πακέτο αυτής της μορφής τις περισσότερες φορές είναι μικρότερο και το εύρος ζώνης για κάθε κόμβο είναι εξαιρετικά χαμηλό. Με βασικότερο στόχο να υποστηριχθούν αξιόπιστες καθώς επίσης και με χαμηλότερη καθυστέρηση (μικρότερη από 10ms) συνδέσεις μέσα σε σχετικά μικρότερο εύρος, σε ασύρματα δίκτυα αυτής της μορφής θα γίνεται χρήση με στόχο την επικοινωνία D2D ελεγχόμενων δικτύων. Η χρησιμότητα δικτύων ευρείας περιοχής κάνει το συγκεκριμένο είδος επικοινωνίας εξαιρετικά διαφορετικά και καινοτόμο σχετικά με τις υπόλοιπες δράσεις διασύνδεσης μικρότερης εμβέλειας (Holma et al. 2020).

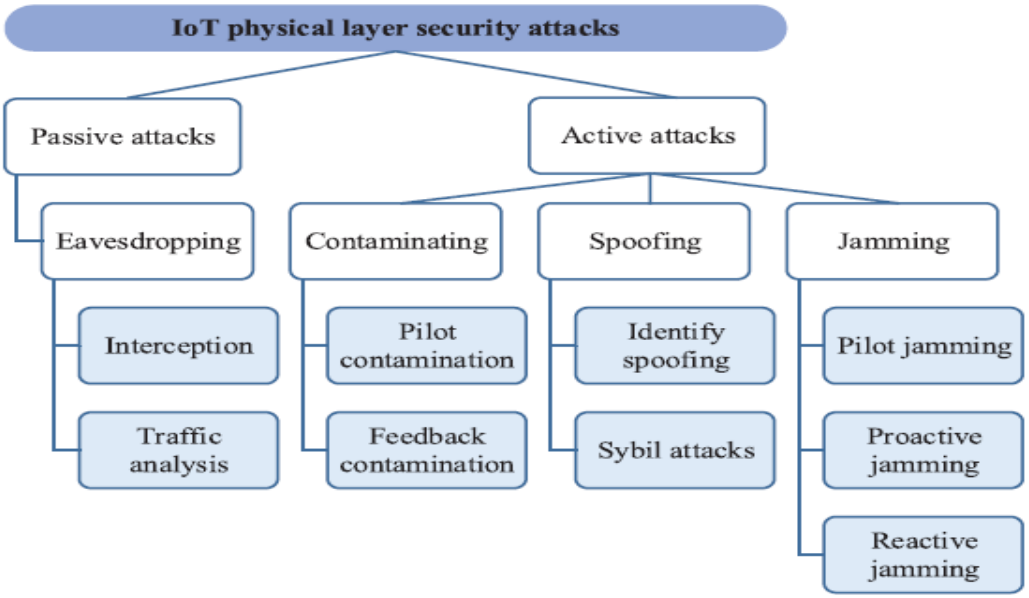
3.5 Ασφάλεια 5G

Οι τεχνολογίες ασύρματης επικοινωνίας 5G όχι μόνο θα μπορούσαν να ανοίξουν την πόρτα για απειλές φυσικού επιπέδου στα δίκτυα IoT, αλλά και να προσφέρουν νέες ευκαιρίες για τον μετριασμό των κινδύνων ασφαλείας. Από τη μία πλευρά, ορισμένες νέες ασύρματες τεχνικές 5G θα μπορούσαν να είναι πιο ευαίσθητες σε υπάρχουσες επιθέσεις φυσικού επιπέδου. Για παράδειγμα, οι μαζικές επικοινωνίες MIMO και NOMA είναι πολύ ευαίσθητες σε πιλοτικές επιθέσεις μόλυνσης (PCA). Από την άλλη πλευρά, ορισμένες απειλές φυσικού επιπέδου περιορίζονται από τεχνολογίες ασύρματης επικοινωνίας 5G. Για παράδειγμα, η ακτινοβολία σε μαζικό MIMO μπορεί να χρησιμοποιηθεί για τη μείωση του κινδύνου υποκλοπής (Wang et al., 2019)

Γενικότερα, είναι σημαντικό να γνωρίζουμε πως με το πέρασμα των ετών καθώς επίσης και την ραγδαία ανάπτυξη της τεχνολογίας το σύγχρονο υπολογιστικό περιβάλλον έχει σαν βασικότερο στόχο τα κινητά δίκτυα τα οποία έχουν σαν βασικό τους γνώρισμα τις υψηλότερες ταχύτητες μεταφοράς δεδομένων και την τεράστια κινητικότητα. Η καταλληλότερη τεχνολογία η οποία έχει αναπτυχθεί με κυριότερο σκοπό την καταπολέμηση αυτών των προβλημάτων είναι η τεχνολογία που μελετάμε σε αυτό το κεφάλαιο (Ahmad et al., 2019).

Η συγκεκριμένη τεχνολογία τα τελευταία έτη αναπτύσσεται με ραγδαίους ρυθμούς και αναμένεται να βελτιωθεί περισσότερο από εδώ και πέρα. Οι επικοινωνίες αυτής της μορφής έχουν σαν απώτερο στόχο την παροχή τεράστιων δεδομένων εύρους ζώνης, άπειρη δυνατότητα δικτύωσης αλλά και εκτεταμένη κάλυψη σήματος με κυριότερο σκοπό την υποστήριξη ενός μεγάλου φάσματος ειδικών υπηρεσιών υψηλότερης ποιότητας στους τελικούς χρήστες (Holma et al. 2020).

Αυτός ήταν και ο κυριότερος λόγος που οι εν λόγω επικοινωνίες θα ενσωματώσουν αρκετές από τις ισχύουσες προηγμένες τεχνολογίες και εφαρμογές και καινοτόμες τεχνολογίες και καινούριες τακτικές. Η συγκεκριμένη ολοκλήρωση θα οδηγήσει, όμως, σε μεγάλες προκλήσεις σε ό,τι έχει να κάνει με τον κλάδο της ασφάλειας για μελλοντικά δίκτυα κινητής τηλεφωνίας αυτού του είδους (Penttinen 2019).

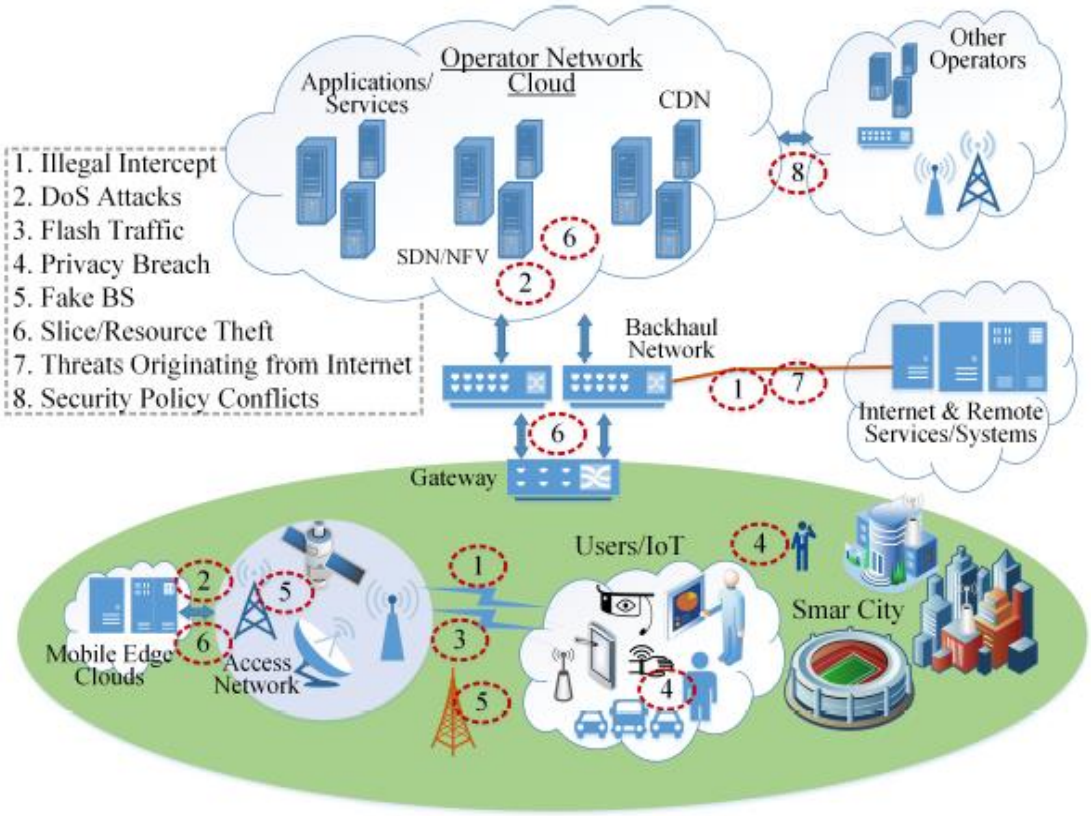


Εικόνα 10 - Απειλές ασφαλείας στο φυσικό επίπεδο του 5G-IoT

Πιο συγκεκριμένα, είναι εξαιρετικά πιθανόν ένα μεγάλο φάσμα ζητημάτων ασφαλείας να τεθεί σε δίκτυα αυτού του είδους εξαιτίας καθορισμένων παραμέτρων, οι οποίες ως επί το πλείστον περιέχουν την ανοικτή αρχιτεκτονική της IP η οποία βασίζεται στην IP 5G, την ποικιλομορφία των υποκείμενων τεχνολογιών δικτύου πρόσβασης του συστήματος αυτής της μορφής, την πληθώρα συνδεδεμένων συστημάτων επικοινωνίας, την ετερογένεια των συστημάτων, τα ανοικτά λειτουργικά συστήματά τους καθώς επίσης και τη χρησιμότητα αυτών των συστημάτων από μη επαγγελματίες χρήστες σε ό,τι έχει να κάνει με σοβαρά ζητήματα ασφαλείας (Μίντης 2018).

Επομένως, τα συστήματα αυτής της μορφής θα πρέπει να αντιμετωπίσουν πιο πολλές απειλές σε σχέση με τα σημερινά συστήματα αυτών των επικοινωνιών. Παρά το γεγονός αυτό, όμως, δεν είναι ακόμα εντελώς σαφές ποιες ακριβώς είναι οι σημαντικότερες απειλές και ποια δεδομένα δικτύου θα αποτελέσουν τεράστιο πρόβλημα.

Γενικότερα, τα μεγαλύτερα και τα πιο σοβαρά ζητήματα αυτής της μορφής κατά κύριο λόγο εντοπίζονται στον εξοπλισμό των χρηστών, στα δίκτυα πρόσβασης, στο κεντρικό δίκτυο κινητού επιχειρησιακού δικτύου, στον κορεσμό HSS, στα εξωτερικά δίκτυα IP, στα συμβιβασμένα επιχειρηματικά δίκτυα κλπ (Penttinen 2019).



Εικόνα 11 - Απειλές ασφαλείας στο δίκτυο 5G

Στην παραπάνω εικόνα βλέπουμε πιθανές επιθέσεις και απειλές σε δίκτυα 5G. Διαπιστώνουμε ότι υπάρχει μια γενικότερη διαδραστηκότητα και αλληλεπίδραση άρα και περισσότερες ευπάθειες.

ΚΕΦΑΛΑΙΟ 4 – Μηχανική Μάθηση

4.1 Η έννοια της μάθησης

Ο άνθρωπος από την στιγμή που θα γεννηθεί μέχρι την στιγμή που θα ολοκληρωθεί για εκείνον ο κύκλος ζωής του μαθαίνει συνεχώς και αδιάληπτος. Δεν θα ήταν καθόλου δύσκολο να μπορούσαμε να χαρακτηρίσουμε και ως μια μηχανή μάθησης. Από την στιγμή που ένα μωρό γεννηθεί με τις αισθήσεις που διαθέτει αρχίζει να «μαθαίνει» τον κόσμο μας, σε μετέπειτα ηλικία μαθαίνει να μιλάει, μαθαίνει να περπατάει, μαθαίνει να τρώει κλπ.

Ουσιαστικά δηλαδή, μιλάμε για την διαδικασία εμπέδωσης καινούργιων δεδομένων σε αντικείμενα και υποκείμενα ικανά προς αυτό με την ακόλουθη αντίστοιχη αλληλεπίδραση (Τζανάκος 2020; Σταματόπουλος 2020).

Η μάθηση θεωρείται ως μια από τις θεμελιώδεις ιδιότητες της νοήμονος συμπεριφοράς του ανθρώπου. Κατά καιρούς έχουν πραγματοποιηθεί ποικίλες μελέτες για την διαδικασία της μάθησης και αυτό γιατί όπως εύκολα μπορούμε να υποπτευθούμε δεν εμπίπτει μόνο σε έναν συγκεκριμένο κλάδο αλλά τουναντίον υπάρχει τόσο ποικιλομορφία ώστε η εντάξει τους σε μια και μοναδική κατηγορία δεν μπορεί να είναι βάσιμη και πλήρης (Σταματόπουλος 2020).

4.2 Ορισμός & Βασικά χαρακτηριστικά μηχανικής μάθησης

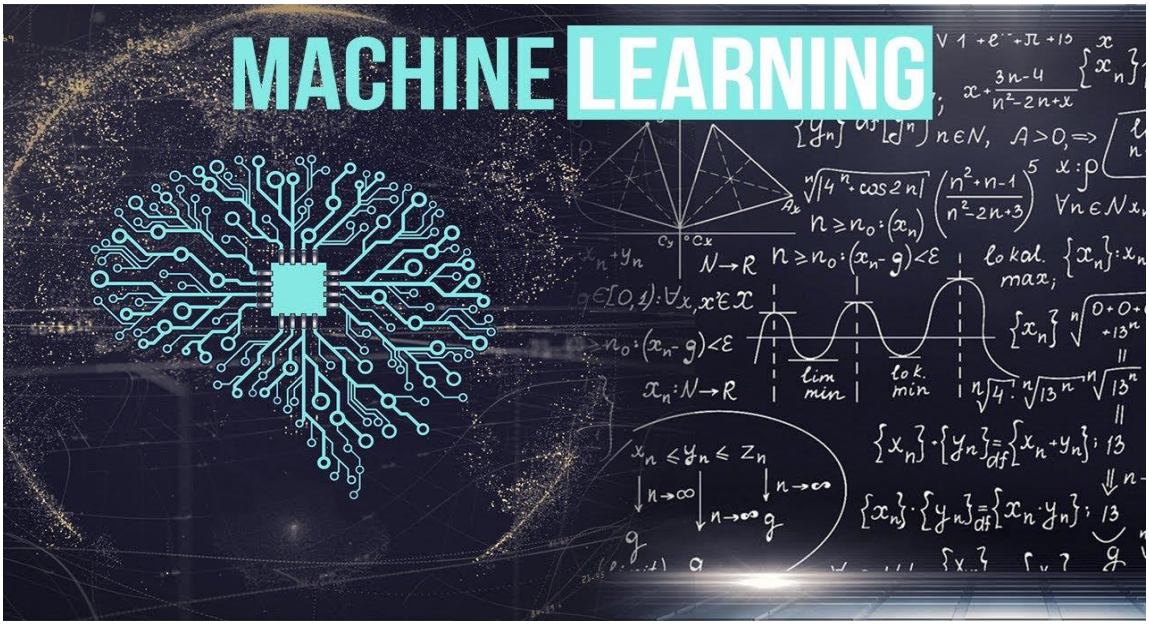
Είμαι πεπεισμένος ότι οι περισσότεροι μόλις αναρωτηθούν τι είναι επι της ουσίας η μηχανική μάθηση θα αποδώσουν μια εικόνα που φάνταζε ιδεατή κάποτε και δεν είναι άλλη από εκείνη την εικόνα ενός Η/Υ που μαθαίνει από τα λάθη του και μπορεί να τα διορθώσει υπολογίζοντας μέχρι και την παραμικρή λεπτομέρεια και προβλέποντας κάθε είδους αντίδραση. Πάρα ταύτα, η αλήθεια μπορεί να μην ορίζεται ακριβώς αυτή αλλά σίγουρα το πάνω σκηνικό που περιεγράφηκε δεν είναι τελείως ουτοπικό.

Η συγκεκριμένη μάθηση είναι ένα επιστημονικό πλαίσιο με αρκετές και διαφορετικές εφαρμογές οι οποίες κατά κύριο λόγο περιέχονται στον ευρύτερο τομέα της τεχνητής νοημοσύνης. Ο βασικότερος σκοπός αυτής της μάθησης είναι η βέλτιστη εφικτή κατανόηση της δομής των πληροφοριών καθώς επίσης και η μοντελοποίησή τους. Η διερεύνηση αυτής της περιοχής εστιάζει στην ανάπτυξη αλγορίθμων οι οποίοι προσφέρουν σε έναν Η/Υ την ευχέρεια να έχει τη δυνατότητα να μαθαίνει από πειραματικά στοιχεία, να εκπαιδεύεται στο να εκτελεί καθορισμένες δράσεις, να υλοποιεί προβλέψεις και να λαμβάνει αποφάσεις σε ό,τι έχει να κάνει με τις εν λόγω πληροφορίες (Chumachenko 2017).

Όπως το διαδίκτυο των πραγμάτων έτσι και η μηχανική μάθηση αποτελεί την σύγχρονη πραγματικότητα. Μέσω της μηχανικής μάθησης έχουμε την δυνατότητα να είμαστε πιο παραγωγικοί, πιο αποτελεσματικοί και διαθέτοντας ένα σωρό προτερήματα ως εφόδια με ότι αυτό συνεπάγεται.

Οι τακτικές αυτής της μάθησης ως επί το πλείστον έχουν σαν βασικό τους γνώρισμα διάφορους αυστηρούς μαθηματικούς αλγορίθμους είτε ακόμα και στατιστικές τακτικές ανάλυσης. Από τις πιο σημαντικές αλλά και διαδεδομένες στατιστικές τακτικές με κυριότερο σκοπό τη διερεύνηση της σχέσης ανάμεσα σε ποσοτικές μεταβλητές είναι η συσχέτιση αλλά και η παλινδρόμηση (Bonaccorso 2017).

Καθοριστικό ρόλο σε αυτές τις τακτικές παίζουν η συλλογή δεδομένων (η οποία κατά κύριο λόγο χρησιμεύει με στόχο την εκπαίδευση και την δοκιμή του εκάστοτε μοντέλου) αλλά και η προετοιμασία δεδομένων (οι πληροφορίες είναι ζωτικής σημασίας να οριοθετηθούν, δηλαδή να απομακρυνθούν πληροφορίες κακής ποιότητας, να κατηγοριοποιηθούν σε μια καθορισμένη ακολουθία και στο τέλος να μεταβληθούν, προκειμένου να εμφανίζουν μια ενιαία μορφή). Τα δυο γνωρίσματα που προαναφέρθηκαν τις περισσότερες φορές είναι εξαιρετικά χρονοβόρα αλλά και είναι ζωτικής σημασίας, μιας και αποτελούν την βάση πάνω στην οποία μετέπειτα αναπτύσσονται τα μοντέλα πρόβλεψης (Αποστολόπουλος 2020).



Εικόνα 12 - Μηχανική Μάθηση

Ένα εξίσου καθοριστικό γνώρισμα αυτής της μορφής είναι η επιλογή μοντέλου αυτής της μάθησης. Στο συγκεκριμένο επίπεδο υλοποιούνται οι δοκιμές και εν τέλει η επιλογή των κυριότερων μοντέλων που θα χρησιμεύσουν στην εκάστοτε περίσταση. Τα μοντέλα αυτής της μορφής είναι αρκετά και δεν υφίσταται σαφής ταξινόμηση ποιο

μοντέλο ταιριάζει σε ποια δράση (Τζανακός 2020).

Παρά το γεγονός αυτός στη σημερινή εποχή υφίστανται αποδεδειγμένες κατηγορίες μοντέλων που προτιμώνται για καθορισμένες δράσεις, όπως είναι για παράδειγμα οι μηχανές διανυσμάτων υποστήριξης είτε ακόμα και τα δέντρα αποφάσεων, τα οποία κατά κύριο λόγο ταιριάζουν σε ζητήματα ομαδοποίησης, ενώ τα συνελικτικά δίκτυα επιλέγονται για ζητήματα επεξεργασίας εικόνας (Bonaccorso 2017).

Εξίσου καθοριστική δράση αυτού του είδους λογίζεται πως είναι και η εκπαίδευση. Στο συγκεκριμένο επίπεδο εντοπίζεται η ουσία της εν λόγω μάθησης. Σε αυτό το σημείο ένα μέρος (σχεδόν το 60 έως και το 80%) από τα σωστά οργανωμένα στοιχεία τα οποία έχουν συλλεχθεί στα παραπάνω επίπεδο περνούν από το μοντέλο αυτής της μορφής με κυριότερο στόχο αυτό να καταρτιστεί και να μάθει να αναλύει τέτοιου είδους πληροφορίες.

Καθοριστικές, όμως, θεωρούνται και οι δράσεις της εκτίμησης (χρησιμεύει με βασικότερο στόχο να δοκιμαστεί εάν το μοντέλο έχει την ευχέρεια να ανταποκριθεί σε καινούριες εισόδους), της δοκιμής (σε αυτή τη δράση το τελευταίο κομμάτι των δεδομένων χρησιμεύει με στόχο τον υπολογισμό της τελικής απόδοσης) καθώς επίσης και της βελτίωσης τους μοντέλου (Serpanos and Wolf 2018).

Εικόνα 13 - Ορισμός & Χαρακτηριστικά ML

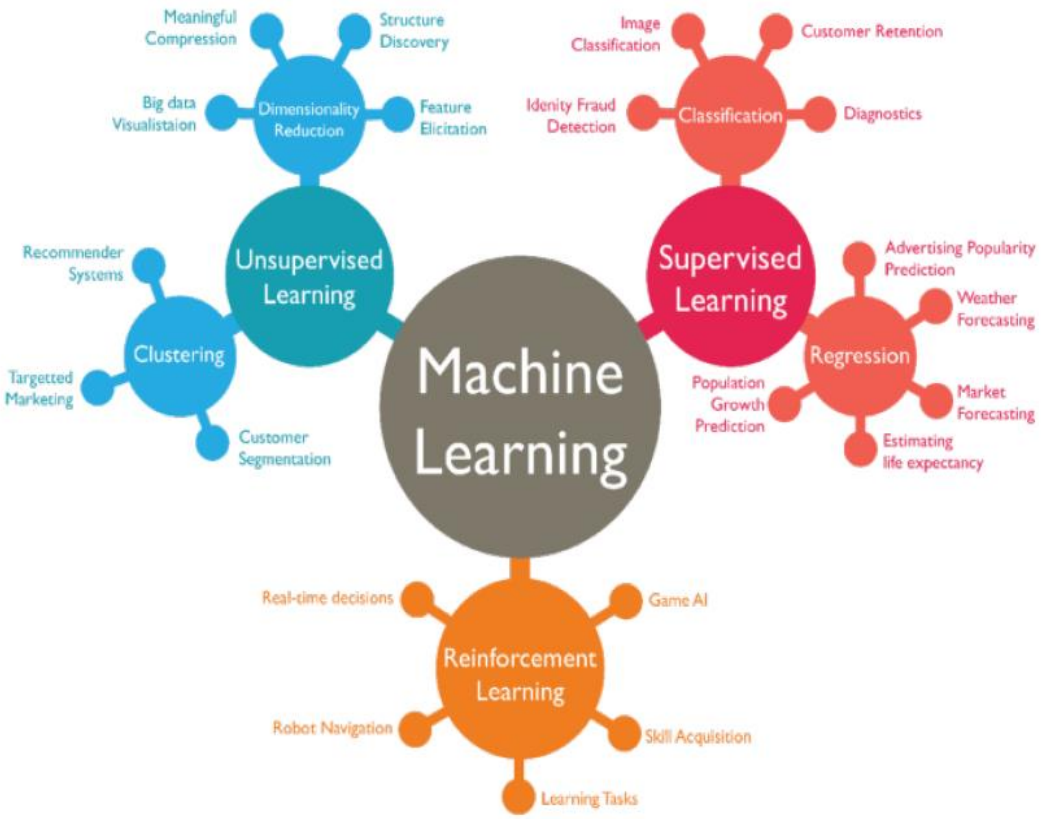
Υπάρχουν αριθμητές διαδικτυακές πλατφόρμες που βασίζονται στην μηχανική μάθηση και ανάλογα τα αποτελέσματα ορίζουν και την επόμενη στρατηγική τους. Τα σημειολογικά αποτελέσματα που παράγει η μηχανική μάθηση βάσει των αλγόριθμων έχουν φανεί κάτι παραπάνω από χρήσιμες σε εταιρείες και επιχειρήσεις. Η Google, η Amazon, το Netflix και άλλοι αναλύουν τα τεράστια δεδομένα που παράγονται μέσω του ML καταφέρνοντας να βελτιώσουν τις υπηρεσίες τους και τα πρωτότυπα τους.

4.3 Είδη μηχανικής μάθησης

Τα βασικά είδη μηχανικής μάθησης είναι τέσσερα (4). Αρχικώς έχουμε την επιβλεπομένη μάθηση (Supervised Learning). Αυτή η μάθηση ορισμένες φορές θα την εντοπίσετε να την αποκαλούν και ως μάθηση με παραδείγματα. Το επόμενο είδος της μηχανικής μάθησης καλείται ως μάθηση χωρίς επίβλεψη (Unsupervised learning) ενώ το τρίτο είδος είναι η ενισχυτική μάθηση (Reinforcement learning). Τέλος, η ημι-επιβλεπόμενη (semi-supervised) έρχεται να συμπληρώσει και να κλείσει τα είδη της μηχανικής μάθησης. Ενίοτε δεν υπολογίζεται ως 4 είδος και από πολλούς θεωρείται ότι συγκαταλέγεται στην Supervised

Σε αυτό το σημείο οφείλεται να υπογραμμιστεί ότι πολλές φορές συναντάμε ως είδη μηχανικής μάθησης παραπάνω από αυτά τα 4 προαναφερθέντα αλλά αυτό επί της ουσίας είναι λάθος καθώς οι τεχνικές που χρησιμοποιούν οι τέσσερις μέθοδοι αυτοί αποτελούν και μέρος τους και όχι εάν αυτούσιο μεμονωμένο κομμάτι.

Απ' την άλλη το Deep Learning δεν συγκαταλέγεται στα είδη της μηχανικής μάθησης γιατί μπορεί να υπάρχει ομοιότητα αλλά επί της ουσίας είναι διαφορετικός τρόπος μάθησης. Στην συνέχεια δίνεται μια εικόνα αναφοράς σχετικά με τα είδη της μηχανικής μάθησης αλλά και που χρησιμοποιούνται για να μας λύσουν προβλήματα.



Εικόνα 14 - Είδη μηχανικής μάθησης

4.4 Supervised Learning

Η εποπτευομένη μάθηση είναι ίσως η πιο κοινή μέθοδος στο ML. Οι αλγόριθμοι της συγκεκριμένης μάθησης ως επί το πλείστον αξιοποιούνται σε περιστατικά στα οποία υφίσταται γνώση καθορισμένων γνωρισμάτων για το σετ δεδομένων που διερευνούμε. Αυτό χρησιμεύει με κυριότερο σκοπό την εκπαίδευση ενός συστήματος το οποίο θα παίξει καθοριστικό ρόλο στην οριοθέτηση των βασικότερων ιδιοτήτων που αποτελούν καθοριστικό γνώρισμα ενός διαφορετικού σετ δεδομένων (Khalifa et al. 2016).

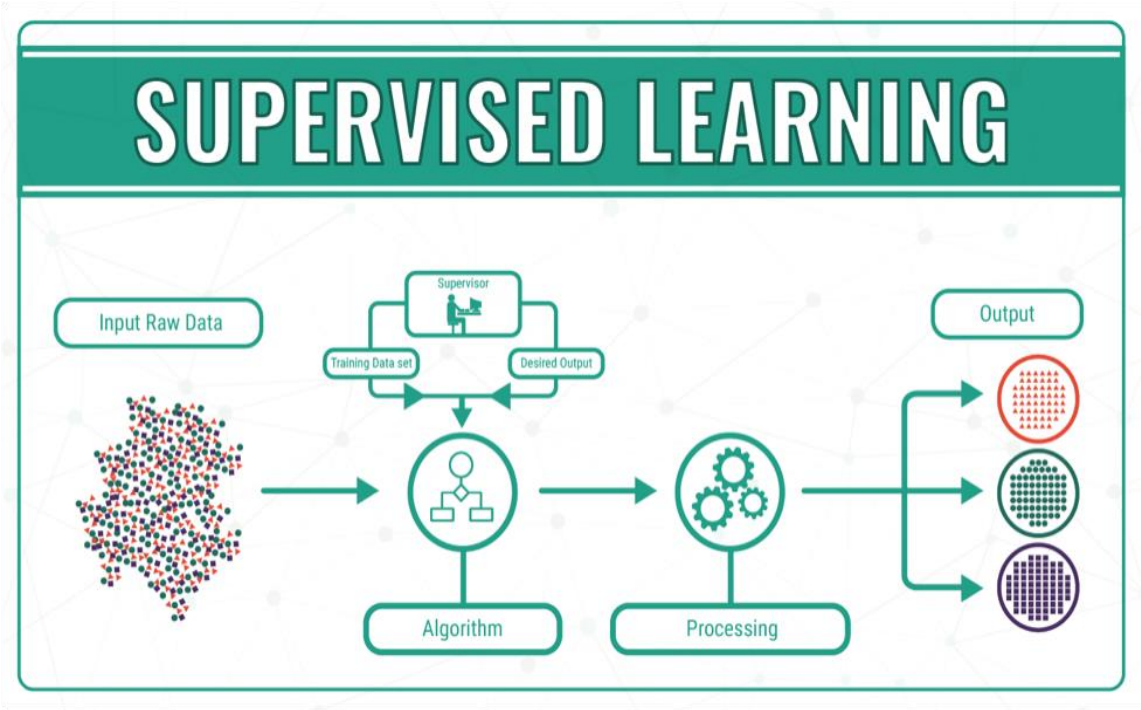
Επί της ουσίας, αποτελεί ένα εξαιρετικά χρήσιμο σύστημα, μια συνάρτηση που μαθαίνει μέσα από ένα σετ δεδομένων εκπαίδευσης. Στη μάθηση αυτής της μορφής γνωρίζουμε ήδη το αναμενόμενο αποτέλεσμα. Έχουμε γνώση, επομένως, της ορθής πρόβλεψης την οποία επιθυμούμε να εξάγουμε από τις πληροφορίες που έχουμε στη διάθεσή μας και μετέπειτα θέλουμε να εκπαιδεύσουμε τον αλγόριθμο, προκειμένου από τα εν λόγω στοιχεία να έχει την ευχέρεια να εξάγει το κατάλληλο αποτέλεσμα που αρμόζει στην εκάστοτε περίσταση (Αποστολόπουλος 2020).

Με αυτόν τον τρόπο σύμφωνα με τις πληροφορίες αλλά και τις δοθείσης απαντήσεις οι αλγόριθμοι αυτής της μορφής είναι ζωτικής σημασίας να αναγνωρίσουν τα μοτίβα και σταδιακά να αναπτύξουν την απαιτούμενη γνώση με κυριότερο στόχο να έχουν την ευχέρεια να υλοποιήσουν την ορθότερη κατηγοριοποίηση (Serpanos and Wolf 2018).

Τα τελευταία χρόνια σε διεθνές επίπεδο έχουν δημιουργηθεί πολλοί αλγόριθμοι αυτής της μορφής, όπου ο καθένας εξ αυτών έχει τα δικά του οφέλη αλλά και ελαττώματα. Ο εκάστοτε αλγόριθμος από αυτούς θεωρείται ως κατάλληλος για καθορισμένα περιστατικά και είναι σημαντικό να διερευνάται το πόσο αποτελεσματικός είναι δίχως να υφίστανται αλγόριθμοι που να λογίζονται ως πιο ικανοί σε σχέση με άλλους, δίχως να υπάρχει η παραμικρή εξάρτηση της μορφής της εκάστοτε εφαρμογής (Bonaccorso 2017).

Τέλος, σε αυτό το σημείο χρειάζεται να επισημανθεί πως οι περισσότερες έρευνες στη σημερινή εποχή αναφέρουν πως οι κυριότεροι αλγόριθμοι αυτού του είδους μάθησης είναι οι ακόλουθες (Hutter et al. 2019):

- Μηχανές Διανυσμάτων Υποστήριξης (Support Vector Machine - SVM)
- Θεώρημα Bayesian
- K-Κοντινότερων Γειτόνων (K Nearest Neighbors - KNN)
- Τυχαία Δάση (Random Forest - RF)
- Δένδρα Απόφασης (Decision Trees)
- Νευρωνικά δίκτυα (Neural Networks)
- Ensemble Learning



Εικόνα 15 - Supervised Learning

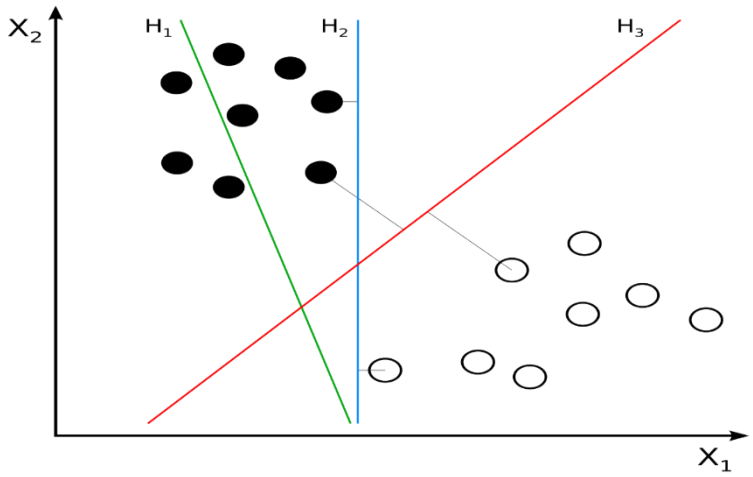
Στην παραπάνω εικόνα δίνεται και οπτικά όλα αυτά που αναλυθήκαν προηγούμενα σχετικά με το Supervised Learning.

Μηχανές Διανυσμάτων Υποστήριξης (Support Vector Machine - SVM)

Ο αλγόριθμος αυτός έχει ως στόχο την μεγιστοποιήσει των κατηγοριών που θέλουμε να διαχωρίσουμε. Αυτό επιτυγχάνεται αφού δημιουργεί ένα μοντέλο που εκχωρεί τις μικρές διαφορές πιο κοντά από κάτι άλλο το οποίο απέχει σε μεγάλο βαθμό από εκείνο.

Ουσιαστικά δηλαδή, πετυχαίνει τον διαχωρισμό μέσω της μεγιστοποίησης από την κάθε κατηγορία που διακρίνει με ένα ελάχιστο σφάλμα στο μέγιστο περιθώριο. Στο παράδειγμα της εικόνας από κάτω βλέπουμε ότι το H1 έχει διαχωριστεί από το H2 δημιουργώντας δυο κατηγορίες. Το H1 όμως είναι σιγουρά πιο κοντά στο H2 από ότι στο H3 που καταλαβαίνουμε ότι απέχει πολύ άρα έχει μεγιστοποιηθεί η κατηγορία.

Όπως συμπεραίνουμε ανήκει στον κλάδο του classification αφού διαχωρίζει την μικρή από την μεγάλη απόσταση ως διαφορά.



Εικόνα 16 - SVM Παράδειγμα

Το SVM διαθέτει υψηλό επίπεδο ακρίβειας κάτι που το καθιστά απολύτως κατάλληλο για εφαρμογές σε IoT. Μπορεί να εντοπίσει κακόβουλα λογισμικά αλλά και να πραγματοποιήσει ανίχνευση εισβολών. Δεν είναι τυχαίο ότι πολλές εταιρείες που ασχολούνται με την ασφάλεια έχουν ενστερνιστεί τα SVM και τα χρησιμοποιούν κατά κόρων (Hutter et al. 2019).

Θεώρημα Bayesian

Το θεώρημα Bayesian βασίζεται σε θεώρημα στατιστικών. Σχετίζεται με την συγκριση της τρέχουσας πιθανότητας με την αρχική πιθανότητα. Ουσιαστικά το θεώρημα αυτό εξαρτάται από τον βαθμό αληθείας σε μια κατάσταση πριν και μετά τον υπολογισμό των δεδομένων. Για να γίνει πιο ευκολά κατανοητό ας υποθέσουμε ότι κάποιος πιστεύει ότι εισέρχεται σε μια σελίδα με κακόβουλο λογισμικό με βεβαιότητα 50%. Όταν θα ξανά εισέλθει ο βαθμός αληθείας έχει αλλάξει, έχει μειωθεί ή αυξηθεί αναλόγως με το προηγούμενο αποτέλεσμα καθώς ο βαθμός βεβαιότητας δεν παραμένει σταθερός.

Με την χρήση του θεωρήματος μπορούμε να ξεπεράσουμε ένα μεγάλο αριθμό παραδειγμάτων και το training set που χρησιμοποιείται για την παραμετροποίηση διαφόρων μοντέλων. Αυτά τα πλεονεκτήματα όπως επίσης το γεγονός ότι είναι αρκετά απλό στην κατανόηση και απαιτούνται λιγότερα δεδομένα για ταξινομήσεις μας κάνει το θεώρημα αυτό χρήσιμο στο IoT καθώς μπορεί να ανίχνευση εισβολείς στο στρώμα εργασίας και να προχωρήσει σε ανίχνευση εισβολών

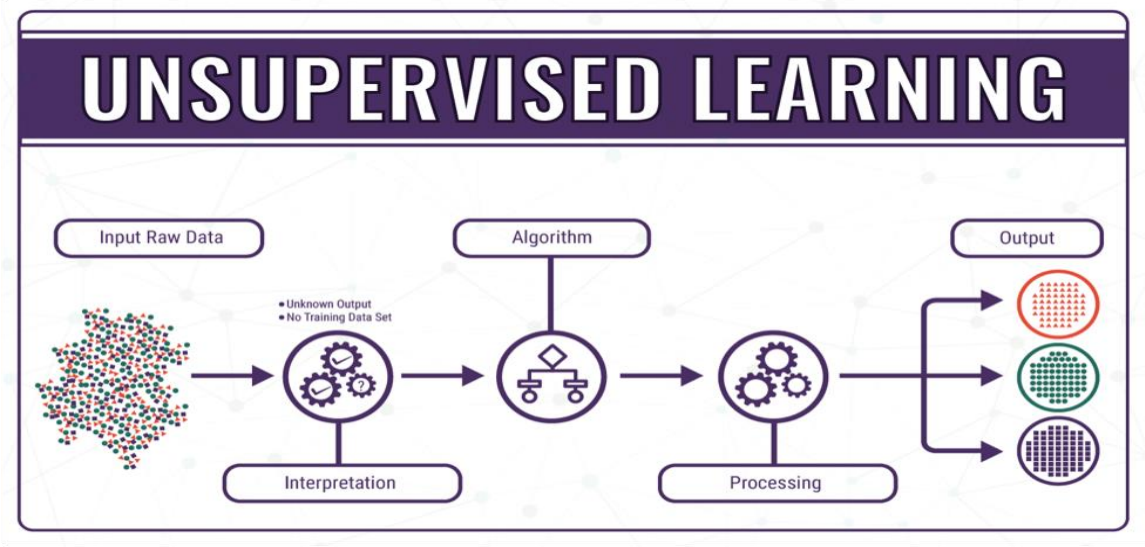
4.5 Unsupervised Learning

Η μάθηση αυτού του είδους αφορά μια από τις πιο σημαντικότερες κατηγορίες της μάθησης που μελετάμε σε αυτό το κεφάλαιο, κυριότερος σκοπός της οποίας αποτελεί η ανακάλυψη πιθανής δομής, η οποία είναι δυνατόν να κρύβεται πίσω από μη χαρακτηρισμένες πληροφορίες. Από τη στιγμή που τα συγκεκριμένα παραδείγματα που χρησιμεύουν σε αυτές τις περιπτώσεις δεν έχουν χαρακτηριστεί δεν είναι εφικτό να γίνει η απαιτούμενη αξιολόγηση των πιθανών λύσεων (Hassen et al. 2017).

Οι αλγόριθμοι της συγκεκριμένης μορφής κατά κύριο λόγο εφαρμόζονται σε περιστατικά στα οποία δεν έχουν γνώση των κυριότερων ιδιοτήτων που διέπουν το σετ δεδομένων τα οποία θα πρέπει να επεξεργαστούν. Σε αυτές τις περιπτώσεις γίνεται προσπάθεια κατανόησης των σχέσεων οι οποίες εξελίσσονται ανάμεσα στα συγκεκριμένα δεδομένα του σετ και στη συνέχεια να ληφθούν οι απαραίτητες αποφάσεις (Chumachenko 2017).

Στη μη εποπτευόμενη μάθηση, όπως καλείται στην εθνική βιβλιογραφία, οι αλγόριθμοι αυτού του είδους δεν έχουν ένα καθορισμένο σετ δεδομένων εκπαίδευσης. Αντίθετα, τους παρέχεται ένα σετ πληροφοριών τα οποία έχουν προέλευση από μια πηγή και είναι σημαντικό μόνοι τους να εξάγουν τα αποτελέσματα και να υλοποιήσουν την απαιτούμενη κατηγοριοποίηση (Τζανακός 2020).

Ως επί το πλείστον, η μάθηση αυτής της μορφής χρησιμεύει με απώτερο στόχο τον εντοπισμό κρυφών μοτίβων σε πληροφορίες, με τεράστια εφαρμογή κυρίως στα social media. Σύμφωνα με έρευνες που έχουν λάβει χώρα τα τελευταία χρόνια οι πιο σημαντικοί, χρήσιμοι αλλά και διαδεδομένοι αλγόριθμοι αυτής της μορφής είναι οι clustering, οι principal component analysis, οι singular value decomposition καθώς επίσης και οι

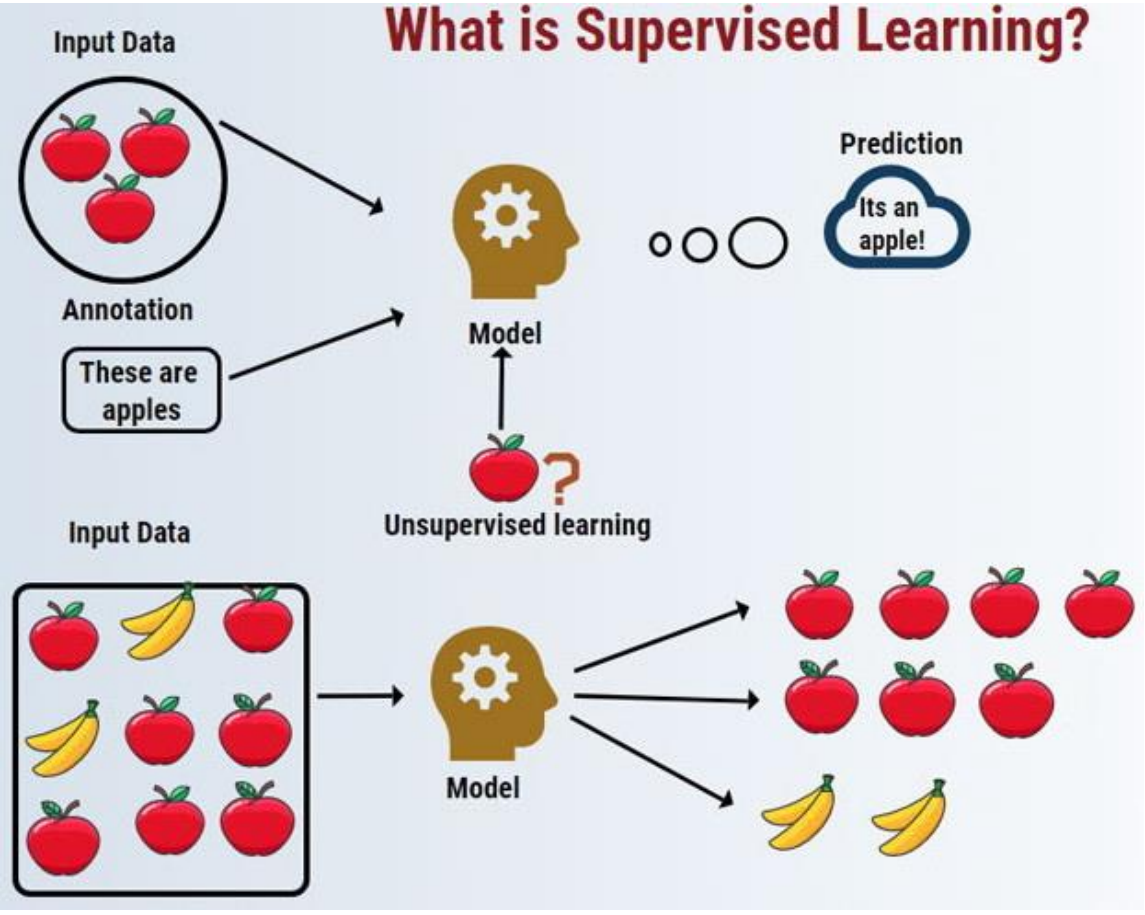


Εικόνα 17 - Unsupervised Learning

independent component analysis (Serpanos and Wolf 2018).

Τέλος, είναι χρήσιμο να γνωρίζουμε πως ένα σύστημα το οποίο χρησιμοποιείται από αυτή τη μάθηση ενεργεί με απώτερο στόχο να καταφέρει να ανακαλύψει ομάδες με ίδια γνωρίσματα στο σετ δεδομένων και καθορισμένα μοτίβα τα οποία δεν έχουν ανακαλυφθεί από πιο πριν, δίχως το διάνυσμα εισόδου να έχουν κάποια ετικέτα. Αυτό σημαίνει πως προσφέρεται η ευχέρεια για εντοπισμό σχέσεων ανάμεσα στα κυριότερα γνωρίσματα αυτού του σετ και αυτό είναι κάτι το οποίο τις περισσότερες φορές κατορθώνεται διαμέσου της ομαδοποίησης είτε όπως καλείται στη διεθνή βιβλιογραφία διαμέσου του clustering (Khalifa et al. 2016).

Η δράση αυτή αφορά την ομαδοποίηση των αντικειμένων με τέτοιο τρόπο, προκειμένου όλα τα αντικείμενα τα οποία περιέχονται σε ένα cluster να μοιάζουν όσο γίνεται περισσότερο μεταξύ τους, συγκριτικά με άλλα τα οποία περιέχονται σε διαφορετικά clusters. Πιο συγκεκριμένα, όμως, στη μάθηση αυτής της μορφής γίνεται χρήση με στόχο την ομαδοποίηση των σετ δεδομένων με ίδια γνωρίσματα και γενικά με στόχο την ομαδοποίηση δεδομένων που δεν έχουν κάποια ετικέτα. Έτσι, εντοπίζονται κοινά σημεία και σύμφωνα με τις ομοιότητες τις οποίες εμφανίζουν το σύστημα δρα αναλόγως (Yeo et al. 2018).



Εικόνα 18 - Supervised vs Unsupervised

4.6 Semi-Supervised Learning

Στη συγκεκριμένη μορφή πάθησης οι περισσότεροι αλγόριθμοι τροφοδοτούνται με ένα όχι πλήρες σετ από training data αλλά είναι σημαντικό να εκπαιδευτούν από αυτό. Χαρακτηριστικότερο παράδειγμα εφαρμογής αυτής της μορφής αποτελεί η περίπτωση ταξινόμησης ταινιών σύμφωνα με καθορισμένες κριτικές. Πάντοτε σε αυτές τις εφαρμογές προστίθενται καινούριες κριτικές που είναι δυνατόν να μεταβάλλουν άρδην το αποτέλεσμα μιας αναζήτησης (Serpanos and Wolf 2018).

4.7 Deep Learning

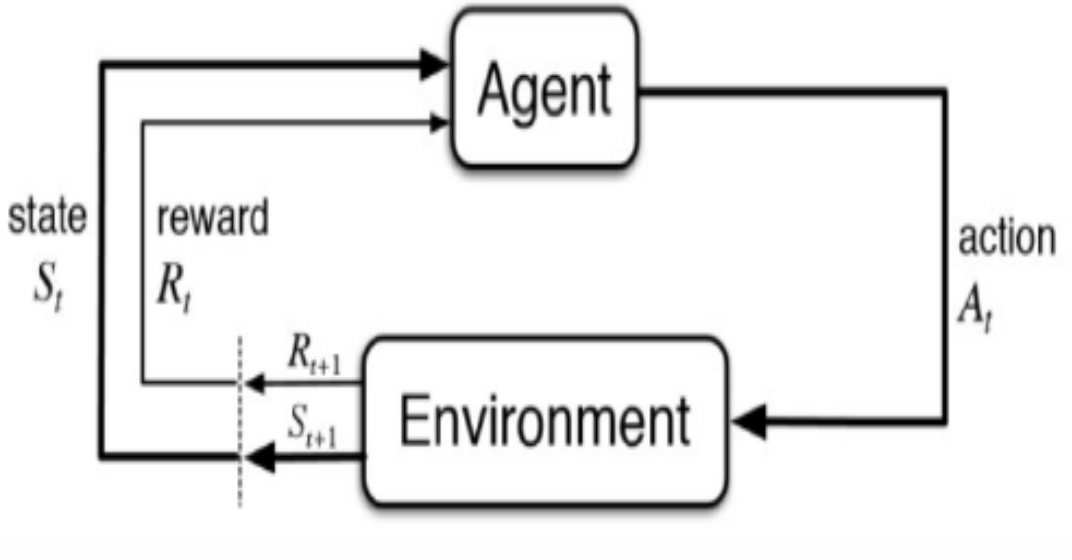
Η μάθηση αυτού του είδους αφορά μια προσέγγιση, που ενεργεί με απώτερο στόχο να κατορθώσει να μοντελοποιήσει τη μέθοδο, με την οποία ο εγκέφαλος των ανθρώπων επεξεργάζεται το φως καθώς επίσης και τον ήχο και έχει την ευχέρεια να τα μετατρέψει σε όραση είτε ακοή. Η αρχιτεκτονική αλλά και η δράση των συγκεκριμένων δικτύων είναι εμπνευσμένη από τα βιολογικά νευρωνικά δίκτυα. Επί της ουσίας αφορά διάφορα τεχνητά νευρωνικά δίκτυα αρκετών και διαφορετικών επιπέδων, τα οποία πραγματοποιούνται σε υλικό και σε μονάδα επεξεργασίας γραφικών (Αποστολόπουλος 2020).

Οι νεύρωνες αυτής της μορφής κατηγοριοποιούνται σε διαφοροποιημένα επίπεδα και αποτελούν μη γραμμικές μονάδες επεξεργασίας ενώ παράλληλα ενεργούν με απώτερο στόχο να καταφέρουν να εξάγουν γνωρίσματα από τις πληροφορίες είτε να τις μετασχηματίσουν. Η έξοδος ενός επιπέδου κατά κύριο λόγο χρησιμοποιείται σαν εισροή του αμέσως επόμενου επιπέδου (Hutter et al. 2019).

Οι αλγόριθμοι αυτοί είναι δυνατόν να είναι επιβλεπόμενοι και να χρησιμοποιούνται με κυριότερο στόχο την κατηγοριοποίηση των πληροφοριών ή μη επιβλεπόμενοι με στόχο την ανάλυση προτύπων. Στη σύγχρονη εποχή ένα τέτοιο δίκτυο περιλαμβάνεται από αρκετά και διαφορετικά επίπεδα αναπαραστάσεων τα οποία κατά βάση αναλογούν σε διαφοροποιημένα επίπεδα αφαίρεσης. Τα συγκεκριμένα επίπεδα αποτελούν μια ιεραρχία των εννοιών (Τζανακός 2020).

Οι συγκεκριμένοι αλγόριθμοι κάνουν ένα σύστημα να έχει την ευχέρεια να αφομοιώσει το πιο μεγάλο σύνολο πληροφοριών, σε σχέση με τους υπόλοιπους αλγορίθμους της μάθησης που μελετάμε σε αυτό το κεφάλαιο. Ένα παρόμοιο σύστημα έχει τη δυνατότητα να νικήσει ακόμη και τους ανθρώπους σε συγκεκριμένες νοητικές δράσεις. Εξαιτίας των εν λόγω γνωρισμάτων, η μάθηση αυτής της μορφής έχει γίνει μια καθοριστική προσέγγιση με μεγάλο δυναμισμό στο σύγχρονο περιβάλλον της τεχνητής νοημοσύνης (Bonaccorso 2017).

Γενικότερα, αυτό το οποίο είναι σημαντικό να γνωρίζουμε για τη μάθηση αυτής της μορφής είναι πως οι αλγόριθμοί της κάνουν χρήση ενός νευρικού δικτύου με στόχο να εντοπίσουν σχέσεις ανάμεσα σε ένα σύνολο εισροών και εκροών. Ένα τέτοιο δίκτυο περιέχεται από διάφορα επίπεδα εισόδου και εξόδου που περιέχονται από κόμβους.



Εικόνα 19 - Ενισχυμένη Μάθηση

Τα επίπεδα εισόδου λαμβάνουν μια αριθμητική αναπαράσταση των πληροφοριών που εισάγονται, ενώ τα επίπεδα εξόδου εξάγουν προβλέψεις, ενώ από την άλλη πλευρά τα κρυφά επίπεδα έχουν άρρηκτη σχέση με την πλειονότητα του υπολογισμού. Όταν το συγκεκριμένο δίκτυο περάσει τις εισόδους του έως τις εξόδους του, το εν λόγω δίκτυο αξιολογεί πόσο καλή ήταν η πρόβλεψη του (συγκριτικά με την αναμενόμενη έξοδο) διαμέσου μιας συνάρτησης απώλειας. Τέλος, είναι χρήσιμο να γνωρίζουμε πως οι πιο διαδεδομένοι αλγόριθμοι αυτού του είδους είναι ο DBM, ο DBN, ο CNN καθώς επίσης και οι Stacked Auto-Encoders (Serpanos and Wolf 2018).

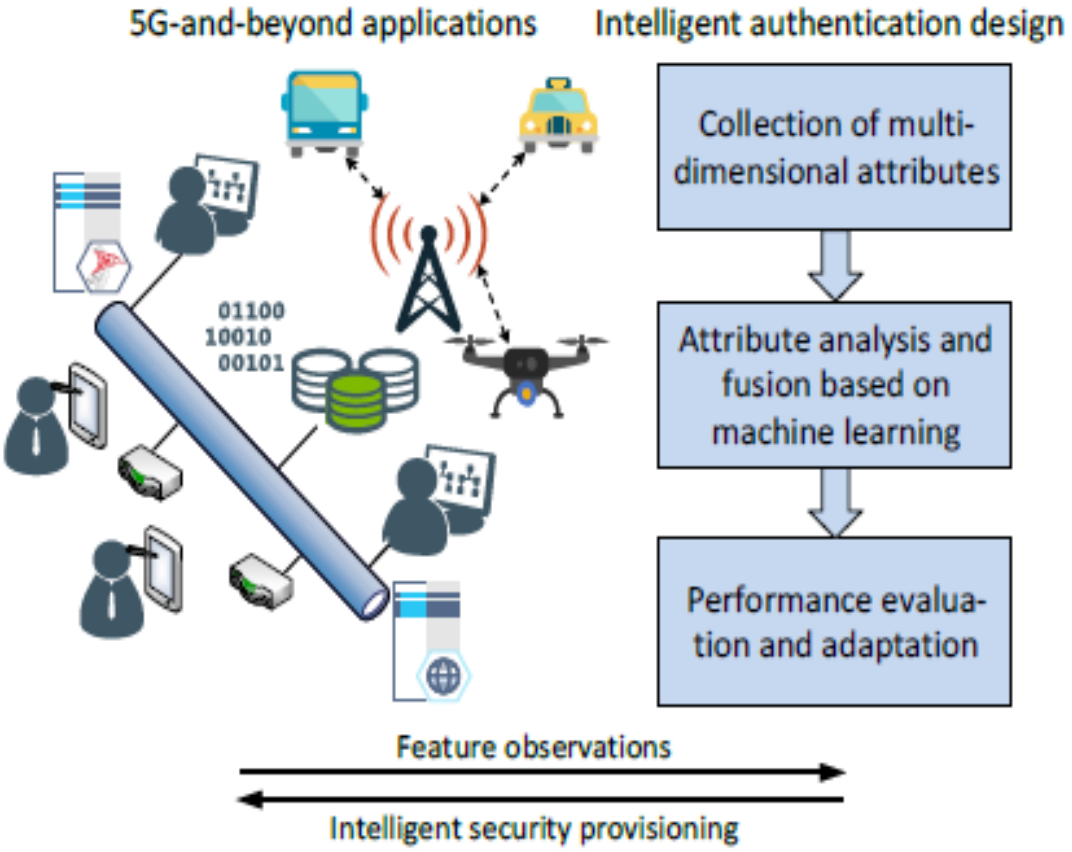
4.8 Deep Reinforcement Learning

Η εν λόγω μάθηση, η οποία στη γλώσσα μας καλείται ενισχυμένη μάθηση εστιάζει κυρίως στην αντίληψη πως ένα πρόγραμμα ζει σε ένα περιβάλλον, στο οποίο είναι ζωτικής σημασίας να υλοποιήσει μια βέλτιστη ενέργεια σε μια καθορισμένη κατάσταση με απώτερο στόχο να βελτιστοποιήσει το κέρδος. Σύμφωνα με τις ενέργειες τις οποίες θα υλοποιήσει ο εκάστοτε agent σε κάθε περίπτωση, θα υπάρχει και ένα διαφοροποιημένο όφελος ενώ παράλληλα ο agent θα έχει την ευχέρεια να μεταβαίνει σε διαφοροποιημένες καταστάσεις (Hussain et al. 2020).

Η βασικότερη διαφοροποίηση αυτής της μάθησης από το supervises είναι πως η δεύτερη εξ αυτών εστιάζει κατά κύριο λόγο στις ετικέτες οι οποίες αναλογούν στο διάνυσμα εισόδου, ενώ από την άλλη πλευρά η πρώτη εξ αυτών εστιάζει κυρίως στον εντοπισμό πιο πολλών και διαφορετικών καταστάσεων με στόχο τη μετάβαση του agent και την επεξεργασία των ήδη υπαρχόντων στοιχείων (Serpanos and Wolf 2018).

Ένα κατανοητό και χαρακτηριστικό παράδειγμα αυτής της μορφής, το οποίο εξηγεί τι είναι η συγκεκριμένη μάθηση είναι ένα παιχνίδι όπου υφίσταται ένας κυνηγός ο

οποίος επιθυμεί να εντοπίσει τον θησαυρό και στο χάρτη υφίστανται εμπόδια, τα οποία είναι σημαντικό να αποφύγει αλλά και διαφορετικές διαδρομές, τις οποίες χρειάζεται να ακολουθήσει με στόχο να εντοπίσει τον θησαυρό. Στόχος του είναι να εντοπίσει την πιο μικρή αλλά και την πιο ακίνδυνη διαδρομή, προκειμένου να φτάσει γρηγορότερα και με μεγαλύτερη ασφάλεια στον στόχο του (OSahn et al. 2018).



Εικόνα 20 - Διάγραμμα πλαισίου ευφυούς σχεδιασμού ελέγχου ταυτότητας

Η μέθοδος μάθησης αυτής της μορφής, έχει ανάγκη από μια είσοδο η οποία θα αποτελεί την πρωταρχική κατάσταση όπου θα υφίσταται το μοντέλο αλλά κα μια έξοδο στην οποία θα υφίστανται αρκετές και διαφορετικές επιλογές για την επίλυση ενός ζητήματος. Στη συνέχεια, θα εκπαιδευτεί το μοντέλο σύμφωνα με την είσοδο, θα επιστρέψει μια κατάσταση και εν τέλει ο χρήστης, σύμφωνα με το τι επιθυμεί, θα τιμωρεί είτε θα επιβραβεύει το μοντέλο. Το συγκεκριμένο μοντέλο θα εφαρμόζεται συνεχώς έως ότου να εντοπιστεί το βέλτιστο εφικτό κέρδος (Chumachenko 2017).

ΚΕΦΑΛΑΙΟ 5 – Μηχανική Μάθηση στον κόσμο του IoT

5.1 Τεχνικές ασφαλείας βασισμένη στην μηχανική μάθηση

Σε αυτό το κεφαλαίο θα εξετάσουμε ενδελεχώς και σε βάθος το πως μπορούμε να αξιοποιήσουμε την μηχανική μάθηση στον κόσμο του IoT προς όφελος μας. Συγκεκριμένα στην συνέχεια θα δούμε τα είδη και τους τρόπους της μάθησης ώστε να επιτύχουμε την αναμενομένη ασφάλεια που επιζητούμε. Μεσώ αυτής αντιμετωπίζουμε πρόβλημα επιθέσεων αλλά και αποκτάμε τους τρεις βασικους πυλώνες της ασφάλειας που εξετάσαμε παραπάνω.

5.1.1 Μάθηση βασισμένη στην αυθεντικοποίηση

Όπως φαίνεται στην εικόνα 17, παρουσιάζουμε το σχεδιασμό προσεγγίσεων ευφυούς ελέγχου ταυτότητας με μηχανική μάθηση χρησιμοποιώντας πολυδιάστατα χαρακτηριστικά και βελτιστοποιώντας την ολιστική διαδικασία ελέγχου ταυτότητας. Στην πρώτη φάση, τα χρονικά μεταβαλλόμενα πολυδιάστατα χαρακτηριστικά συλλέγονται για έλεγχο ταυτότητας, τα οποία μπορεί να εκτιμηθούν ατελή με θορύβους και σφάλματα μέτρησης (Naeem et al. 2018).

Στα παραδείγματα περιλαμβάνονται τα χαρακτηριστικά φυσικού επιπέδου, η επιλογή δικτύου σε ετερογενή ασύρματα δίκτυα και τα μοτίβα κινητικότητας. Σε ένα συγκεκριμένο σενάριο ασύρματης επικοινωνίας 5G, εκείνα τα χαρακτηριστικά που παρέχουν περισσότερες πληροφορίες για έλεγχο ταυτότητας μπορούν να επιλεγούν πρώτα. Αναλυτικά, τα μη εξαρτώμενα χαρακτηριστικά που έχουν ευρύτερο εύρος διανομής και μεγαλύτερη ακρίβεια εκτίμησης θα μπορούσαν να προσφέρουν περισσότερες πληροφορίες για τη διάκριση διαφορετικών πομπών (Khalifa et al. 2016).

Χρησιμοποιώντας πολυδιάστατα χαρακτηριστικά καθώς και κοινή χρήση πληροφοριών μεταξύ διαφορετικών επιπέδων και δικτύων, η αξιοπιστία του ελέγχου ταυτότητας είναι εφικτό να βελτιωθεί. Προφανώς, ο σχεδιασμός του έξυπνου ελέγχου ταυτότητας βασίζεται μόνο στα δεδομένα εκτίμησης των χαρακτηριστικών χωρίς να απαιτείται ακριβής δομή της χρονικής μεταβολής (π.χ. το μοντέλο καναλιού, με αποτέλεσμα την επικύρωση συσκευής χωρίς μοντέλο) (Hassen et al. 2017).

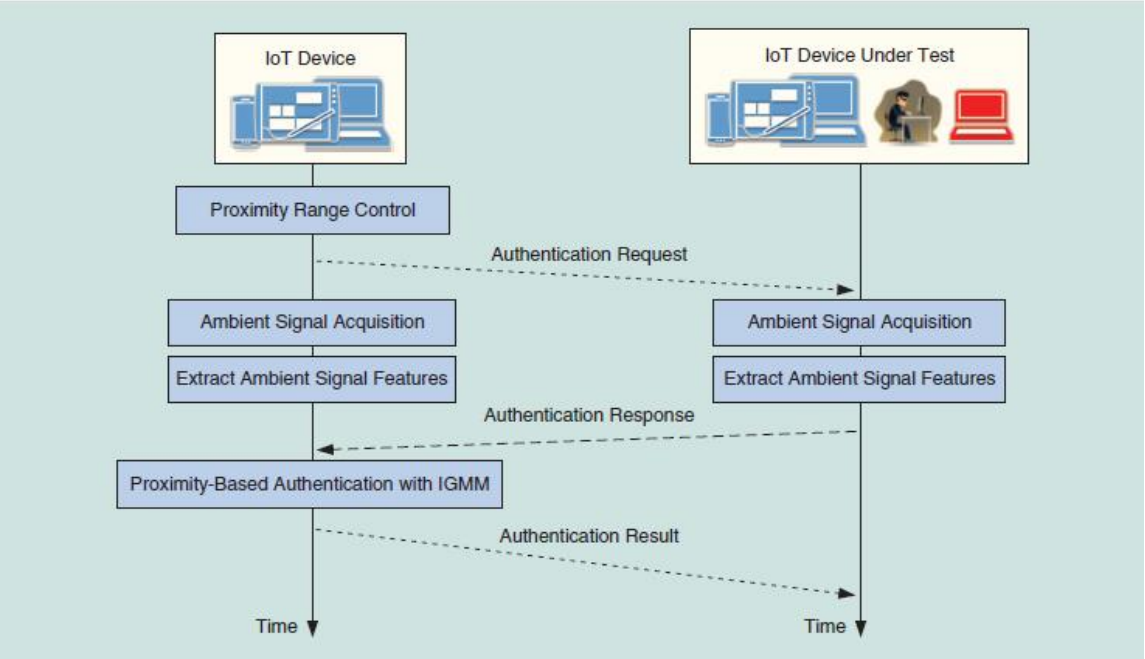
Από την άλλη πλευρά στην φάση 2 τα πολυδιάστατα χαρακτηριστικά μπορούν να συγχωνευτούν για έλεγχο ταυτότητας βάσει τεχνικών μηχανικής μάθησης. Ένα παράδειγμα είναι ένα πρόγραμμα ελέγχου ταυτότητας φυσικού επιπέδου βασισμένο σε μηχανική μάθηση πυρήνα. Λαμβάνοντας υπόψη τις χρονικά μεταβαλλόμενες συνθήκες δικτύου, όπως οι περιορισμοί πόρων και οι αβεβαιότητες, τα χαρακτηριστικά ενδέχεται να είναι ευκαιριακά και για αυτό το λόγο τις περισσότερες φορές επιλέγεται για ταυτόχρονη διαχείριση τόσο της γενικής επικοινωνίας όσο και της διαχείρισης ασφάλειας. Επιπλέον, η ανάπτυξη ενός κατάλληλου αλγορίθμου μηχανικής μάθησης και η μείωση

της διάστασης του συστήματος ελέγχου ταυτότητας ωφελεί την απόδοση της επικοινωνίας, κάτι το οποίο θα βοηθήσει να επιτευχθεί οικονομικός έλεγχος ταυτότητας (Yeo et al. 2018).

Αντίθετα, στην τρίτη φάση ο έλεγχος ταυτότητας μπορεί να πραγματοποιηθεί με βάση τη νέα συλλογή πολυδιάστατων χαρακτηριστικών. Για να επιτευχθεί αυτό καθοριστικό ρόλο παίζει η παλινδρόμηση ή η ταξινόμηση. Το μοντέλο πρέπει να κατασκευαστεί με βάση τα δεδομένα εκπαίδευσης που συλλέγονται. Στη συνέχεια, η απόδοση ελέγχου ταυτότητας μπορεί να αξιολογηθεί και η διαδικασία ελέγχου ταυτότητας μπορεί να προσαρμοστεί στο πολύπλοκο περιβάλλον που ποικίλλει από το χρόνο με την εξερεύνηση της μηχανικής μάθησης για την παρακολούθηση των παραλλαγών των πολυδιάστατων χαρακτηριστικών. Ως εκ τούτου, η συνεχής και συνειδητοποιημένη διαδικασία προτείνεται για έξυπνη παροχή ασφάλειας σε εφαρμογές 5G και πέραν αυτών (Holma et al. 2020).

5.1.2 Μάθηση βασισμένη στο Access Control

Είναι δύσκολο να σχεδιαστεί ο έλεγχος πρόσβασης για συστήματα IoT σε ετερογενή δίκτυα με πολλαπλούς τύπους κόμβων και δεδομένα πολλών πόρων. Τεχνικές αυτής της μάθησης όπως SVMs, K-NNs και NNs έχουν χρησιμοποιηθεί για ανίχνευση εισβολής. Για παράδειγμα, η ανίχνευση επίθεσης DoS, όπως προτείνεται, χρησιμοποιεί ανάλυση συσχέτισης πολλαπλών παραλλαγών για την εξαγωγή των γεωμετρικών συσχετίσεων μεταξύ των χαρακτηριστικών κυκλοφορίας δικτύου. Αυτό το σχήμα αυξάνει την ακρίβεια ανίχνευσης κατά 3,05% σε 95,2% σε σύγκριση με την προσέγγιση πλησιέστερων γειτόνων με βάση το τρίγωνο χρησιμοποιώντας το σύνολο δεδομένων KDD Cup 99.



Εικόνα 21 - Απεικόνιση Access Control με χρήση ML (Xiao et al.2018)

Οι συσκευές IoT, όπως οι εξωτερικοί αισθητήρες, έχουν συνήθως αυστηρούς περιορισμούς πόρων και υπολογισμών, προκαλώντας προκλήσεις για τεχνικές ανίχνευσης εισβολών ανωμαλιών και υποβαθμίζοντας έτσι την απόδοση ανίχνευσης εισβολής για συστήματα IoT. Οι τεχνικές μηχανικής μάθησης βοηθούν στη δημιουργία ελαφρών πρωτοκόλλων ελέγχου πρόσβασης για εξοικονόμηση ενέργειας και παράταση της διάρκειας ζωής των συστημάτων IoT. Για παράδειγμα, το σχήμα ανίχνευσης ακραίων τιμών, εφαρμόζει τα K-NN για την αντιμετώπιση του προβλήματος της μη εποπτευόμενης ανίχνευσης ακραίων τιμών στα WSN και προσφέρει ευελιξία στον καθορισμό των ακραίων τιμών με μειωμένη κατανάλωση ενέργειας. Αυτό το σχήμα μπορεί να εξοικονομήσει τη μέγιστη ενέργεια κατά 61,4% σε σύγκριση με το κεντρικό σχήμα με παρόμοια μέση κατανάλωση ενέργειας (Hussain et al. 2020).

Γενικότερα, είναι χρήσιμο να γνωρίζουμε πως οι εποπτευόμενες τεχνικές μάθησης, όπως οι SVM, χρησιμοποιούνται για την ανίχνευση πολλαπλών τύπων επιθέσεων για την κίνηση στο Διαδίκτυο και το έξυπνο δίκτυο. Για παράδειγμα, ένας ελαφρύς μηχανισμός ανίχνευσης επιθέσεων, χρησιμοποιεί μια ιεραρχική δομή βασισμένη σε SVM για τον εντοπισμό επιθέσεων πλημμύρας κυκλοφορίας. Στο πείραμα επίθεσης, το σύστημα συλλογής συνόλων δεδομένων συγκεντρώνει δεδομένα βάσης πληροφοριών Simple Network Management Protocol (SNMP) από το σύστημα θύματος χρησιμοποιώντας μηνύματα ερωτήματος SNMP. Τα αποτελέσματα ενός τέτοιου πειράματος έχουν δείξει ότι αυτό το σχήμα μπορεί να επιτύχει ποσοστό ανίχνευσης επίθεσης πάνω από 99,40% και ακρίβεια ταξινόμησης πάνω από 99,53% (Xiao et al. 2018).

Στην εικόνα 18 βλέπουμε την συσκευή IoT να εξάγει και να στέλνει τα χαρακτηριστικά και τις δυνατότητες των σημάτων ως νόμιμη συσκευή. Μόλις ληφθούν τέτοια μηνύματα ελέγχου ταυτότητας ο δέκτης εφαρμόζει την ανάλογη τεχνική για να συγκρίνει το αναφερόμενο σήμα με εκείνα τα σήματα του περιβάλλοντος ώστε να παρατηρηθεί η εγγύτητα βασισμένη στην δοκιμή. Μπορούν να χρησιμοποιηθούν όλες οι τεχνικές που αναφέρθηκαν τις ML. Στο συγκεκριμένο παράδειγμα χρησιμοποιείται Deep Learning αλλά κάλλιστα δουλεύουν και άλλοι όπως η εποπτευομένη μάθηση.

5.1.2 Μάθηση βασιζόμενη στο Malware Detection

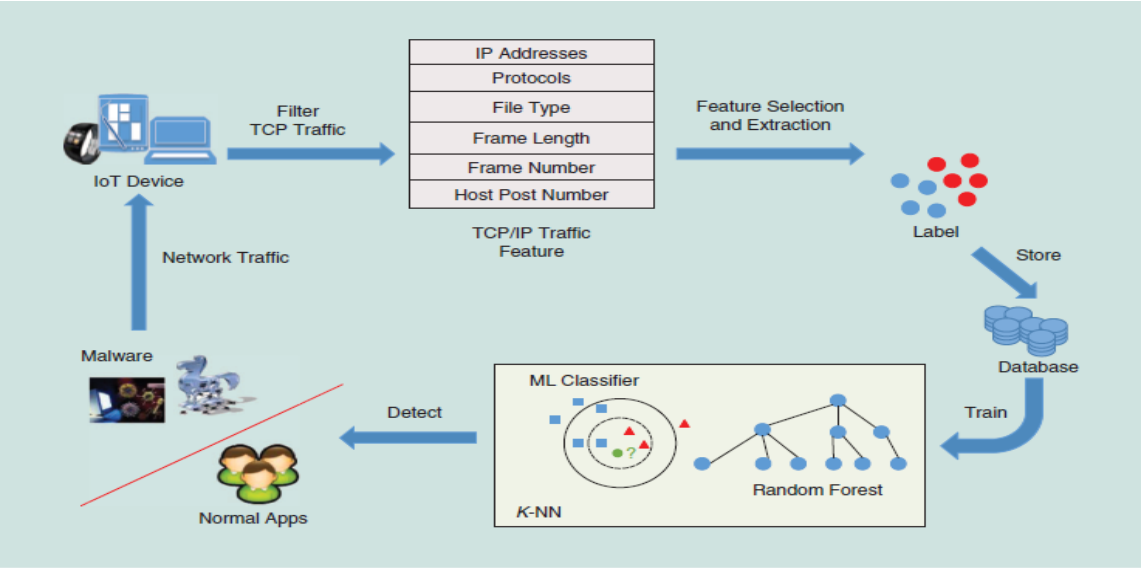
Όπως έχουμε ήδη αναλύσει παραπάνω η μηχανική μάθηση είναι ένα εργαλείο ανάλυσης δεδομένων που χρησιμοποιείται για την αποτελεσματική εκτέλεση συγκεκριμένων εργασιών χωρίς ρητές οδηγίες. Τα τελευταία χρόνια, οι δυνατότητες αυτής της μάθησης έχουν χρησιμοποιηθεί για το σχεδιασμό τόσο στατικών όσο και δυναμικών τεχνικών ανάλυσης για τον εντοπισμό κακόβουλου λογισμικού (malware detection) (Yeo et al. 2018).

Τα τελευταία χρόνια έρευνες πρότειναν μια νέα τεχνική ταξινόμησης κακόβουλου λογισμικού. Οι εν λόγω έρευνες χρησιμοποίησαν στατική ανάλυση για να ταξινομήσουν την παρουσία κακόβουλου λογισμικού σε νέες γνωστές οικογένειες κακόβουλου λογισμικού. Με εξαγόμενα χαρακτηριστικά από αποσυναρμολογημένα κακόβουλα δυαδικά αρχεία και χρησιμοποιήθηκε τυχαίος αλγόριθμος δάσους για την

ταξινόμηση κακόβουλου λογισμικού χρησιμοποιώντας τις εξαγόμενες δυνατότητες. Χρησιμοποιώντας ένα σύνολο δεδομένων 10.260 παρουσιών κακόβουλου λογισμικού, αναφέρθηκε ακρίβεια έως 99,21% (Hassen et al. 2017).

Μελέτες, τα προηγούμενα χρόνια πρότειναν μια τεχνική στατικής ανάλυσης για την ανίχνευση κακόβουλου λογισμικού IoT. Η προτεινόμενη τεχνική μετατρέπει ένα αρχείο κακόβουλου λογισμικού σε εικόνα σε κλίμακα του γκρι και εξάγει ένα σύνολο οπτικών χαρακτηριστικών από την εικόνα του κακόβουλου λογισμικού για να εκπαιδεύσει έναν ταξινομητή SVM που θα μπορούσε να διακρίνει μεταξύ οικογενειών κακόβουλου λογισμικού χρησιμοποιώντας οπτικές δυνατότητες. Χρησιμοποιώντας ένα σύνολο δεδομένων 9342 δειγμάτων που ανήκουν σε 25 οικογένειες κακόβουλου λογισμικού και αναφέρθηκε ακρίβεια 97,4% (Naeem et al. 2018). Επίσης, έχουν προταθεί πολλά έργα για τον εντοπισμό εφαρμογών κακόβουλου λογισμικού Android χρησιμοποιώντας τεχνικές στατικής ανάλυσης. Μελέτες έχουν προτείνει ένα μοντέλο ανίχνευσης κακόβουλου λογισμικού Android που χρησιμοποιεί άδεια εφαρμογής για τον εντοπισμό κακόβουλων εφαρμογών. Οι εν λόγω έρευνες χρησιμοποίησαν τα δικαιώματα που απαιτούνται από την εφαρμογή με μια λειτουργία σταθμισμένης απόστασης και τον ταξινομητή KNN και Naive Bayes για τον εντοπισμό κακόβουλων εφαρμογών και αναφέρθηκε ακρίβεια έως και 93,27% (OSahn et al. 2018).

Άλλοι ερευνητές έχουν προτείνει μια νέα μέθοδο ανίχνευσης κακόβουλου λογισμικού παρακολουθώντας κακόβουλες συμπεριφορές στην κίνηση του δικτύου. Σχεδίασαν 35 λειτουργίες για να περιγράψουν κακόβουλη κίνηση παρουσιών κακόβουλου λογισμικού. Δοκίμασαν, επίσης, διάφορους αλγόριθμους μηχανικής μάθησης, όπως CNN, MLP, SVM και τυχαίο δάσος. Η προτεινόμενη μέθοδος πέτυχε ακρίβεια άνω του 85% όταν χρησιμοποιήθηκε CNN ή τυχαίο δάσος. Αυτές οι τεχνικές προσπαθούν να βελτιώσουν την ποιότητα και την απόδοση των συστημάτων ανίχνευσης κακόβουλου λογισμικού για να δημιουργήσουν ένα ισχυρό σύστημα αυτής της μορφής (Yeo et al. 2018).



Εικόνα 22 - Απεικόνιση ανίχνευσης κακόβολου λογισμικού που βασίζονται σε ML (Xiao et al 2018)

Στην εικόνα 22 βλέπουμε το IoT να φιλτράρει τα πακέτα TCP και να επιλεγεί μεταξύ των χαρακτηριστικών διάφορες δυνατότητες δικτύου. Τις επισημαίνει και τις αποθηκεύει σε βάση δεδομένων. Η ανίχνευση κακόβολου λογισμικού βασίζεται στο K-NN που εκχωρεί την κίνηση στο δίκτυο βάσει του μεγαλύτερου αριθμού των αντικειμένων. Πριν από αυτό το Random Forest μέχρι τώρα ταξινομεί την επισκεψιμότητα με την ετικέτα διάκρισης κακόβολου λογισμικού. Είναι ουσιαστικά μια σύμπραξη δυο τεχνικών. Το ποσοστό επιτυχίας σύμφωνα με την βιβλιογραφία ακουμπάει το 99,7%

5.2 Αυθεντικοποίηση & Έλεγχος IoT

Η αυθεντικοποίηση είναι μία από τις πρωταρχικές απαιτήσεις ασφαλείας στο IoT. Οι χρήστες πρέπει να πιστοποιούνται για να χρησιμοποιούν εφαρμογές και υπηρεσίες αυτής της μορφής. Συνήθως, οι εφαρμογές και οι υπηρεσίες IoT βασίζονται στην ανταλλαγή δεδομένων σε διαφορετικές πλατφόρμες. Τα δεδομένα που ανακτώνται από τις συσκευές IoT είναι προ-επεξεργασμένα, υποβάλλονται σε επεξεργασία και στη συνέχεια διαβιβάζονται μέσω ενός συστήματος υποστήριξης αποφάσεων. Αυτές οι διαδικασίες ενδέχεται να ποικίλλουν ανάλογα με την υποκείμενη αρχιτεκτονική IoT. Ωστόσο, η ροή δεδομένων μπορεί να είναι ίδια σε αυτά τα συστήματα (Hussain et al. 2020).

Χωρίς απώλεια γενικότητας, όταν μια εφαρμογή και ένας χρήστης χρειάζονται ορισμένα δεδομένα από μια συσκευή IoT, η οντότητα (χρήστης ή εφαρμογή) πρέπει να πιστοποιηθεί στο δίκτυο IoT και θα πρέπει να διασφαλιστεί ότι ο αιτών έχει απαιτήσει δικαιώματα πρόσβασης για τα δεδομένα. Διαφορετικά, το αίτημα πρόσβασης σε τέτοια δεδομένα θα απορριφθεί. Όπως και σε άλλα δίκτυα, ο έλεγχος πρόσβασης είναι επίσης υψίστης σημασίας στα δίκτυα IoT και εξίσου απαιτητικός αλλά δεν περιορίζεται στην ετερογένεια του δικτύου, του όγκου δικτύου, των περιορισμών πόρων των συσκευών, της ασφάλειας δικτύου και στις επιθέσεις ευπάθειας κλπ (Hussain et al. 2020).

Γενικότερα, είναι σημαντικό να γνωρίζουμε πως στο IoT,ο αλγόριθμος ελέγχου πρόσβασης αποφασίζει εάν η νέα σύνδεση γίνεται αποδεκτή όταν η ποιότητα επικοινωνίας είναι ήδη εξασφαλισμένη. Όταν φτάσει μια νέα κλήση υπηρεσίας, εάν το εύρος ζώνης στην κοινότητα εξακολουθεί να είναι διαθέσιμο, η κλήση θα υποβληθεί σε επεξεργασία. Εάν δεν υπάρχει αρκετό εύρος ζώνης κατά την άφιξη μιας νέας κλήσης, η κλήση θα είναι κορεσμένη (απορρίπτεται) ή θα τεθεί στη λίστα αναμονής (Hutter et al. 2019).

Στο IoT, υπάρχουν δύο τύποι κλήσεων που χρειάζονται σύνδεση εισόδου. Το ένα είναι νέες κλήσεις υπηρεσιών που ξεκινούν από χρήστες κινητής τηλεφωνίας στην τρέχουσα κοινότητα ενώ το δεύτερο είναι η αλλαγή υπηρεσίας που απαιτείται από χρήστες κινητών σε άλλες κοινότητες για να στραφούν στην τρέχουσα κοινότητά τους. Από τη σκοπιά του χρήστη, μια διακοπή κατά τη διάρκεια της κλήσης είναι πιο αποδεκτή από το να μην μπορεί να πραγματοποιηθεί μια κλήση (Hussain et al. 2020).

Αυτός είναι ο λόγος για τον οποίο η υπηρεσία εναλλαγής έχει μεγαλύτερη προτεραιότητα στη στρατηγική ελέγχου εισδοχής. Στο IoT, διαφορετικά δίκτυα έχουν διαφορετικά χαρακτηριστικά. Το IoT παρέχει περιορισμένο εύρος ζώνης υπηρεσίας, αλλά έχει μικρή καθυστέρηση μετάδοσης. Το ασύρματο LAN μπορεί να αυξήσει το εύρος ζώνης υπηρεσίας, αλλά έχει μεγάλη καθυστέρηση μετάδοσης (Serpanos and Wolf 2018).

Οι ροές υπηρεσιών μπορούν να χαρακτηριστούν ως διαφορετικά επίπεδα υπηρεσίας και μεταδίδονται σε ξεχωριστά δίκτυα, τα οποία βελτιώνουν την ποιότητα υπηρεσιών ολόκληρου του δικτύου IoT. Όσον αφορά τους κόμβους στο διασυνδεδεμένο δίκτυο IoT, η ροή δεδομένων που λαμβάνεται ή αποστέλλεται μπορεί να χωριστεί σε κόμβους στο δίκτυο IoT. Οι αρχές διαίρεσης ποικίλλουν ανάλογα με τις απαιτήσεις υπηρεσίας (Naeem et al. 2018).

Η διαιρεμένη ροή δεδομένων μπορεί να μεταδοθεί μόνο σε IoT. Η ροή συγκλίνει όταν η ροή δεδομένων φτάνει στο τερματικό ή οι κόμβοι μπορούν να βελτιωθούν έτσι ώστε να υπάρξει και η ανάλογη βελτίωση στην ποιότητα των υπηρεσιών στο δίκτυο IoT. Ως εκ τούτου έχει σχεδιαστεί ένας νέος αλγόριθμος ελέγχου εισαγωγής IoT. Όταν φτάσει μια νέα σύνδεση, ο μηχανισμός ελέγχου εισδοχής θα κρίνει εάν υπάρχουν δωρεάν πόροι για διασυνδεδεμένα δίκτυα που ξεκινούν αιτήματα σύνδεσης. Θα αποφασίσει επίσης ποιος μηχανισμός απαιτείται για την αποδοχή του τρέχοντος αιτήματος σύνδεσης (Yeo et al. 2018).

Όταν έχουμε προγραμματισμό ροής σε πολλές υπηρεσίες στο δίκτυο IoT, όλες οι υπηρεσίες αναμονής και προτεραιότητας ροών δεδομένων είναι υπεύθυνες για τον ενιαίο προγραμματιστή ροής και βρίσκονται υπό τον έλεγχο της ενιαίας εισαγωγής. Ο αλγόριθμος ελέγχου εισαγωγής βελτιστοποιεί τον όγκο του συστήματος και μειώνει την πτώση της ποιότητας που προκαλείται από την αύξηση του ρυθμού έλλειψης δεδομένων έτσι ώστε και τα δύο να μπορούν να εξισορροπηθούν. Είναι εύκολο να ελεγχθεί η συγκέντρωση χρησιμοποιώντας τη διαχείριση πόρων βάσει στρατηγικής (Hutter et al. 2019).

Με τη χρήση μιας τέτοιας μεθόδου, η κατάσταση του δικτύου μπορεί να έχει συνέπεια και η διαχείριση του IoT διαφορετικών τεχνολογιών δικτύου μπορεί να γίνεται από κοινού. Οι μέθοδοι που βασίζονται στη συγκεκριμένη στρατηγική διευκολύνουν την εφαρμογή ενιαίου ελέγχου επί ετερογενών δικτύων και τη δημιουργία τοπικού ελέγχου σε υπο-δίκτυα χρησιμοποιώντας ιεραρχικό μηχανισμό στρατηγικής. Ένας ρόλος αντιπροσωπεύει μια συγκεκριμένη λειτουργία μέσα σε έναν οργανισμό και μπορεί να θεωρηθεί ως ένα σύνολο δράσεων ή ευθυνών που σχετίζονται με αυτήν τη λειτουργία (Hassan 2018).

5.3 Πώς η Μηχανική Μάθηση μας δίνει την λύση – Τι μπορεί να αντιμετωπίσουμε ;

Σε προηγούμενο κεφάλαιο έγινε ήδη αναφορά στο ότι η μηχανική μάθηση αποτελεί κλάδο του γενικότερου φάσματος της τεχνικής νοημοσύνης. Η μηχανική μάθηση λοιπόν χρησιμοποιεί αλγορίθμους που βοηθούν τις ίδιες τις συσκευές να μαθαίνουν από την ήδη προυπάρχουσα εμπειρία τους. Αποτελείται κυρίως από μεθόδους με μαθηματικούς αλγορίθμους και λειτουργούν δια δραστικά σε πολλούς τομείς. Τα τελευταία χρόνια οι τεχνικές του ML έχουν σημείωση αξιοσημείωτη πρόοδο στους σκοπούς ασφαλείας των IoT. Χρησιμοποιούνται για τον εντοπισμό επιθέσεων σε πρώιμο στάδιο με ανάλυση συμπεριφοράς συσκευών (Hussain et al. 2020).

Η μηχανική μάθηση μπορεί αν όχι να μας διασφαλίσει στο έπακρο την ασφάλεια στα devices του IoT να μας διευκολύνουν δεόντως παρέχοντας μας μια σειρά από τρόπους για να ελέγχουμε ότι τα δεδομένα μας κρατούν τους 3 βασικούς πυλώνες της ασφάλειας.

Στην συνέχεια και βήμα - βήμα θα διαπιστώσουμε το πως μπορούμε να πέτυχουμε αυθεντικοποίηση, να εντοπίσουμε ανωμαλίες που προκύπτουν και μας δίνουν το έρισμα ότι κάτι είναι λάθος. Χρησιμοποιούνται σχεδόν όλα τα είδη της μάθησης που παρουσιάστηκαν στο ανάλογο κεφάλαιο όπως επίσης και σχεδόν όλα τα μοντέλα σε κάθε είδος. Συνοψίζοντας μπορεί να αναφερθεί ότι υλοποιείται ένα είδους σχεδίου που καταφέρνει να κάνει το θεωρητικό κομμάτι πρακτικό ώστε να μας προστατεύει. Θα γίνει περιήγηση στους τρόπους διασταυρώσεις για τον εντοπισμό προβλημάτων και επιθέσεων, θα παρουσιαστούν πάρα πολλά μοντέλα που έχουν ως απόδειξη τα ίδια τα αποτελέσματα που προέκυψαν τόσο από τα πειραματικά στάδια όσο και από την τωρινή πραγματική κατάσταση (Hussain et al. 2020).

Με την χρήση μηχανικής μάθησης μπορούμε μετά βεβαιότητας να πούμε ότι είμαστε σε θέση να μετριάσουμε η να εξολοθρεύσουμε σοβαρές απειλές του IoT.

5.3.1 Authentication & Access Control in IoT

Συνηθίζεται στις εφαρμογές και στις υπηρεσίες του IoT όλα να βασίζονται στην ανταλλαγή δεδομένων σε διαφορετικές πλατφόρμες. Ο έλεγχος ταυτότητας είναι μια από τις κυρίες απαιτήσεις ασφαλείας στο IoT. Οι χρήστες όπως έχει αναφερθεί πολλάκις και παραπάνω οφείλουν να είναι πιστοποιημένοι ώστε να έχουν την δυνατότητα να χρησιμοποιήσουν τις εν λόγω υπηρεσίες ή τις εφαρμογές. Τα δεδομένα που ανακτώνται από τις συσκευές IoT έχουν υποστεί ήδη κάποια επεξεργασία και είναι πιθανόν να υποβληθούν σε εκ νέου. Στην συνέχεια διαβιβάζονται μέσω ενός συστήματος υποστήριξης αποφάσεων ώστε να εξάγουν τα ακόλουθα αποτελέσματα – συμπεράσματα. Όλη αυτή η διαδικασία όπως έγινε εξάλλου γνωστό ποικίλλει ανάλογα με την αρχιτεκτονική που ακολουθείται από το εκάστοτε IoT. Υπενθυμίζεται ότι ο έλεγχος πρόσβασης είναι υψίστης σημασίας καθώς αποτελεί έναν από τους πυλώνες της ασφάλειας. Στα δίκτυα IoT είναι αρκετά απαιτητική η ασφάλεια λόγω ετερογένειας, περιορισμένων πόρων, όγκου δικτύου και διάφορων επιθέσεων ευπάθειας. Επιπροσθέτως, μην λησμονούμε ότι οποιαδήποτε στιγμή και αν απαιτηθεί πρέπει να έχει διασφαλιστεί η

ανάκληση της πρόσβασης από κάποιον χρήστη στα δεδομένα εφαρμογών και υπηρεσιών (Hussain et al. 2020).

Πριν αναλυθούν οι μηχανισμοί ελέγχου πρόσβασης που βασίζονται στην μηχανική μάθηση θα είναι εξίσου χρήσιμο να αναφερθούν οι διάφορες κατηγορίες που υπάρχουν στον έλεγχο αυτό. Στους μηχανισμούς ελέγχου πρόσβασης υπάρχει μια έντονη διαφωνία ως προς τον αριθμό τους όπως εξάλλου έχουμε ήδη συνηθίσει να συμβαίνει στον τομέα αυτό καθώς αποτελεί μια νέα καινοτομία – τεχνολογία. (Hussain et al. 2020). Πολλοί ήταν εκείνοι που ισχυρίζονται ότι οι κατηγορίες είναι τρεις (3) και είναι οι ακόλουθες:

α) Έλεγχος πρόσβασης βάσει ρόλου (RBAC)

β) Έλεγχος πρόσβασης περιβάλλοντος (CWAC)

γ) Έλεγχος πρόσβασης βάσει πολιτικής (PBAC)

Η παραπάνω ταξινόμηση επεκτάθηκε από κάποιους σε περισσότερες κατηγορίες που περιλαμβάνουν και τα ακόλουθα:

δ) Έλεγχος πρόσβασης βάσει χαρακτηριστικών (ABAC)

ε) Έλεγχος πρόσβασης βάσει ελέγχου χρήσης (UCAC)

ζ) Έλεγχος πρόσβασης βάσει ικανότητας (CAC)

η) Έλεγχος πρόσβασης βάσει οργανισμού (OAC)

Για να κατανοήσουμε τώρα το πως χρησιμοποιούνται οι μηχανισμοί αυτοί πρέπει να σκεφτούμε που χρησιμοποιούνται στην καθημερινότητα μας οι εφαρμογές IoT. Επί της ουσίας υπάρχουν 2 μεγάλες κατηγορίες, οι εφαρμογές που χρησιμοποιούνται για προσωπική χρήση και οι εφαρμογές που χρησιμοποιούνται σε επιχειρήσεις. Όταν αναφερόμαστε σε προσωπικές εφαρμογές εννοούμε εκείνες που χρησιμοποιούνται στα έξυπνα σπίτια, έξυπνο γραφείο, σε συνδυασμό με τους αισθητήρες σώματος για βελτίωση της υγείας μας, στα δίκτυα αισθητήρων και άλλες. Απ' την άλλη οι εφαρμογές που συναντάμε σε επιχειρήσεις έχουν να κάνουν με έξυπνες βιομηχανίες, κρίσιμες υποδομές, επιχειρηματικές εφαρμογές και ούτω καθεξής (Hussain et al. 2020).

Ο μηχανισμός ελέγχου πρόσβασης λοιπόν μπορεί να χρησιμοποιηθεί σε επίπεδο εφαρμογής αλλά και σε επίπεδο αρχιτεκτονικής. Στο επίπεδο της αρχιτεκτονικής οι πάροχοι υπηρεσιών έχουν ορίσει μια γλώσσα σήμανσης για τον έλεγχο πρόσβασης. Αυτή η γλώσσα σήμανσής μπορεί να είναι η XACML ή κάποιου είδους Open Authorization (OAuth). Το Open Authorization αναφέρθηκε και προηγούμενα καθώς χρησιμοποιείται κατά χιλιάδες αφού το έχουν συμπεριλάβει υπηρεσίες μεγάλων εταιρειών όπως το Facebook, το Netflix, το Instagram σε δισεκατομμύρια λογαριασμούς χρηστών. Το αποκαλούμενο OAuth εφαρμόζεται σε υπάρχοντα πρωτόκολλα IoT και συνεργάζεται με

αυτά όπως το MQTT ή το CoAP (Hussain et al. 2020).

Στο επίπεδο υπηρεσίας λοιπόν, ο μηχανισμός ελέγχου πρόσβασης που προτάθηκε βασίζεται σε CoAP εφαρμογές IoT που καθοδηγούνται από την αρχιτεκτονική προσανατολισμένη στην υπηρεσία (SOA). Μπορεί να υπάρχουν στο πρωτόκολλο TCP/IP μηχανισμοί όπως το IPSec, SSL, DTLS και TLS που είναι αναγκαίοι για το SOA αλλά αυτοί δεν δουλεύουν στο CoAP σε εφαρμογές δηλαδή IoT. Έτσι λοιπόν, το πρόβλημα ξεπεράστηκε χρησιμοποιώντας μηχανισμούς Kerberos και RADIUS με CoAP ώστε να δίνεται η απόλυτη πληρότητα και να παρέχεται λεπτομερής έλεγχος πρόσβασης για τις υπηρεσίες.

Μπορούμε να πούμε όμως, ότι και πάλι το πρόβλημα δεν ξεπεράστηκε τουλάχιστον στο έπακρο και αυτό γιατί υπάρχουν εφαρμογές που τα δεδομένα που περιέχουν δεν πρέπει ουδέποτε να παραβιαστούν. Αυτές οι εφαρμογές μπορεί να είναι κάποιες υγειονομικής περίθαλψης και άλλες ιδιωτικές εφαρμογές που περιέχουν αυστηρώς απόρρητα δεδομένα και απαιτούν έναν αδιαπέραστο έλεγχο πρόσβασης. Έτσι προτάθηκαν νέοι προσαρμοστικοί μηχανισμοί ελέγχου που αρχικώς αποθηκεύονται σε κάποιο cloud τα δεδομένα σε κρυπτογραφημένη μορφή.

Με τον μηχανισμό αυτό παρέχονται πολύπλευρες δυνατότητες όπως η ανταλλαγή δεδομένων, ύπαρξη σεναρίου έκτακτης ανάγκης και ο καθορισμός πολίτικων βάση δικαιωμάτων πρόσβασης. Εν ολίγοις, μετά την νέα επέκταση ο μηχανισμός βασίζεται σε κρυπτογραφικά θεμελιακά στοιχεία όπως η μυστική κοινή χρήση , η διγραμμικη σύζευξη και η επανακρυπτογράφηση Ciphertect. Η αποκαλουμένη κρυπτογράφηση CP-ABE μαζί με άλλους τρόπους κρυπτογραφίας όπως το MHTs προσπάθησαν να δώσουν το καλύτερο αποτέλεσμα στο ζητούμενο μας την ασφάλεια. Το edge computing platform μπορεί να αναλάβει ένα κομμάτι της εργασίας αυτής, δηλαδή να γίνει εξωτερική ανάθεση των κρυπτογραφικών συναρτήσεων. Έτσι καταλήγουμε στην ακόλουθη ροή. Αρχικώς τα δεδομένα του κατόχου κρυπτογραφούνται με βάσει τα χαρακτηριστικά και μετά από χρήση πολλαπλών πολιτικών και εν συνέχεια μεταφέρονται στο cloud / edge platform

Στον βιομηχανικό κόσμο τώρα συναντάμε μηχανισμούς όπως το Blockchain που έχουν αξιοποιηθεί για να εγγυηθούν τον έλεγχο πρόσβασης στα IoT με μεγάλα έξοδα όμως. Μέσα από διαδικασίες και μεγάλες προσπάθειες ώστε να μειωθεί το κόστος των τεχνικών αποφασίστηκε να δημιουργείται μια «καμπίνα ασφαλείας» με τα δικαιώματα πρόσβασης να βρίσκονται εκεί και να ανακαλούνται για χρήση όταν γίνει η αυθεντικοποίηση. (Hussain et al. 2020).

Εύλογα μπορούμε να αναρωτηθούμε στο που μας έχει βοηθήσει στον έλεγχο ταυτότητας και πρόσβασης σε δίκτυα IoT η μηχανική μάθηση.

Ένας έλεγχος ταυτότητας συνήθως χρησιμοποιεί φυσικές ιδιότητες καναλιού όπως για παράδειγμα την ισχύ του σήματος. Έτσι ένας πολύ διαδιδόμενος έλεγχος, το

ANN έχει αξιοποιηθεί για τη αντιμετώπιση του προβλήματος. Ουσιαστικά, ο έλεγχος ταυτότητας με βάση τη μη κλωνική λειτουργία PUF μπορεί να είναι αποτελεσματικός στο IoT όπου οι φυσικές ιδιότητες του πομπού αναλύονται σε περίπτωση διαφοροποιήσεις απορρίπτονται υπό μορφή θορύβου. Με αυτό ακριβώς το σκεπτικό χρησιμοποιήθηκε αλγόριθμος ML για την ταξινόμηση των πομπών. Ο αλγόριθμος ML εφαρμόζεται στο δέκτη και έτσι γίνεται η εξαγωγή των δεδομένων για την επιτυχή αναγνώριση και ταξινόμηση των πομπών. Με λίγα λόγια, εφαρμόζεται ο τρόπος λειτουργίας της μηχανικής μάθησης ταξινόμηση που αναφερθήκαμε παραπάνω σε συνδυασμό με τις φυσικές ιδιότητες των IoT συσκευών ώστε να γίνει η διαλογή «καλού» και «κακού». Μετά από συνεχόμενες δοκιμές και πειραματισμούς το σφάλμα ανίχνευσης είναι ελάχιστο και από την άποψη της απόδοσης δεν υπάρχει επιβάρυνση από τον πομπό, ενώ ο δέκτης χρειάζεται 2 νευρωνικά δίκτυα. Τα 2 αυτά νευρωνικά δίκτυα υπολογίζονται ως ανάγκη για επιπλέον ισχύ της τάξεως του 3% (Hussain et al. 2020).

Το Deep Learning έχει εξίσου χρησιμοποιηθεί για έλεγχο ταυτότητας χρήστη σε IoT. Το πρώτο εγχείρημα που συναντάμε βασίζεται σε ανθρώπινές φυσιολογικές δραστηριότητες μέσω σημάτων WiFi. Γίνεται ένα είδους αναγνώρισης δραστηριότητας. Η δραστηριότητα αυτή προκύπτει από τις πληροφορίες κατάστασης του καναλιού σε σήματα WiFi που δημιουργούνται γύρω από συσκευές IoT. Αυτά που προκύπτουν τα κατατάσσουμε σε τρία επίπεδα DNN. Το πρώτο επίπεδο στο Deep Neural Network εξάγει τον τύπο δραστηριότητας, στο δεύτερο μαθαίνει λεπτομέρειες της δραστηριότητας αυτής και στο τρίτο μαθαίνει χαρακτηριστικά υψηλού επιπέδου και βάσει αυτών γίνεται και η πιστοποίηση. Αν κάνουμε μια αναδρομή σε αυτά που ήδη έχουμε διαβάσει στην διπλωματική, το όλο μοντέλο έχει αναλυθεί εκ νέου στο κεφάλαιο της μηχανικής μάθησης και των διαχωρισμών βάσει χαρακτηριστικών. Αυτό το θεωρητικό κομμάτι λοιπόν γίνεται πράξη επί της ουσίας που μας βοηθάει πάρα πολύ (Hussain et al. 2020).

Ένας ακόμα μηχανισμός ταυτότητας υλοποιείται με βάση το LSTM σε δίκτυα IoT χαμηλής ισχύος. Το LSTM αξιοποιείται για να μάθει για τις ατέλειες υλικού με διαφορετικές συχνότητες. Αυτό επηρεάζει την ισχύ του σήματος. Το αναπτυγμένο μοντέλο DL μαθαίνει αυτές τις ατέλειες και προσδιορίζει τους χρήστες με βάση αυτές τις δυνατότητες. Μάλιστα, στο Machine Learning και στο Deep Learning η διαδικασία της μάθησης είναι ένα καθοριστικό σημείο για την μετέπειτα εξέλιξη, άρα είναι πολύ κρίσιμο να γίνει η όλη διαδικασία παρουσία επιτιθέμενων, κάτι σαν εμβόλιο δηλαδή (Hussain et al. 2020).

Σε Smart Home προτάθηκε ως λύση η χρησιμοποιήσει ενός RNN σε συνδυασμό της ακουστικής και των φωνητικών εντολών. Μάλιστα, όπως προκύπτει και από την βιβλιογραφία το RNN ξεπερνά λύσεις που βασίζονται σε SVM και LSTM για την συγκεκριμένη περίπτωση.

Διαπιστώνουμε λοιπόν, ότι έχουμε λύσεις που προκύπτουν συνδυαστικά. Πάρα ταύτα, ότι έχουμε ένα καλό αποτέλεσμα στην μια περίπτωση δεν μας εξασφαλίζει ότι και στην επόμενη περίπτωση θα υπάρξει το ίδιο. Όλο αυτό μας επιβεβαιώνει ότι όλα τα παραπάνω με τα αμφίβολα αποτελέσματα γίνονται λόγο ανομοιογένειας.

5.3.2 Attack Detection and Mitigation

Οι επιθέσεις που συναντάμε σε γενικότερη κλίμακα στα δίκτυα ποικίλουν. Έτσι και στο IoT μπορούμε να βρούμε επίθεση με χαμηλό προφίλ εισβολής σε μια συσκευή έως μεγάλη μαζική κλίμακας επίθεση ransomware. Γνωστές επιθέσεις όπου έχουν προκαλέσει σοβαρές ζημίες τα προηγούμενα χρόνια είναι οι Mirai, το Dvn αλλά και το Wanacry. Οι μηχανισμοί ανίχνευσης εισβολών βασίζονται και αυτές σε κρυπτογραφικά θεμελιώδη στοιχεία έχοντας όμως παράλληλα ένα σοβαρότατο πρόβλημα που τους ταλανίζει. Αυτό το πρόβλημα δεν είναι άλλο από τους ψευδούς συναγερμούς. Υπάρχει έλλειψη ακρίβειας και έχουμε θετικά αποτέλεσμα ως διάγνωση επίθεσης ορισμένες φορές που είναι λανθασμένα. Κατά κύρια βάση, χρησιμοποιούνται τεχνικές όπως το SVM, το Deep Learning, το K-NN και η μη εποπτευόμενη μάθηση (Hussain et al. 2020).

Στον κόσμο του IoT τώρα ο προτεινόμενος τρόπος αντιμετώπισης τέτοιων καταστάσεων είναι η χρήση ενός ημί - εποπτευόμενο μηχανισμό με βάση τη μάθηση. Μέσω του αλγορίθμου ELM και αξιοποιώντας μεθόδους FCM καταλήγουμε σε ένα επαρκέστατο αποτέλεσμα. Αυτά τα δυο μαζί αναφέρονται συλλογικά ως ESFCM. Στον ESFCM λοιπόν, συναντάμε ένα αυξημένο ποσοστό ανίχνευσης κατανεμημένων επιθέσεων και αυτό συμβαίνει καθώς χρησιμοποιεί δεδομένα με «ετικέτα». Πάρα ταύτα τα ποσοστά ακριβείας ανίχνευσής που εξάγουμε στον ESFCM είναι μικρότερα από εκείνα της μηχανικής μάθησης και της βαθειάς μάθησης. Αυτό όμως δεν σημαίνει ότι μας είναι άχρηστος κάθε άλλο γιατί μπορεί τα ποσοστά ανίχνευσης να είναι μικρότερα δεν παραβλέπετε όμως το γεγονός ότι εκμεταλλεύεται τα θετικά από δυο είδη μάθησης με τα αποτελέσματα της αντιμετώπισης αυτών που ανιχνεύτηκαν να είναι συντριπτικώς επιτυχημένα (Hussain et al. 2020) .

Στην ανίχνευση εισβολών λοιπόν έχουν διερευνηθεί και ο ρόλος της εποπτευόμενης μάθησης και της ημί - εποπτευόμενης μάθησης αλλά και της συγχώνευσης μεταξύ των μοντέλων των αλγορίθμων. Τα συμπεράσματα λοιπόν που προέκυψαν και σύμφωνα και με τις βιβλιογραφικές πηγές για μικρά δίκτυα IoT η ιδανικότερη λύση που αποδίδει σε μεγαλύτερο βαθμό είναι η χρήση K-NN. Αντιθέτως το SVM αποδίδει καλυτέρα όσον αφορά την ακρίβεια. Σε πραγματικό χρόνο οι αποδόσεις αξιολογούνται ως όμοιες (Hussain et al. 2020).

5.3.3 DoS & Distributed DoS (DDoS) Attacks

Οι επιθέσεις με την μορφή DDoS Attack ίσως να είναι οι πιο διαδομένες επιθέσεις που υπάρχουν. Μεγάλες εταιρείες και επιχειρήσεις έχουν πέσει θύματα τέτοιων επιθέσεων και συνέχεια γίνονται γνωστές νέες επιθέσεις τύπου DDoS. Για τις μεγάλες εταιρείες μάλιστα μια τέτοια επίθεση προκαλεί ζημιά πολλών εκατομμυρίων καθώς βγάζει εκτός λειτουργίας από ένα απλό site έως ολόκληρα συστήματα. Όσον αφορά τα δίκτυα IoT αξίζει να σημειωθεί ότι μόλις το 2016 σημειώθηκε μια άνευ προηγούμενη αύξηση σε επιθέσεις εναντίων υποδομών IoT με τεράστιά κλίμακα. Πολλές συσκευές τα καλούμενα ως IoT devices βοήθησαν ως bots για να πραγματοποιηθεί αυτή η επίθεση. Μπορούμε να αναφέρουμε ότι επλήγησαν δίκτυα όπως οικιακές συσκευές, βρεφικές κάμερες, εκτυπωτές, κάμερες web ώστε να γίνει η εκκίνηση επιθέσεων DDoS σε πολλούς οργανισμούς. Στις επιθέσεις DDoS χρησιμοποιούνται εκατοντάδες χιλιάδες συσκευές

ώστε να «ρίξουν» ένα σύστημα. Γι' αυτόν ακριβώς τον λόγο μέχρι σήμερα έχουν πραγματοποιηθεί πολλά ερευνητικά project με αξιόλογα ερευνητικά αποτελέσματα ώστε να αντιμετωπισθεί ή έστω να μετριασθούν οι επιθέσεις. Όπως έχει αναφερθεί ήδη σχεδόν σε κάθε είδους επίθεση οι διαφορετικές πλατφόρμες του IoT και εδώ μας δημιουργούν μείζον πρόβλημα για την καταπολέμηση τους. Είναι πάρα πολύ δύσκολο να δημιουργηθεί ένας ενιαίος κοινά αποδεχούμενος ενοποιημένος μηχανισμός που να μας δίνει την λύση (Hussain et al. 2020).

Οι παραδοσιακοί μηχανισμοί ανίχνευσης και πρόληψης για την καταπολέμηση του DDoS στα δίκτυα IoT εφαρμόζεται στους δρομολογητές, στα gateways και στα σημεία εισόδου δικτυών IoT. Όπως αναφέρθηκε και προηγουμένως τα MQTT και CoAP είναι δυο από τα πιο ευρέως χρησιμοποιούμενα πρωτόκολλα τηλεμετρίας στο IoT. Με την χρήση αυτών αλλά και με τεχνολογίες αιχμής όπως το fog και το cloud computing γίνεται προσπάθεια η ανίχνευση DDoS σε IoT. Τα δίκτυα που είναι οριζόμενα από το λογισμικό ή αλλιώς SDN έχουν καταφέρει να αναχαιτίσουν σε μεγάλο βαθμό το πρόβλημα αυτό. Το SDN χρησιμοποιείται στο χαμηλότερο επίπεδο και επεξεργάζοντας τα δεδομένα κίνησης του δικτύου. Οι controllers που διαθέτουν τα SDN προσπαθούν να εντοπίσουν DDoS επιθέσεις πριν συμβούν. Δυστυχώς, όμως όλα τα παραπάνω δεν μας έχουν δώσει μια δυναμική λύση όπου και να είναι εφαρμόσιμη σε κάθε περίπτωση. Όλα τα παραπάνω δουλεύουν υπό προϋποθέσεις. Έτσι, η μηχανική μάθηση προσπαθεί και εκείνη με την σειρά της να αντιμετωπίσει την κατάσταση αυτή και να δώσει λύση με τους τρόπους που δίνονται παρακάτω (Hussain et al. 2020).

Για να βρεθεί μια αξιόπιστη λύση έχει γίνει σύγκριση μεθόδων της μηχανικής μάθησης όπως οι K-πλησιέστεροι γείτονες, τα δέντρα αποφάσεων, τα νευρωνικά δίκτυα, το RF και το SVM. Η χρήση λοιπόν της μηχανικής μάθησης, μας δίνει ουσιαστικά την λύση σε επιθέσεις DDoS καθώς εντόπισαν με επιτυχία τις επιθέσεις αυτές με ακρίβεια 99%. Αυτό επιτυγχάνεται καθώς έγινε αύξηση στα διακριτικά χαρακτηριστικά κυκλοφορίας του IoT όπου οι συσκευές IoT ασχολούνται συνήθως μόνο με μια πεπερασμένη επικοινωνία, με τελικά σημεία και όχι με διακομιστές back to end. Όμως, δεν είναι πάντα εφικτή η αύξηση στα διακριτικά χαρακτηριστικά όποτε έγιναν προσπάθειες να εντοπιστούν και άλλοι μέθοδοι. Μια απ' αυτές ήταν η χρήση SVM στα δεδομένα κίνησης που συλλέχθηκαν από τον ελεγκτή SDN. Επίσης έγινε σύγκριση και άλλων τεχνικών όπως οι Naive Bayes και η RFB. Το SVM όμως αποδείχτηκε πιο αποτελεσματικό από τα προαναφερθέντα με το αρνητικό του στοιχείο να εντοπίζεται στην υποχρεωτική χρήση του παράλληλα με SDN. Αποτέλεσμα τα δίκτυα που δεν βασίζονται στο SDN δεν μπορούν να χρησιμοποιήσουν αυτή την μέθοδο της μηχανικής μάθησης (Hussain et al. 2020).

Άλλη τεχνική ML που μπορεί να χρησιμοποιηθεί για την ανίχνευση DDoS είναι η MCA. Ο μηχανισμός ανίχνευσης DDoS που βασίζεται σε MCA επικεντρώνεται στην πλευρά του διακομιστή και στο πλαίσιο του IoT. Ο μηχανισμός είναι σε θέση να εντοπίσει την επίθεση DDoS ως αποτέλεσμα της ροής δεδομένων μεταξύ των διακομιστών back-end για τη συλλογή δεδομένων, την επεξεργασία και τη λήψη αποφάσεων. Τα αποτελέσματα που εξάγονται βασίζονται σε συμπεριφορική ανάλυση της κυκλοφορίας. Όταν υπάρχει κάποια παρεμβολή ή γενικότερα κάποια διαταραχή στη συσχέτιση μεταξύ

των χαρακτηριστικών αυτό θα μπορούσε να αποτελέσει ένδειξη πιθανής παραβατικής δραστηριότητας. Το MCA έχει σχεδόν το απόλυτο επιτυχημένο αποτέλεσμα στην συνολική ακρίβεια (Korenda et al. 2019).

Μια ακόμη τεχνική ML στο συγκεκριμένο τρόπο επίθεσης θεωρείται το SIRN. Από την στιγμή που υπάρχει μια σχετική σταθερότητα της κατανάλωσης ισχύος μετάδοσης για τον αισθητήρα όλα κυλούν ομαλά. Απ' εκεί και πέρα υπάρχει μια οριοθέτηση και στην κατανάλωση ισχύος παρεμβολής ενός εισβολέα και υπάρχει ένα είδους παιχνίδι μεταξύ αισθητήρα και επιτιθέμενου. Για να δημιουργηθεί αυτό το «παιχνίδι» έχει χρησιμοποιηθεί στον υπολογισμό της σταθερότητας ένας αλγόριθμος βασιζόμενος στο Nash Q Learning. Αν η ισορροπία αυτή χαλάσει τότε το παιχνίδι τελειώνει και υπάρχει εισβολέας (Korenda et al. 2019). Τέλος, να αναφερθεί ότι τα τεχνικά νευρωνικά δίκτυα (ANNs) χρησιμοποιούνται και αυτά στο να αποτρέψουν το DDoS στο IoT (Hussain et al. 2020).

5.3.4 Anomaly / Instrusion Detection

Έως τώρα έχουν χρησιμοποιηθεί αρκετές τεχνικές που βασίζονται σε ML για τον εντοπισμό ανωμαλιών και εισβολών στα δίκτυα IoT και στις διαφορές που υπάρχουν στις συσκευές τους. Στο πεδίο του IoT, χρησιμοποιούνται διάφορα μοντέλα ταξινόμησης κυκλοφορίας και συμπεριφοράς. Το φιλτράρισμα κυκλοφορίας, ένας από τους μηχανισμούς ανίχνευσης, όπου πραγματοποιείται ανάλυση των πληροφοριών για την απομόνωση πληροφοριών από τα κακόβουλα λογισμικά, θεωρείται μια αποτελεσματική μέθοδος αλλά βέβαια αμφισβητείται έντονα η αξιοπιστία της (Hussain et al. 2020).

Επιπλέον, μια τεχνική που βασίζεται στην εμπιστοσύνη, χρησιμοποιεί το επίπεδο εμπιστοσύνης σε συνδυασμό με τον τύπο και την κατηγορία της κυκλοφορίας. Ο καλύτερος συνδυασμός θεωρείται η διαχείριση εμπιστοσύνης με την ταξινόμηση επισκεψιμότητας για εντοπισμό εισβολής σε IoT. Ωστόσο, είναι σημαντικό να σημειωθεί ότι τα παραδοσιακά σχήματα που βασίζονται στην υπογραφή και στη συμπεριφορά αποτυγχάνουν να εντοπίσουν εισβολές με μηδενική επισκεψιμότητα στην ημέρας. Συμπεραίνουμε ότι, η τεχνητή νοημοσύνη χρησιμοποιείται στο σύστημα ανίχνευσης εισβολής (IDS), και μπορεί να ανιχνευσεί μια εισβολή σε IoT όταν ένας μηχανισμός τεχνητής νοημοσύνης (AI) βασίζεται σε SDN (Hussain et al. 2020).

Επιπροσθέτως, οι μηχανισμοί ασφαλείας, ο έλεγχος πρόσβασης και οι τεχνικές προστασίας δεν είναι ομοιογενείς σε διαφορετικές πλατφόρμες IoT. Επομένως, για να αντιμετωπιστεί το ζήτημα της ανίχνευσης εισβολής σε διαφορετικές τεχνολογίες διεξάχθηκαν έρευνες τεχνικών ανίχνευσης εισβολής σε διαφορετικά πρότυπα δικτύωσης, IDS σε ασύρματα δίκτυα αισθητήρων (Hussain et al. 2020).

Ακόμα παραθέτετε μια μεταανάλυση που πραγματοποιήθηκε από τους Benkhelifa et al. για την αρχιτεκτονική για το IDS στο IoT όπου αναφέρει υπάρχοντα πρωτόκολλα, μεθόδους ανίχνευσης και μελλοντικές ερευνητικές προκλήσεις για το

σύστημα αυτό.

Στη μεταανάλυση των Benkhelifa et al. (2018) αρχικά αναλύεται για IDS που βασίζονται σε ML στο IoT όπου παραθέτετε μια έρευνα των Shukla et al. (2017) που χρησιμοποιεί ελαφρύ IDS βασισμένο σε ML για δίκτυα IoT χαμηλής ισχύος που εκτελούν 6LoWPAN. Στην έρευνα χρησιμοποίησαν τον μηχανισμό IDS για τον εντοπισμό επιθέσεων τύπου wormhole σε δίκτυα IoT. Ο μηχανισμός IDS χρησιμοποιεί τρεις τεχνικές ML, δηλαδή την ομαδοποίηση με K-τρόπους (μη εποπτευόμενη μάθηση) 70-93% ανίχνευση ανάλογα με το μέγεθος του δικτύου, το δέντρο αποφάσεων (εποπτευόμενη μάθηση) 71-80% ρυθμό ανίχνευσης και μια υβριδική τεχνική που συνδυάζει τις προαναφερθείσες τεχνικές με 71-75% στα δίκτυα IoT. Η έρευνα καταλήγει στο συμπέρασμα ότι παρά το χαμηλό ποσοστό ανίχνευσης, ο υβριδικός μηχανισμός είναι πιο ακριβής από τους δύο προηγούμενους μηχανισμούς. Από την άλλη πλευρά, οι Canedo et al. (2016) αξιοποίησαν δύο τεχνικές ML για τον εντοπισμό εισβολών στις πύλες IoT. Οι συγγραφείς χρησιμοποίησαν ANN και γενετικούς αλγόριθμους (δύο και τρεις νευρώνες εισόδου) για την ασφάλεια του IoT. Τα αποτελέσματα έδειξαν ότι ποσοστό πρόβλεψης ανωμαλιών ήταν ακόμη πάνω από 99% με 1% ψευδώς αρνητικό και στις δυο περιπτώσεις των νευρώνων (Hussain et al. 2020).

Άλλες τεχνικές ML που χρησιμοποιούνται για την ανίχνευση εισβολής και ανωμαλίας περιλαμβάνουν την ανίχνευση Naïve Bayes, RNN, δέντρο αποφάσεων και DL. Στην έρευνα των Nesa et al. (2018) οι υλοποιητές χρησιμοποίησαν έναν μηχανισμό ανίχνευσης ακραίων τιμών για την αντιμετώπιση των μη χρήσιμων ή μολυσματικών δεδομένων στα δίκτυα IoT. Οι συγγραφείς χρησιμοποίησαν μη παραμετρική προσέγγιση ,σε σχέση με τις παραδοσιακές μεθόδους, που είναι κατάλληλη για IoT επειδή δεν απαιτεί μεγάλο αποθηκευτικό χώρο για την αποθήκευση των εισερχόμενων δεδομένων. Επομένως αξιοποίησαν την εποπτευόμενη μάθηση βάσει αλληλουχίας με βάση το Influential Relative Grade (IRG) και το Relative Mass Function (RMF) που ανιχνεύει αποτελεσματικά τα ακραία σημεία και τα αποτελέσματα έδειξαν 99,65% και 98,53% ποσοστό ανίχνευσης σφαλμάτων σε διαφορετικά σύνολα δεδομένων. Οι Viegas et al. (2018) στόχευσαν στην ενεργειακά αποδοτική και φιλική προς το υλικό εφαρμογή των συστημάτων ανίχνευσης εισβολής στο IoT. Χρησιμοποιήθηκαν τρεις ταξινομητές, το Decision Tree (DT), το Naive Bayes (NB) και το Linear Discriminant Analysis (LDA) κατά τη διάρκεια του πειραματισμού τους για ανίχνευση εισβολής. Με αυτό τον τρόπο, οινανέλυσαν πρώτα την επίδραση του μοναδικού ταξινομητή μεταξύ των προαναφερθέντων ταξινομητών που έδειξε μεγάλη ακρίβεια πάνω από 99% και στη συνέχεια χρησιμοποίησαν τον συνδυασμό αυτών των ταξινομητών για να δουν την επίδραση στην ανίχνευση όπου τα αποτελέσματα ήταν απογοητευτικά καθώς το ποσοστό μειώθηκε κατά 30% σε περίπτωση νέων επιθέσεων. Ομοίως, την ιδιά ερεύνα διεξήγαγαν και οι Sedjelmaci et al. (2016) όπου επικεντρώθηκαν περισσότερο στη θεωρητική προσέγγιση παιχνιδιών για την ανίχνευση νέων τύπων εισβολής στα δίκτυα IoT και είχαν παρόμοια αποτελέσματα (Hussain et al. 2020).

Έπειτα, στη μετααναλυση των Benkhelifa et al. (2018) αναλυεται και για IDS που βασίζονται σε DL στο IoT όπου αναλύεται η έρευνα των Kim et al. (2016) που χρησιμοποιούν το Recurrent Neural Network (RNN) για να εκπαιδεύσει το μοντέλο IDS

που βασίζεται στην αρχιτεκτονική Long Short Term Memory (LSTM). Εντόπισαν σαν μέση ακρίβεια 96,93% με υπερ-παράμετρο για να βρουν τον βέλτιστο λανθασμένο συναγερμό και ρυθμό ανίχνευσης. Μια παρόμοια έρευνα των Saeed et al. (2016) όπου χρησιμοποίησαν Random Neural Networks (RaNN) για την ανίχνευση εισβολής που βασίζεται σε ανωμαλίες σε δίκτυα IoT χαμηλής ισχύος. Έγινε πρόταση για ένα μοντέλο δύο επιπέδων, στο πρώτο επίπεδο η φυσιολογική συμπεριφορά μαθαίνεται από το σύστημα και στο δεύτερο επίπεδο, εντοπίζονται διαφορετικά είδη σφαλμάτων παράνομης πρόσβασης μνήμης (IMA) και επιθέσεις ακεραιότητας δεδομένων στο δίκτυο. Τα πειραματικά αποτελέσματα δείχνουν ότι η ακρίβεια ανίχνευσης είναι κατά μέσο όρο 97,23% με 10,45% με τη μορφή κατανάλωσης ενέργειας. Ωστόσο, αυτά τα πειράματα δεν περιλαμβάνουν το πλήρες φάσμα επιθέσεων και τις επιθέσεις μηδενικών ημερών (Hussain et al. 2020).

5.3.5 Malware Analysis in IoT

Σε αυτό το υποκεφάλαιο θα γίνει μια εκτεταμένη αναφορά στα κακόβουλα λογισμικά που μπορούμε να συναντήσουμε στο IoT. Τι είναι όμως ένα κακόβουλο λογισμικό ; Πρόκειται ουσιαστικά για έναν από τους πιο διαβόητους τομείς επίθεσης και είναι η εισαγωγή κι η εκτέλεση κώδικα σε συσκευές IoT εκμεταλλεύοντας τις υπάρχουσας ευπάθειας που υπάρχουν στα devices. Οι συσκευές IoT επί της ουσίας χρησιμοποιούνται για να «φυτευτεί» ένα κακόβουλο λογισμικό. Οι ευπάθειες – αδυναμίες που έχουν τα IoT devices δίνουν την ευκαιρία να τις εκμεταλλευτεί ο επιτιθέμενος ώστε να έχει ο ίδιος κάποιο όφελος. Οι ευπάθειες αυτές συνηθώς σχετίζονται κυρίως με εφαρμογές, με τον έλεγχο ταυτότητας και με την εξουσιοδότηση. Μερικοί από τους πιο συνηθισμένους τύπους κακόβουλων λογισμικών είναι τα adware, τα Trojan, τα Spyware, τα Ransomware και τα virus. Όλα τα προαναφερθέντα περιέχουν κάποιο κώδικα στον πυρήνα τους που έχει ως σκοπό να βλάψει το σύστημα μας. Αν σε όλα αυτά συνυπολογίσουμε ότι υπάρχουν τεράστιες έξυπνες συσκευές που διασυνδέονται στο διαδίκτυο χωρίς να διαθέτουν την κατάλληλη προστασία ασφαλείας που όχι μόνο εκτίθενται εκείνες σε κίνδυνο σε ενδεχόμενο επιθέσεις αλλά μπορούν να παίξουν τον ρόλο του φιλοξενητή μια μαζική επίθεση κλίμακας τύπου DDoS είναι το λιγότερο εφικτό σενάριο. Κατά καιρούς κακόβουλα λογισμικά όπως το Red October, το Night Dragon, το Cryptlocker, το Stuxnet έχουν διαταράξει την κανονικότατα σε πολλά πληροφοριακά συστήματα αλλά πλέον και τον κόσμο του IoT. Μάλιστα, οι «δημιουργοί» τέτοιων λογισμικών προσπαθούν να βελτιώσουν την αποτελεσματικότητα τους κεντράροντας τον στόχο τους και επικεντρώνοντας πιο πολύ στον σκοπό τους ώστε να δημιουργήσουν βελτιστοποιημένες οικογένειες επιθέσεων κακόβουλού λογισμικού που στοχεύουν ιδιαίτερα τις συσκευές του IoT. Τέτοιες επιθέσεις προκαλούν τα κακόβουλα λογισμικά όπως το WanaCry, το Mirai, το Stuxnet και ούτω καθεξής. Δεν πρέπει να ξεχνάμε ότι οι απώλειες είναι πολύπλευρες και κυμαίνονται από χρηματικά πόσα έως και την δημόσια εικόνα της εκάστοτε εταιρείας που δημιουργείται στους καταναλωτές της (Hussain et al. 2020).

Η γενικευμένη προσέγγιση των εισβολών ώστε να ξεκινήσουν την επίθεση με πιθανό στόχο κάποιο δίκτυο αισθητήρων, κάποιο μέσω αναγνώρισης η άλλο device ξεκινά με την λεγόμενη παρακολούθηση. Υπάρχουν μέθοδοι και εργαλεία που μερικά απ' αυτά χρησιμοποιούνται ακόμα και για εκπαιδευτικούς σκοπούς που μπορούν να παρακολουθούν τις κινήσεις ενός δικτύου. Μερικά τέτοια εργαλεία είναι το Nmap, το Metasploit και το Wireshark. Ένα ακόμα μεγάλο εργαλείο που έγινε εκτεταμένη αναφορά

σε προηγούμενο κεφάλαιο και αποτελεί τον ακρογωνιαίο λίθο στο κομμάτι της παρακολούθησης είναι φυσικά το αποκαλούμενο social engineering. Αφού ληφθεί υπόψιν από το πρώτο βήμα η κίνηση οι επιτιθέμενοι έχουν ήδη αρχίσει να δημιουργούν βασικές ιδέες ως προς το είδος της ευπάθειας που υπάρχει και πρέπει να χρησιμοποιήσουν σε μια συγκεκριμένη κατηγορία συσκευών. Εσφαλμένες διαμορφώσεις ασφαλείας, σπασμένος έλεγχος ταυτότητας, τρύπες και κενά στα λειτουργικά ακόμα και στην βάση παραδείγματος χάρη όπως το SQL Injection λειτουργεί πάντα υπερ του επιτιθέμενου και όχι του αμυνόμενου. Μάλιστα, ανάλογα με τον τύπο της συσκευής οι εισβολείς μπορούν να στείλουν κάποιο υλικό στον στόχο μέσω πολλών τρόπων όπως το phishing ή ενημερώσεις Rookit ώστε να προχωρήσουν ακόμα ένα βήμα πιο μπροστά σε αυτό που ετοιμάζουν. Τα σημερινά έξυπνα κακόβουλα λογισμικά είναι επίσης ιδιαιτέρως προσαρμοστικά σύμφωνα με το περιβάλλον IoT που συναντάνε με το υποκείμενο φυσικά δίκτυο. Ορισμένα εξ αυτών είναι σε θέση με μεγάλη ευκολία να αποφύγουν τους μηχανισμούς ανίχνευσης και να παραμείνουν σε αδράνεια για κάποιο χρονικό διάστημα. Το να μην εκμεταλλεύονται αμέσως τον κακόβουλο κώδικα τους έως ότου νιώσουν την ασφάλεια που επιδιώκουν ίσως να είναι ακόμα πιο επικίνδυνο γιατί σίγουρα ισοδυναμεί με μια ισχυρότερη τελική επίθεση έχοντας τον χρόνο να προετοιμαστούν (Hussain et al. 2020).

Στον αντίποδα τώρα υπάρχουν ορισμένες προσπάθειες για να βρεθούν οι αρμόζουσες τεχνικές αντίμετρων για τα κακόβουλα λογισμικά. Η όλη σκέψη για το πως μπορούν να αντιμετωπιστεί ένα κακόβουλο λογισμικό ξεκινάει αν ληφθεί υπόψιν ότι το κακόβουλο λογισμικό είναι κρυπτογραφημένο και περιέχει και ένα αντίστοιχο μη κρυπτογραφημένο υλικό ώστε να γίνει η παράκαμψη των Antivirus. Όλο αυτό φυσικά γιατί βασίζεται στην ψηφιακή υπογραφή. Το αρνητικό για το λογισμικό σε αυτό το σημείο εντοπίζεται στο μη κρυπτογραφημένο μήνυμα καθώς επαναλαμβάνεται ολόιδιος για διαφορετικές εκδόσεις του ίδιου του κακόβολου λογισμικού. Αυτό καθ' αυτό και μόνο είναι αρκετό για ένα antivirus που είναι ενημερωμένο στο να καταλάβει ότι είναι πιθανό να υπάρχει πρόβλημα κατά το άνοιγμα του κρυπτογραφημένου μηνύματος. Γι' αυτό άλλωστε, οι προγραμματιστές των αντιικών προγραμμάτων τονίζουν εντόνως ότι τα antivirus πρέπει να είναι διαρκώς ενημερωμένα. Μπορεί να γίνει φυσικά αντικατάσταση ενός antivirus με κάποιον μηχανισμό ασφαλείας απλά λόγω της πιο απλής και εύκολης κατανόησης στην περίπτωση μας ταιριάζει απόλυτα (Hussain et al. 2020).

Συνεχίζοντας λοιπόν, τα κακόβουλα λογισμικά έχουν λάβει πλέον υπόψιν και αυτού του είδους την άμυνα οπότε και το αποκρυπτογραφημένο κομμάτι μπορεί να μεταλλαχθεί ώστε να μην γίνει ο εντοπισμός του. Ο τύπος αυτός λογισμικού καλείται ως ολιγομορφικό. Φυσικά υπάρχουν και λογισμικά πολυμορφικά που περιλαμβάνουν μια σειρά από κρυπτογραφημένα μηνύματα. Εκεί είναι εύκολα εννοούμενο ότι η ανίχνευση και η αντιμετώπιση σαφώς και δυσκολεύει. Υπάρχει άλλη μια κατηγορία κακόβουλου λογισμικού και ονομάζεται μεταμορφικό. Πρόκειται για ένα άκρως εξελιγμένο μεταξύ των ομάδων λογισμικό που είναι δύσκολα εντοπίσιμο αφού εκμεταλλεύεται τα θετικά και των δυο ως συνδυασμό (Hussain et al. 2020).

Λύσεις που δοθήκαν ώστε να αντιμετωπιστούν τα παραπάνω είναι η εισαγωγή νεκρού κώδικα , η εγγραφή υπορουτινών , η αντικατάσταση εντολών, η ανάθεση μητρώου

και η ενσωμάτωση κώδικα που εξαλειφτεί εντολές. Πιο συγκεκριμένα έγινε ιδιαίτερη μελέτη στον τρόπο που δρουν οι εισβολείς και προέκυψε το συμπέρασμα ότι τα κινητά τηλέφωνα παίζουν καθοριστικό ρόλο καθώς είναι οι βασικές πύλες εισόδων. Ακόμα και από μια σκωπτική πλευρά δεν γίνεται να αμφισβητηθεί το παραπάνω καθώς οι κινητές συσκευές χρησιμοποιούνται ως πύλη μεταξύ των διακομιστών back-end και αισθητήρων στο περιβάλλον του IoT. Επομένως, λόγω και των εγγενών χαρακτηριστικών που διαθέτουν όπως το λειτουργικό σύστημα είναι άκρως ευάλωτες. Για να αντιμετωπισθεί το πρόβλημα αυτό έγινε χρήση ενός αόρατου μηχανισμού Captcha παραλλήλως με έναν έξυπνο αισθητήρα σε κινητό τηλέφωνο. Ο αισθητήρας με την σειρά του καταγράφει τη συμπεριφορά του χρήστη στο τηλέφωνο και παρέχει πρόσβαση στις υπηρεσίες IoT με βάσει τη συμπεριφοράς του χρήστη του τηλεφώνου. Αρχικώς, φάνηκε να προκύπτει λύση μέσω του τρόπου που περιγράφηκε μόλις από πάνω όμως τα αποτελέσματα αποκάλυψαν άλλον έναν παράγοντα που παίζει δραστικό ρόλο. Οι εφαρμογές που χρησιμοποιούνται στο εν λόγω κινητό και είναι κατασκευασμένος κώδικας εταιρειών όπως η Google ή Apple μπορούν να τροποποιήσουν το αποτέλεσμα. Με δυο λόγια, όταν γίνεται χρήση μιας εφαρμογής (πχ Google Translate) που έχει στον κώδικα της τρωτά σημεία ακόμα και άριστη ως προς την ασφάλεια να είναι η χρήση που γίνεται από τον ιδιοκτήτη το αποτέλεσμα μπορεί να είναι τραγικό (Hussain et al. 2020).

Επομένως, προκύπτει το συμπέρασμα ότι οι παραδοσιακές τεχνικές ανίχνευσης κακόβουλου λογισμικού ενδέχεται να μην τόσο αποτελεσματικές ενάντια σε εξελιγμένα κακόβουλα λογισμικά. Σε αυτό το πλαίσιο λοιπόν αναπτυχθήκαν άλλες τεχνικές που βασίζονται σε ML και DL ώστε να δώσουν την λύση.

Η καλύτερη τεχνική ML που δύναται να χρησιμοποιηθεί είναι η χρήση PCA, SVM με βάση n-gram. Μέσω ημί-εποπτευόμενων προσεγγίσεων οι ταξινομητές επιτυγχάνουν υψηλότερο ποσοστό ανίχνευσης και ακρίβειας. Μάλιστα έχει γίνει και πειραματική δοκιμή με χρήση του Miai αλλά και διαφορετικές παραλλαγές του. Τα αποτελέσματα ήταν άκρως ενθαρρυντικά καθώς έδειξαν ποσοστό ανίχνευσης 100% με χρήση PCA όπως αυτό αναλύθηκε προηγουμένως και μάλιστα χωρίς ψευδή μηνύματα (Hussain et al. 2020).

Επειδή όμως βρισκόμαστε σε ένα κόσμο που κινείται με φρενήρεις ρυθμούς και υπήρχε η ανάγκη υπερκαλύψεις του θέματος για νέα κακόβολου λογισμικά έγινε δοκιμή άλλη μιας τεχνικής όπου το SVM παίζει τον ρόλο του «μοχλού» όπου τα δεδομένα με ετικέτα χρησιμοποιούνται για εποπτευόμενη μάθηση του SVM. Επιπλέον εξίσου δοκιμή έγινε κατά την χρήση μη επιτηρούμενης μάθησης. Αυτές οι τεχνικές ML ως ολοκληρωτικό συμπέρασμα έδειξαν ότι η μηχανική μάθηση είναι σε θέση να αντιμετωπίσει τους επιτιθέμενους. Σε μεγάλες εταιρείες όπου «δουλειά» τους είναι η διασφάλιση συσκευών και πληροφοριακών συστημάτων χρησιμοποιείται κατά κόρον η μηχανική μάθηση ως εργαλείο (Hussain et al. 2020).

Ομοίως το Deep Learning βασίστηκε σε προσεγγίσεις βασισμένες σε RNN ως τεχνική ανάλυση κακόβουλών λογισμικών στο IoT. Εξετάστηκαν εφαρμογές που βασίζονται σε ARM. Αρχικώς γινόταν εκπαίδευση στα μοντέλα με διαφορετικά σύνολα

δεδομένων κακόβολου λογισμικού και στη συνέχεια δοκιμαζόταν το πλαίσιο τους με νέο επιβλαβές λογισμικό. Υπήρξε ακρίβεια λοιπόν της τάξεως του 98% στον εντοπισμό αυτών των νέων λογισμικών (Hussain et al. 2020). Ακολούθως μια άλλη τεχνική DL ονόματι IoBT χρησιμοποιήθηκε για να ανάλυση την ακολουθία λειτουργικών κωδικών (OpCode) των συσκευών. Στην συγκεκριμένη περίπτωση έγινε αξιοποίηση τεχνικής του DL για να γίνει η ταξινόμηση των εφαρμογών που είναι συμβατές με ARM. Άρα, ουσιαστικά το IoBT ήρθε να υποστήριξη το ήδη υπάρχουν εγχείρημα. Στην ανάλυση χρησιμοποιήθηκαν τεχνικές Class-Wise Information Gain για την επιλογή των χαρακτηριστικών όπου έγινε η επιλογή σε δείγματα τόσο καλοπροαίρετου όσο και κακοπροαίρετου κώδικα. Μετά, αυτός ο κώδικας ταξινομήθηκε πάλι βάσει OpCode. Τα αποτελέσματα στον εντοπισμό αγγίζουν το 98,59% ενώ για ανάκληση έχουμε 98,37% (Hussain et al. 2020).

Όπως έχει γίνει ήδη αντιληπτό σε όλα τα υποκεφάλαια έχει αναπτυχθεί και παρουσιαστεί πάνω από ένας τρόπος αντιμετώπισης των «προβλημάτων». Αυτό γίνεται καθώς αλλιώς οφείλεται να αντιμετωπιστεί μια επίθεση DDoS και αλλιώς μια επίθεση με κάποιο ransomware. Έτσι με όπως επεξηγήθηκε ήδη με το όρο κακόβουλο λογισμικό αναφέρουμε πάνω από μια επίθεση που είναι πιθανή. Ακολούθως παρουσιάζονται αλλά δυο μοντέλα τελευταία αντιμετωπίσεις επιθέσεων (Hussain et al. 2020).

Για την ανίχνευση επιθέσεων Botnet στο IoT χρησιμοποιούνται βαθιές αυτόματες κωδικοποιήσεις ώστε να εξάγουμε την συμπεριφορά του δικτύου και στην συνέχεια να απομονωθούν οι ανωμαλίες συμπεριφορές. Η χρήση βαθιών αυτόματων κωδικοποιητών επιλύει το ζήτημα.

Απ’ την άλλη χρησιμοποιήθηκαν δίκτυα Deep Q με συνδυασμό της τεχνικής εκμάθησης για την αντιμετώπιση προβλημάτων σε εφαρμογές υγειονομικής περίθαλψης δικτυών IoT. Η τεχνική Q-Learning και η αξιοποίηση της αναλύει τα δεδομένα ασθενών μέσω πολυεπίπεδων δικτυών. Μάλιστα τα συγκεκριμένα δίκτυα καταναλώνουν και ελάχιστη ενέργεια οπότε και τα καθιστά ιδανικά (Hussain et al. 2020).

ΚΕΦΑΛΑΙΟ 6 – Συνοπτικοί Πίνακες & Ιδιαιτερότητες

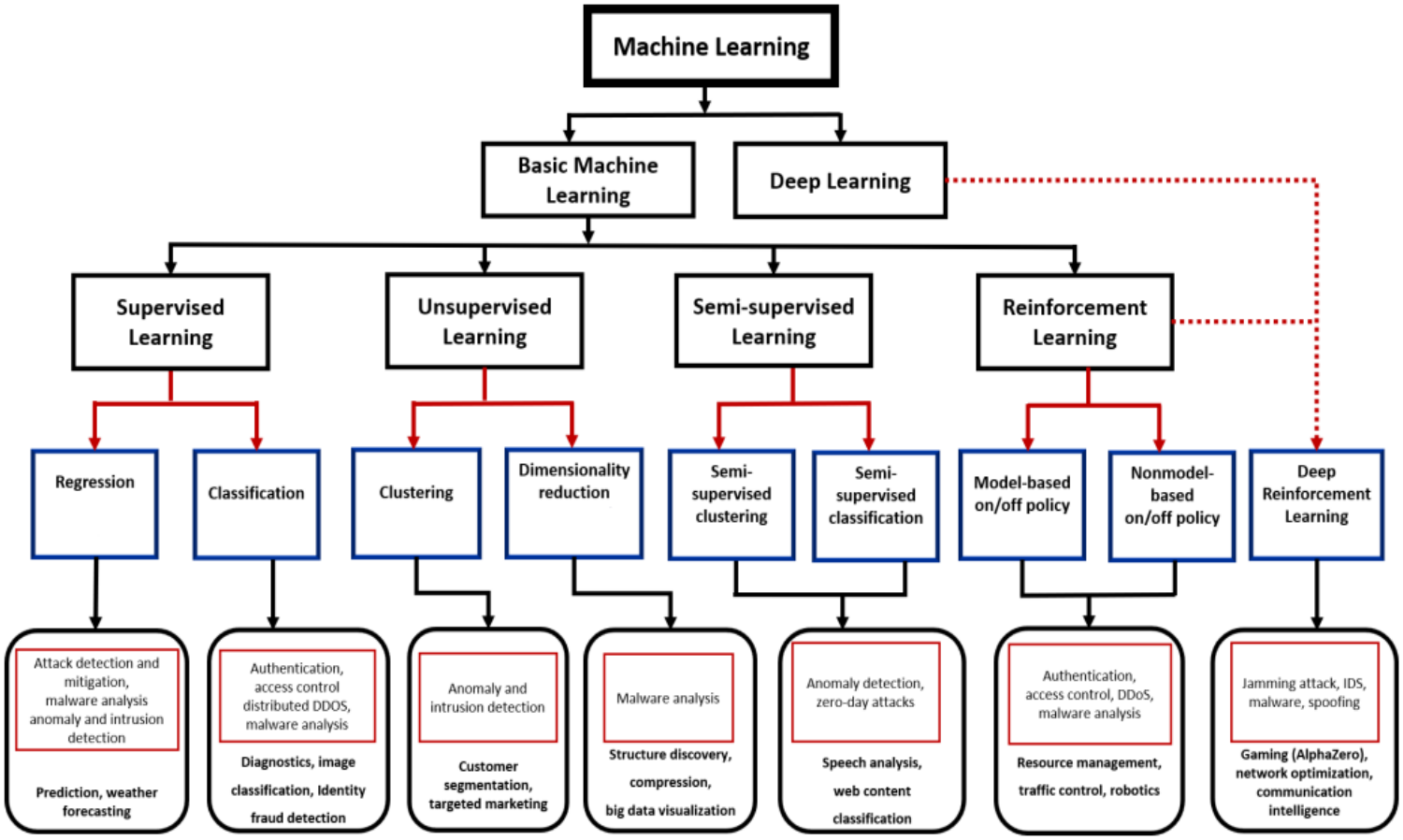
6.1 Συνοπτικοί Πίνακες

Ερευνητικό Θέμα - Επίθεση	Τεχνική Ασφαλείας ML	Συγκριση
Authentication & Access Control	• Deep Learning & LSTM • Artificial Neural Network (ANNs) • Recurrent Neural Networks (RNNs) • Deep Neural Network (DNN)	Το RNN υπερτερεί των άλλων αλγορίθμων ML / DL στην απόδοση, στην ακρίβεια και την πολυπλοκότητα. Αγγίζει ακρίβεια 90%. Το SVM αποδίδει ικανοποιητικά το LSTM όμως ξεπερνά το SVM. Το πρόβλημα που αντιμετωπίζουν οι τεχνικές ML εντοπίζεται στον μικρό αριθμό διαθέσιμων δεδομένων.
Attack Detection & Mitigation	• SVM • Unsupervised Learning • ESFCM • K Nearest Neighbours KNN and SVM	Η ESFCM ασχολείται με τα δεδομένα ως ετικέτα οπότε όλο αυτό έχει ως αποτέλεσμα να αυξάνει το ποσοστό ανίχνευσης κατανεμημένων επιθέσεων. Το K-NN αποδίδει καλυτέρα σε μικρά δίκτυα ενώ το SVM αποδίδει καλυτέρα σε μεγάλα δίκτυα όσον αφορά την ακρίβεια.
DOS Attacks	• K-Nearest Neighbours KNN • Random Forest • SVM • MCA • Q Learning	Το RF έχει χαμηλό αριθμό ελέγχου αλλά και παραμέτρους του μοντέλου. Είναι πειστικά ανθεκτικό στην παρατεταμένη χρήση. Η τεχνική δεν απαιτεί επιλογή χαρακτηριστικών αλλά η διακύμανση του μοντέλου μειώνεται καθώς αυξάνονται οι αριθμοί. Το SVM είναι κατάλληλο υπό την προϋπόθεση ύπαρξης μεγάλου αριθμού από στοιχεία. Το MCA βασίζεται σε ανάλυση συμπεριφοράς της κυκλοφορίας και ανίχνευση έως 99%.
Anomaly/Intrusion Detection	• Naïve Bayes • Decisioon Tree • ANN • K means Clustering	Η ομαδοποίηση K-Means χρησιμοποιεί τα δεδομένα με ετικέτα επομένως το πλεονεκτήματα του είναι ότι μπορεί να μάθει από τον έλεγχο χωρίς να απαιτεί σαφείς περίγραφες επιθέσεων. Το DT είναι εύχρηστο, εφαρμόζεται αμέσως και έχει υψηλή ακρίβεια. Το Naive Bayes έχει χαμηλή απαιτήσει δείγματος εκπαίδευσης. Έχει την ικανότητα να πραγματοποιήσει διαχείριση ανεξάρτητων χαρακτηριστικών οπότε σε τέτοια περίπτωση είναι ο βέλτιστος ταξινομητής ιδιαιτέρως εάν το training phase μπορεί να ολοκληρωθεί σε γραμμικό χρόνο.

Malware Analysis	• Random Forest • SVM • PCA & SVM • Linear SVM • Deep Q Networks	Το PCA επιτυγχάνει μείωση διαστάσεων και γενικότερα μειώνει την πολυπλοκότητα των μοντέλων Το πρόβλημα των ML τεχνικών όπως τα Bayesian Networks , το SVM κλπ είναι στο ότι υποφέρουν όταν δεν υπάρχει μεγάλη βάση δεδομένων χωρίς να σημαίνει αυτό ότι δεν είναι αποτελεσματικά.

Table 1 - Σύγκριση τεχνικών ασφαλείας ML σε επιθέσεις

Ο παραπάνω πίνακας βασίζεται στο άρθρο (Hussain et al. 2020).



Εικόνα 23 - ML & Αντιμετώπιση απειλών (Hussain et al. 2020)

Ακολουθεί πίνακας με τις τεχνικές που έχουν όλα τα είδη της μηχανικής μάθησης.

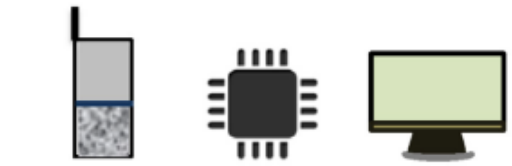
Machine Learning Algorithm	Description	Application
Supervised Learning		
Naïve Bayes	Ο Naive Bayes είναι αλγόριθμος ταξινόμησης. Πραγματοποιεί προβλέψεις για τον υπολογισμό πιθανοτήτων σε μια συγκεκριμένη υπόθεση. Μπορεί τα χαρακτηριστικά να είναι ανεξάρτητα μεταξύ τους.	Χρησιμοποιείται σε περιβάλλον πολλαπλών τάξεων και διαφοροποιήσεων. Αποτελεσματικό στην ανίχνευση ανωμαλιών & εισβολής. Λειτουργεί καλυτέρα με διακριτά δεδομένα και μπορεί να κάνει λάθος εάν χρησιμοποιούνται συνεχόμενα δεδομένα.
K – Nearest Neighbors	Είναι αλγόριθμος εποπτευομένης μάθησης και χρησιμοποιείται για συσχέτιση νέων δεδομένων με τα υπάρχοντα. Το μοντέλο εκπαιδεύεται και ομαδοποιείται ανάλογα καθορισμένα κριτήρια. Από τα δεδομένα μετά ελέγχονται ομοιότητες εντός των γειτόνων.	Πολύ απλός στην εφαρμογή όπως επίσης μπορεί να χρησιμοποιηθεί και ως αρχική αξιολόγηση της απλής ταξινόμησης σε μικρά δίκτυα. Η απόδοση του υποβαθμίζεται σε μεγάλα σύνολα δεδομένων αλλά και σε μεγάλα δίκτυα. Αυτό οφείλεται στο γεγονός ότι το κόστος του υπολογισμού της απόστασης μεταξύ των σημείων είναι μεγάλο. Είναι ευαίσθητος αλγόριθμος σε θορυβώδη δεδομένα. Το KNN είναι πολύ γρήγορος αλγόριθμος και δεν απαιτεί περίοδο training. Μαθαίνει μόνο από την δεδομένη στιγμή.
Random Forest & Decision Tree (DT)	Πρόκειται για εποπτευομένη μάθηση όπου ορίζει ένα μοντέλο με την εφαρμογή ορισμένων κανόνων που συνάγονται από τα χαρακτηριστικά των δεδομένων. Έπειτα αυτό το μοντέλο χρησιμοποιείται για την πρόβλεψη των στοχευόντων μεταβλητών. Επίσης, χρησιμοποιείται σε ταξινόμηση και σε παλινδρόμησή. Επί της ουσίας χωρίζει το σύνολο των δεδομένων σε πολλά υποσύνολα βάσει κανόνων.	Τα τυχαία δάση λαμβάνοντας υπόψιν ότι μπορούν να λειτουργήσουν σε υποσύνολα μπορούν να διαχειριστούν υψηλή διάσταση δεδομένων. Ωστόσο ενδέχεται να επιβαρύνονται με κόστος αποθήκευσης. Εμπεριέχονται σε αυτόν μέθοδοι εξισορρόπησης σφάλματος καθώς επίσης χειρίζεται και μη ισορροπημένα δεδομένα.
Support Vector Machines (SVM)	Το SVM είναι μια εποπτευομένη τεχνική ML με χαμηλή πολυπλοκότητα.	Λειτουργεί καλά με μη δομημένα ή με ημιδομημενα δεδομένα. Ο αλγόριθμος δεν είναι κατάλληλος

	Χρησιμοποίει ταξινόμηση και παλινδρόμηση. Κατατάσσει δεδομένα σε ν διαστατικό χρόνο και σχεδιάζει ένα χώρο για να διαίρεση τα δεδομένα σε ομάδες.	όμως να επεξεργάζεται μεγάλα σετ δεδομένων. Πάρα ταύτα μπορεί και λειτουργεί με κείμενα και εικόνες.
Neural Network (NN)	Πρόκειται για μια εποπτευομένη μάθηση που χρησιμοποιεί για την ανάπτυξη μια αλυσιδωτή αλυσίδα αποφάσεων. Κατασκευάζει δίκτυο με συγκεκριμένες εισόδους και εξόδους. Διαφορά νευρωνικά δίκτυά είναι το MLP, το CNN, το RNNs.	Εκτέλεση μη γραμμικής στατικής μοντελοποίησης. Μικρή εκπαίδευση. Δυνατότητα έμμεσης ανίχνευσης μη γραμμικών σχέσεων με εξαρτημένες μεταβλητές. Επομένως είναι εύκολος ο εντοπισμός των αλληλεπιδράσεων μεταξύ μεταβλητών.
Deep Learning	Πρόκειται ουσιαστικά για ένα νευρωνικό σύστημα το ο οποίο ο κάθε νευρώνας συνδέεται με άλλο στρώμα. Ο όρος βαθιά μάθηση αναφέρεται σε πολλαπλάσια κρυμμένα στρώματα μεταξύ επιπέδων εισόδων και εξόδων ώστε κάθε επίπεδο να λαμβάνει είσοδο το προηγούμενο και να τροφοδοτεί το επόμενο.	Έχει την ικανότητα να συνεργάζεται με μη δομημένα δεδομένα σε όλα τα προβλήματα. Επεξεργάζεται ουσιαστικά διαφορετικές μορφές δεδομένων καθώς μπορεί να τα χρησιμοποιήσει και για εκπαίδευση. Ο αλγόριθμος σαρώνει τα δεδομένα για να προσδιορίσει χαρακτηριστικά που σχετίζονται μεταξύ τους και μετά προωθούνται. Μπορεί να χειριστεί μεγάλο όγκο δεδομένων και να εκτελέσει παράλληλους υπολογισμούς. Τέλος η απόδοση βελτιώνεται εάν λάβει μεγάλη ποσότητα δεδομένων. Αντιμετωπίζει πρόβλημα με τα ελάχιστα δεδομένα ως είσοδο.
Unsupervised Learning		
K – Means Algorithm	Η πιο διαδεδομένη τεχνική στην μη εποπτευομένη μάθηση στην οικογένεια της μηχανικής. Χρησιμοποιεί συστοιχίες ή ομάδες βασιζομένη στα χαρακτηρίστηκα. Δημιουργεί K αριθμό ομάδων όπου K θετικός ακέραιος αριθμός που έχει την σημαντικότερη αξία.	Κατάλληλο σε ταξινόμηση δεδομένων χωρίς γνώση της συσχέτισης. Αναλαμβάνει σφαιρικά σχήματα clusters και δεν λειτουργεί καλά όταν το σύνολο – σμήνος είναι σε διαφορετικά σχήματα. Επίσης δεν λειτουργεί καλά όταν δυο cluster αλληλεπικαλύπτονται, επειδή δεν έχει το εγγενές μετρό να ξεχωρίσει το σύμπλεγμα.

Principal Component Analysis (PCA)	Είναι μια μη εποπτευομένη τεχνική ML που πραγματοποιεί συμπίεση δεδομένων. Εκτελεί μείωση διαστάσεων σε μεγάλο βαθμό ώστε να εξάγει ένα απόσπασμα πληροφορίας σαν βασικό συστατικό. Υστέρα ταξινομεί με αυξανομένη σειρά τα συστατικά αυτά όπου στην κορυφή μπαίνει εκείνο με την υψηλότερη διακύμανση δεδομένων και συνεχίζει μέχρι το τελευταίο. Εκείνα με την λιγότερη διακύμανση μπορούν να απορριφθούν.	Εξαιρετικό εργαλείο σε πραγματικό χρόνο και σε κατάσταση με πολλά χαρακτηριστικά χωρίς κάποια συσχέτιση. Ελάχιστος χρόνος προπόνησης, ειδικότερα εξαλείφοντας εκείνα τα στοιχεία που δεν συμβάλουν στην λήψη αποφάσεων. Το PCA μετατρέπει δεδομένα υψηλής διάστασης σε χαμηλή (2 διαστάσεις) και βοηθά έτσι την επίλυση του προβλήματος.
Reinforcement Learning		
Q-Learning	Ανήκει στην ενισχυμένη μάθηση της μηχανικής. Μαθαίνει από την δοκιμή και το σφάλμα ως προς τον τρόπο που οι δράσεις επηρεάζουν το περιβάλλον της εργασίας. Προβαίνει σε εκτίμηση μετά από κάθε δράση και μεταβαίνει σε νέα κατάσταση ανάλογα την εκτίμηση αυτή.	Προτιμά να επιτύχει μακροπρόθεσμα αποτελέσματα και μπορεί να χρησιμοποιηθεί για την επίλυση πολύπλοκων προβλημάτων όπου δεν μπορούν να λυθούν με συμβατικό τρόπο. Είναι η πιο κατάλληλη επιλογή όταν δεν υπάρχει διαθέσιμο σύνολο δεδομένων για εκπαίδευση. Αναλαμβάνει προβλήματα πραγματικού χρόνου. Για να αντιμετωπίσει περιορισμούς χρησιμοποιείται συνδυαστικά με άλλες τεχνικές.

Table 2 - Ανάλυση ειδών & τεχνικών της ML

Ο παραπάνω πίνακας βασίζεται στο άρθρο (Hussain et al. 2020).

Attack Surface		Attack Name
Physical Device/Perception Surface	 Phone Sensors PCs Any physical devices	DoS Eavesdropping Counterfeiting Radio interference Jamming Physical Attacks Node Capture Attacks User Tracking

Εικόνα 24 - Επιθέσεις Φυσικού Επιπέδου

Attacks	Security techniques	Machine Learning Techniques	Performance
DoS	Access Control	Q-Learning Neural Network	Ακρίβεια Ανίχνευσης Μέσο Σφάλμα
Jamming	Secure IoT offloading	Q-Learning	Καταναλ. Ενέργειας SINR
Spoofing	Authentication	Q-learning SVM DNN	Μέσο ποσοστιαίο σφάλμα Ακρίβεια ανίχνευσης Λανθασμένη ειδοποίηση Απώλεια εντοπισμού
Instrusion	Access Control	SVM Naïve Bayes K-NN Neural Networks	Ακρίβεια ταξινόμησης Λανθασμένο θετικό δείγμα Ακρίβεια Ανίχνευσης
Malware	Malware Detection Access Control	Random Forest K-nearest neigh	Ακρίβεια ταξινόμησης Ακρίβεια Ανίχνευσης Ακρίβεια απώλειας Λανθασμένο θετικό δείγμα
Eavesdropping	Authentication	Q - Learning	Ποσοστό εγγύτητας Όγκος δεδομένων απορρήτου

Table 3 - Επίθεση & Προτεινόμενος τρόπος άμυνας

Ο παραπάνω πίνακας βασίζεται στο άρθρο (Xiao et al. 2018).

6.2 Περιορισμοί της εφαρμογής της μηχανικής μάθησης

Μπορεί η μηχανική μάθηση να μας έδωσε κάποιες λύσεις στο κομμάτι της ασφάλειας του IoT αλλά δυστυχώς λόγω ότι δεν είναι εγγενώς αποτελεσματικές να διαχειρίζονται τα δεδομένα Internet of Things χρειάζονται κάποιες τροποποιήσεις για να είναι λειτουργικές. Ακολουθούν μερικοί από τους κοινούς περιορισμούς των τεχνικών του ML στο IoT.

Λαμβάνοντας λοιπόν στα υπόψιν ότι μια εκ των ιδιαιτεροτήτων των συσκευών IoT αλλά και WSNs είναι η ελαχιστοποίηση της καταναλισκομένης ενέργειας όπως επίσης και η μικρή επεξεργαστική ισχύ (MCU) διαπιστώνουμε ότι άμεση εφαρμογή των τεχνικών του ML δεν είναι κατάλληλες σε τέτοιου είδους πόρους. Τα περιβάλλοντα είναι περιορισμένα οπότε δεν είναι και το ιδανικότερο σενάριο η εφαρμογή τεχνικής ML ως αυτούσια. Μην ξεχνάμε ότι οι κομβόι συνήθως τροφοδοτούνται από μπαταρίες και μάλιστα λειτουργούν για μεγάλα χρονικά διαστήματα χωρίς επίβλεψη.

Ο δεύτερος μεγάλος περιορισμός στην εφαρμογή της μηχανικής μάθησης εντοπίζεται στην ανάλυση ετερογενών δεδομένων. Όπως ήδη έχει αναφερθεί και γνωρίζουμε τα δεδομένα παράγονται από διαφορετικές πηγές συμπεριλαμβανομένων και τα δίκτυα πληροφοριακών συστημάτων. Είναι φυσικό επόμενο δηλαδή να έχουν διαφορετικούς τύπους, διαφορετική μορφή και διαφορετικό χαρακτήρα παρουσιάζοντας έτσι συντακτική και σημασιολογική ετερογένεια. Με τον όρο συντακτική εννοείται η ποικιλομορφία των τύπων δεδομένων των μορφών αρχείων, των μοντέλων κωδικοποίησης αλλά και των μοντέλων δεδομένων. Από την άλλη πλευρά τώρα με την έννοια σημασιολογική ετερογένεια αναφέρεται ως η διαφορά που προκύπτει ανάμεσα σε ερμηνείες των δεδομένων. Μπορεί μια ερμηνεία για ένα πληροφοριακό σύστημα να σημαίνει αυτόματο συναγερμό και για μια συσκευή IoT να μην σημαίνει κάτι ή και το αντίθετο.

Οι περισσότερες τεχνικές ML χειρίζονται τα δεδομένα και τα παίρνανε μέσω ενός είδους training phase δηλαδή μιας εκπαιδευτικής διαδικασίας ώστε να μάθουν από αυτή και να εντοπίσουν διάφορες ώστε να καταλήξουν στο πλησιέστερο ζητούμενο αποτέλεσμα. Άλλο ένα επιπλέον πρόβλημα λοιπόν δημιουργείται επειδή ενίοτε τα δεδομένα από συσκευή IoT δεν είναι όλα σε αναμονή και προς διάθεση με αποτέλεσμα η ικανότητα της πρόβλεψής ενός αλγορίθμου να μειώνεται καθώς η διάσταση μεταξύ των δεδομένων αυξάνεται. Με λίγα λόγια, επεξεργάζονται λιγότερα δεδομένα λόγω της φύσης των devices τα αποτελέσματα δεν είναι τόσο βέβαια.

Επιπροσθέτως η επιλογή ενός κατάλληλου αλγορίθμου ML για ένα συγκεκριμένο σενάριο είναι ζωτικής σημασίας για το αποτέλεσμα που θα εξάγουμε. Για παράδειγμα, όπως έχει γίνει ήδη γνωστό εάν έχουμε δεδομένα με ετικέτες χρησιμοποιούνται αλγόριθμοι ταξινόμησης (Supervised), εάν από την άλλη δεν υπάρχει ετικέτα ο αλγόριθμος που χρησιμοποιείται έχει να κάνει με ομαδοποίηση δηλαδή κάποιος αλγόριθμος στην χωροταξία του Unsupervised.

Σε περίπτωση όμως που έχουμε υβριδικά δεδομένα, πρέπει να χρησιμοποιηθεί συνδυασμός δυο αλγορίθμων ή και περισσοτέρων.

Μην ξεχνάμε λοιπόν, ότι συνήθως στο IoT τα δεδομένα είναι πραγματικού χρόνου άρα είναι εύκολα κατανοητό ότι ο συνδυασμός δυο αλγορίθμων μας το καθιστά ακόμα πιο περίπλοκο.

Κάνοντας μια ανασκόπηση στους περιορισμούς και αφού λάβουμε υπόψιν ότι οι εφαρμογές IoT περιλαμβάνουν έναν συνδυασμό ευπροσάρμοστων συσκευών και μονάδων επεξεργασίας που κυμαίνονται από cloud διακομιστές έως και συσκευές με εξαιρετικά μικρή χαμηλώσει ισχύ καταγράφεται ένα ακόμα πρόβλημα. Απαιτείται ο επανασχεδιασμός και η εκ νέου ανάπτυξη κυκλωμάτων μνήμων με εξαιρετικά χαμηλή τάση που πρέπει να περιλαμβάνεται σε αυτές ένα πολύ ελαφρύς τρόπο κρυπτογράφησης για προστασία των συσκευών.

Συνοπτικά, ακόμα και ο τομέας της κρυπτογραφίας πρέπει να τροποποιήσει τα χαρακτηριστικά του ώστε να μπορέσουν αυτοί οι κλάδοι να συνεργαστούν όλοι μαζί αρμονικά. Ο σχεδιασμός ειδικών κυκλωμάτων και chip για νευρωνικά ML και DL ώστε να έχουμε δυναμικότητα στην ασφάλεια θεωρείται δεδομένος.

6.3 Μελλοντικές Λύσεις - Προκλήσεις

Οι τεχνικές που χρησιμοποιούνται από την μηχανική μάθηση έχουν να διανύσουν μεγάλη πορεία ακόμα ώστε να αναφερθεί ότι είναι απολύτως αποτελεσματικές. Δεν πρέπει να λησμονούμε ότι επί της ουσίας όλες οι τεχνικές που εξετάστηκαν παραπάνω λειτουργούν υπό συνθήκες η κάθε μια. Υπενθυμίζεται ότι εκεί που σε μια περίπτωση η τεχνική SVM μπορεί να μοιάζει ιδεατή σε μια άλλη περίπτωση ίσως να είναι τελείως αναποτελεσματική.

Η μηχανική μάθηση αντιμετωπίζει προκλήσεις που οφείλει να βρει λύση όπως οι περιπτώσεις μη διαθεσιμότητας και η μη παροχή συνολικών δεδομένων ώστε να επεξεργαστούν και να προχωρήσει η όλη διαδικασία. Το βασικό ελάττωμα της μάθησης αυτής εντοπίζεται στο ότι σε όλες σχεδόν οι τεχνικές πραγματοποιούν εξομοιώσεις.

Εξίσου πρόβλημα αποτελεί και η ανισορροπία δεδομένων όπως αναφέρεται σε αγγλικούς ορούς το «Data Imbalance». Η ανισορροπία που προκύπτει αυτή στο IoT επηρεάζουν σημαντικά την απόδοση των τεχνικών.

Επίσης, η μίξη των δεδομένων από διάφορες πηγές μπορεί από την μια να είναι θετικό αλλά μην ξεχνάμε ότι πρέπει να γίνει και ο διαχωρισμός των «κάλων & χρήσιμων» από τα «άχρηστα & βλαβερά» στοιχεία. Αυτή η εργασία φυσικά και δυσκολεύει το εγχείρημα.

Τέλος, τα τελευταία χρόνια έχει γίνει μεγάλη συζήτηση για το αποκαλούμε GDPR δηλαδή τα προσωπικά μας δεδομένα. Η πιο δύσκολη και ίσως η πιο σημαντική πρόκληση της μηχανικής μάθησης είναι ότι πρέπει να ανακαλύψει το πως θα είναι εφικτό να διασφαλιστούν αυτά τα δεδομένα τόσο κατά την χρήση των ειδών του ML όσο και κατά την διάρκεια των επιθέσεων.

Εικόνα 25 - Το GDPR στην Μηχανική Μάθηση

ΚΕΦΑΛΑΙΟ 7 – Συζήτηση

Στη συγκεκριμένη εργασία αναφερθήκαμε στην τεχνολογία IoT αλλά και στα δίκτυα 5G ενώ εστιάσαμε στην ασφάλειά τους. Επίσης, μελετήσαμε τη μηχανική μάθηση και πως αυτή συμβάλλει με διάφορες τεχνικές στην αντιμετώπιση των προβλημάτων ασφάλειας αυτών των δικτύων. Μελετήσαμε, επίσης, διάφορες τεχνικές ασφαλείας IoT που βασίζονται στην εν λόγω μάθηση, συμπεριλαμβανομένου του ελέγχου ταυτότητας IoT, του ελέγχου πρόσβασης, της ανίχνευσης κακόβουλου λογισμικού κλπ, οι οποίες φαίνεται να αποτελούν εξαιρετικά υποσχόμενες τακτικές προστασίας για το IoT (Hussain et al. 2020).

Γενικότερα, όπως είδαμε στη συγκεκριμένη εργασία η ασφάλεια του IoT αλλά και του δικτύου 5G αποτελεί ένα ζήτημα ζωτικής σημασίας που παίζει καθοριστικό ρόλο στην εμπορευματοποίηση και στην ανάπτυξη των συγκεκριμένων τεχνολογιών. Οι παραδοσιακές λύσεις ασφάλειας και απορρήτου υποφέρουν από διάφορα ζητήματα που σχετίζονται με τη δυναμική φύση των δικτύων αυτής της μορφής.

Όπως είδαμε στη συγκεκριμένη εργασία, οι τεχνικές μηχανικής μάθησης μπορούν να χρησιμοποιηθούν για να επιτρέψουν στις συσκευές IoT και στο δίκτυο 5G να προσαρμοστούν στο δυναμικό τους περιβάλλον. Αυτές οι τεχνικές μάθησης μπορούν να υποστηρίξουν τη λειτουργία αυτό-οργάνωσης και επίσης να βελτιστοποιήσουν τη συνολική απόδοση του συστήματος με την εκμάθηση και την επεξεργασία στατιστικών πληροφορίες από το περιβάλλον (π.χ. ανθρώπινοι χρήστες και συσκευές IoT κλπ) (Hussain et al. 2020).

Ένα από τα βασικότερα πλεονεκτήματα των τεχνικών αυτής της μορφής είναι πως δεν απαιτούν κεντρική επικοινωνία μεταξύ συσκευής και ελεγκτή. Ωστόσο, τα απαιτούμενα σύνολα δεδομένων για αλγόριθμους εξακολουθούν να είναι λιγοστά, γεγονός που καθιστά δύσκολη τη συγκριτική αξιολόγηση της αποτελεσματικότητας των λύσεων ασφαλείας που βασίζονται σε μηχανική μάθηση.

Εικόνα 26 - Συζήτηση ML

ΚΕΦΑΛΑΙΟ 8 – Βιβλιογραφία

1. AHMAD, I., SHAHABUDDIN, S., KUMAR, T., OKWUIBE, J., GURTOV, A., YLIANTILA, M., 2019. *Security for 5G and Beyond, Department of Computer and Information Science,* Link¨oping University, Sweden.

2. AL-SARAWI, S., ANBAR, M., ALIEYAN, K., and ALZUBAIDI, M., 2017. *Internet of things (iot) communication protocols: Review. 8th International Conference on Information Technology (ICIT).* [Online] May 2017, pp. 685–690. [ημερομηνία πρόσβασης 25 Οκτωβρίου]. Διαθέσιμο στο: https://ieeexplore.ieee.org/abstract/document/8079928

3. BENKHELIFA, E., WELSH, T., and HAMOUDA, W., 2018. *A critical review of practices and challenges in intrusion detection systems for iot: Towards universal and resilient systems*, IEEE Communications Surveys Tutorials, pp. 1–1.

4. BONACCORSO, G., 2017. *Machine Learning Algorithms: A reference guide to popular algorithms for data science and machine learning*, Packt Publishing.

5. BRAIN BRIDGE., 2020. *FROM 1G TO 5G: A BRIEF HISTORY OF THE EVOLUTION OF MOBILE STANDARDS.* [Online]. [ημερομηνία πρόσβασης 25 Οκτωβρίου]. Διαθέσιμο στο: https://www.brainbridge.be/news/from-1g-to-5g-a-brief-history-of-the-evolution-of-mobile-standards

6. CANEDO, J. and SKJELLUM, A., 2016. *Using machine learning to secure iot ˜ systems, in 2016 14th Annual Conference on Privacy*, Security and Trust (PST), pp. 219–222, Dec 2016.

7. CHEN, J., LI, S., YU, H., ZHANG, Y., RAYCHAUDHURI, D., RAVINDRAN, R., GAO, H., DONG, L., WANG, G., and LIU, H., 2016. *Exploiting icn for real-izing service oriented communication in iot. IEEE Communications Magazine.* [Online] December 2016, Vol. 54, Issue 12, pp. 24–30 [ημερομηνία πρόσβασης 25 Οκτωβρίου]. Διαθέσιμο στο: https://ieeexplore.ieee.org/document/7785885

8. CHUMACHENKO, K., 2017. *Machine learning methods for malware detection and classification,* Bachelor's Thesis Information Technology, University of Applied Sciences.

9. EL MOUAATAMID, O., LAHMER, M., BELKASMI, M., 2016. *Internet of Things Security: Layered classification of attacks and possible Countermeasures*, SIME Lab, 9(1), pp. 24-37.

10. FREMANTLE, P., 2015. *A REFERENCE ARCHITECTURE FOR THE INTERNET OF THINGS.* [Online] [ημερομηνία πρόσβασης 3 Νοεμβρίου]. Διαθέσιμο στο: https://docs.huihoo.com/wso2/wso2-whitepaper-a-reference-architecture-for-the-internet-of-things.pdf

11. GALLARDO, L., 2019. *5G Networking: Learning 5G Technology Explained For Dummies*, Kindle Edition.

12. GREENGARD, S., 2015. *The Internet of Things*, MIT Press Essential Knowledge series.

13. HASSAN, Q.F., 2018. *Internet of Things A to Z: Technologies and Applications*, Wiley-IEEE Press.

14. HASSEN. M., CARVALHO, M.M., CHAN, P.K., 2017. *Malware classification using static analysis based features*, IEEE Symposium Series on Computational Intelligence (SSCI).

15. HOLMA, H., TOSKALA, A., NAKAMURA, T., 2020. *5G Technology: 3GPP New Radio*, Wiley.

16. HUSSAIN, F., HUSSAIN, R., HASSAN, S.A., HOSSAIN, E., 2020. *Machine Learning in IoT Security: Current Solutions and Future Challenges*, University of Canberra.

17. HUTTER, F., KOTTHOFF, L., VANSCHOREN, J., 2019. *Automated Machine Learning: Methods, Systems*, Challenges, Springer.

18. IETF. *The Internet of Things.* [Online]. [ημερομηνία πρόσβασης 30 Σεπτεμβρίου]. Διαθέσιμο στο: https://www.ietf.org/topics/iot/

19. KHALIFA, W.H., ROUSHDY, M., SALEM, A.B.B., 2016. *Machine Learning Techniques for Intelligent Access Control,* New Approaches in Intelligent Image Analysis, Springer.

20. KIM, J., KIM, J., THU, H. L. T., and KIM, H., 2016. *Long short term memory recurrent neural network classifier for intrusion detection*, in 2016 International Conference on Platform Technology and Service (PlatCon), pp. 1–5, Feb 2016.

21. KORENDA, R.A., AFHAH, F., CAMBOU, B., PHILABAUM, C., 2019. *A Proof of Concept SRAM-based Physically Unclonable Function (PUF) Key Generation Mechanism for IoT Devices,* SECON 2019 workshop on Security Trust and Privacy in Emerging Cyber-Physical Systems.

22. LAWTON, G., 2004. *Machine-to-machine technology gears up for growth. Computer* [Online]. Sept. 2004, Volume: 37, Issue: 9, pp.12-15. [ημερομηνία πρόσβασης 30 Σεπτεμβρίου]. Διαθέσιμο στο: https://ieeexplore.ieee.org/document/1332996?tp=&arnumber=1332996&url=http:%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1332996

23. LIU, Y., KUANG Y., XIAO, Y., and XU, G., 2018. *Sdn-based data transfer security for internet of things.* IEEE Internet of Things Journal [Online], vol. 5, Issue 1, pp. 257– 268. [ημερομηνία πρόσβασης 28 Οκτωβρίου]. Διαθέσιμο στο: https://ieeexplore.ieee.org/abstract/document/8125690

24. NAEEM, H., GUO, B., NAEEM, M., 2018. *A light-weight malware static visual analysis for IoT infrastructure,* Computer Science 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD).

25. NESA, N., GHOSH, T., and BANERJEE, I., 2018. *Non-parametric sequence-based learning approach for outlier detection in iot*, Future Generation Computer Systems, vol. 82, pp. 412 – 421, 2018.

26. Net-informations, 2020. *1G Vs. 2G Vs. 3G Vs. 4G Vs. 5G.* [Online]. [ημερομηνία πρόσβασης 25 Οκτωβρίου]. Διαθέσιμο στο: http://net-informations.com/q/diff/generations.html

27. OSAHN, D., KURAL, O.E., AKLEYLEK, S., KILIC, E., 2018. *New results on permission based static analysis for Android malware*, 6th International Symposium on Digital Forensic and Security (ISDFS).

28. PATIL, H. K., and SESHADRI, R., 2014. *Big data security and privacy issues in healthcare.* [Online] [ημερομηνία πρόσβασης 28 Οκτωβρίου]. Διαθέσιμο στο: https://ieeexplore.ieee.org/document/6906856?denied=

29. PENTTINEN, J.T.J., 2019. *5G Simplified: ABCs of Advanced Mobile Communications,* Independently published.

30. PRESS, G., 2014. *A Very Short History Of The Internet Of Things*. [Online]. [ημερομηνία πρόσβασης 30 Σεπτεμβρίου]. Διαθέσιμο στο: https://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/?sh=39dd000710de#bcacd59350a3

31. SADEGHI, A.-R., WACHSMANN, C., and WAIDNER, M., 2015. *Security and privacy challenges in industrial internet of things. 52Nd Annual Design Automation Conference.* [Online] [ημερομηνία πρόσβασης 28 Οκτωβρίου]. Διαθέσιμο στο: https://ieeexplore.ieee.org/document/7167238

32. SAEED, AHMADINIA, A., JAVED, A., and LARIJANI, H., 2016. *Intelligent intrusion detection in low-power iots,* ACM Trans. Internet Technol., vol. 16, pp. 27:1–27:25, Dec. 2016.

33. SALAMEH, H. B., ALMAJALI, S., AYYASH, M., and ELGALA, H., 2018. *Spectrum assignment in cognitive radio networks for internet-of-things delay-sensitive applications under jamming attacks.* IEEE Internet of Things Journal [Online] March 2018, Volume: 5, Issue 3, pp. 1904–1913. [ημερομηνία πρόσβασης 28 Οκτωβρίου]. Διαθέσιμο στο: https://ieeexplore.ieee.org/document/8320276

34. SEDJELMACI, H., SENOUCI, S. M., and AL-BAHRI, M., 2016. *A lightweight anomaly detection technique for low-resource iot devices: A gametheoretic methodology*, in 2016 IEEE International Conference on Communications (ICC), pp. 1–6, May 2016.

35. SERPANOS, D., WOLF, M., 2018. *Internet-of-Things (IoT) Systems: Architectures, algorithms, methodologies,* Springer.

36. SHUKLA, P., 2017. *Ml-ids: A machine learning approach to detect wormhole attacks in internet of things*, in 2017 Intelligent Systems Conference (IntelliSys), pp. 234–240, Sept 2017.

37. SOMASUNDARAM, K., SELVAM K., 2018. *IOT - Attacks and Challenges*, International Journal of Engineering and Technical Research (IJETR), 8(9), pp. 9-12.

38. SOMAUSUNDARAM, K., SELVAM, K., 2018. *IOT - Attacks and Challenges*, International Journal of Engineering and Technical Research (IJETR), 8(9), pp. 9-12.

39. VIEGAS, E., SANTIN, A., OLIVEIRA, L., FRANCA, A., JASINSKI, R., and PEDRONI, V., 2018. *A reliable and energy-efficient classifier combination scheme for intrusion detection in embedded systems*, Computers & Security, vol. 78, pp. 16 – 32, 2018.

40. VOHRA, S., SRIVASTAVA, R., 2015. *A Survey on Techniques for Securing 6LoWPA.* [Online]. [ημερομηνία πρόσβασης 30 Σεπτεμβρίου]. Διαθέσιμο στο: https://ieeexplore.ieee.org/abstract/document/7279997

41. WANG, N., WANG, P., ALIPOUR-FANID, A., JIAO, L., ZENG, K., 2019. *Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities*, IEEE Internet of Things Journal, 6(5), pp.8169-8181.

42. WIKIPEDIA., 2020. *1G.* [Online]. [ημερομηνία πρόσβασης 25 Οκτωβρίου]. Διαθέσιμο στο: https://en.wikipedia.org/wiki/1G

43. XIAO, L., WAN, X., LU, X., ZHANG, Y., WU, D., 2018. *IoT Security Techniques Based on Machine Learning*, IEEE Signal Processing Magazine.

44. YEO, M., KOO, Y., YOON, Y., HWANG, T., RYU, J., SONG, J., PARK, C., 2018. *Flow-based malware detection using convolutional neural network*, International Conference on Information Networking (ICOIN).

45. ΑΓΓΙΣΤΡΙΩΤΗΣ, Ν., 2020. *ΜΗΧΑΝΙΚΗ ΜΑΘΗΣΗ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ 5G.* [Online]. Διπλωματική Εργασία. Πανεπιστήμιο Πατρών.

[ημερομηνία πρόσβασης 20 Νοεμβρίου]. Διαθέσιμο στο: https://nemertes.lis.upatras.gr/jspui/bitstream/10889/14047/1/%CE%94%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE%20%CE%B5%CF%81%CE%B3%CE%B1%CF%83%CE%AF%CE%B1.pdf

46. ΑΠΟΣΤΟΛΟΠΟΥΛΟΣ, Π., 2020. *INTERNET OF THINGS.* [Online]. [ημερομηνία πρόσβασης 13 Νοεμβρίου]. Διαθέσιμο στο: https://securityreport.gr/magazine-archive/etos-2020/item/8271-internet-of-things

47. BOULOGEORGOS, A.A., PAPPI, K.N., KARAGIANNIDIS, G.K., 2017. *Low Power Wide Area Networks for IoT Applications,* Aristotle University of Thessaloniki, Thessaloniki.

48. ΒΕΛΛΙΣΣΑΡΗΣ, Γ.Κ., 2017. *Μελέτη χρήσης τεχνολογιών διασυνδεδεμένων δεδομένων στο διαδίκτυο των πραγμάτων,* Διπλωματική εργασία, Εθνικό Μετσόβειο Πολυτεχνείο, Αθήνα.

49. ΓΛΕΤΖΑΚΟΣ, Δ., 2016. Σύστημα διαχείρισης ραντεβού (Php-Html-Βάση Δεδομένων). [Online]. Διπλωματική Εργασία. ΑΝΩΤΑΤΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ ΤΕΧΝΟΛΙΓΙΚΟΥ ΤΟΜΕΑ. [ημερομηνία πρόσβασης 13 Νοεμβρίου]. Διαθέσιμο στο: http://okeanis.lib2.uniwa.gr/xmlui/handle/123456789/3150

50. ΚΑΡΑΓΙΑΝΝΗΣ, Ε., 2017. *Μελέτη τεχνικών εξόρυξης δεδομένων και μηχανικής μάθησης για χρήση σε συστήματα ανίχνευσης εισβολών.* [Online]. Μεταδιπλωματική εργασία. ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ. [ημερομηνία πρόσβασης 20 Νοεμβρίου]. Διαθέσιμο στο: http://dione.lib.unipi.gr/xmlui/handle/unipi/10987

51. ΚΑΤΖΑΒΕΛΟΥ, Ι., 2018. Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων. Αθήνα: Πανεπιστήμιο Δυτικής Αττικής.

52. ΚΑΤΣΙΚΑ, Σ., ΓΚΡΙΤΖΑΛΗ, Δ., ΓΚΡΙΤΖΑΛΗ, Σ., 2004. Ασφάλεια Πληροφοριακών Συστημάτων. 1η εκδ. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

53. ΚΟΥΛΟΥΒΑΚΗΣ, Θ., 2019. Η τεχνητή νοημοσύνη, η μηχανική μάθηση και το διαδίκτυο των πραγμάτων στον τομέα της υγείας. [Online]. [ημερομηνία πρόσβασης 13 Νοεμβρίου]. Διαθέσιμο στο: https://www.offlinepost.gr/2019/12/02/%CE%B7-%CF%84%CE%B5%CF%87%CE%BD%CE%B7%CF%84%CE%AE-%CE%BD%CE%BF%CE%B7%CE%BC%CE%BF%CF%83%CF%8D%CE%B

D%CE%B7-%CE%B7-%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%B9%CE%BA%CE%AE-%CE%BC%CE%AC%CE%B8%CE%B7%CF%83%CE%B7/

54. ΜΙΝΤΗΣ, Δ., 2018. *Επικοινωνίες 5ης Γενιάς (5G)-Εφαρμογές, Τεχνολογίες και Πρότυπα,* Διπλωματική εργασία, Αλεξάνδρειο ΤΕΙ Θεσσαλονίκης, Θεσσαλονίκη.

55. ΜΙΧΑΗΛ, Ι., 2019. Μελέτη και μοντελοποίηση δικτύου επικοινωνίας IoT οντοτήτων και εκτέλεση σεναρίων επίθεσης/άμυνας από εξωτερικούς πράκτορες καθώς και πρόταση τεχνικών/πρωτοκόλλων ασφάλειας. [Online]. Διπλωματική Εργασία. Πανεπιστήμιο Δυτικής Μακεδονίας. [ημερομηνία πρόσβασης 20 Νοεμβρίου]. Διαθέσιμο στο: http://dspace.uowm.gr/xmlui/handle/123456789/1509

56. ΠΑΝΤΖΙΟΥ, Γ., ΜΑΜΑΛΗΣ, Β., ΚΑΡΚΑΖΗΣ, Π., 2020. Δίκτυα Αισθητήρων και Διαδίκτυο των Αντικειμένων. IoT Basics & Applications. Αθήνα: Πανεπιστήμιο Δυτικής Αττικής.

57. ΠΑΓΚΑΛΟΥ, Γ., ΜΑΥΡΙΔΗ, Ι., 2002. Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων. 1η εκδ. Θεσσαλονίκη: Εκδόσεις Ανικούλα.

58. ΠΑΠΑΖΩΗΣ, Π., 2007. Ασφάλεια στο διαδίκτυο των πραγμάτων. [Online]. Μεταδιπλωματική Εργασία. Πανεπιστήμιο Αιγαίου. [ημερομηνία πρόσβασης 20 Νοεμβρίου]. Διαθέσιμο στο: https://hellanicus.lib.aegean.gr/handle/11610/18539

59. ΣΟΛΔΑΤΟΣ, Φ., 2017. *Internet of Things (IoT).* [Online]. Εργασία Εξαμήνου. Πανεπιστήμιο Πατρών. [ημερομηνία πρόσβασης 20 Οκτωβρίου]. Διαθέσιμο στο: http://telematics.upatras.gr/telematics/system/files/bouras_site/ergasies_foithtwn/IoT_soldatos.pdf?language=el

60. ΣΤΑΜΑΤΟΠΟΥΛΟΣ, Δ., 2020. *Μελέτη και αξιολόγηση των προτεινόμενων τεχνολογιών στα δίκτυα 5G και μεταγενέστερα (6G).* [Online]. Διπλωματική Εργασία. Πανεπιστήμιο Πατρών. [ημερομηνία πρόσβασης 3 Νοεμβρίου]. Διαθέσιμο στο: http://telematics.upatras.gr/telematics/system/files/bouras_site/ergasies/diplwmatikes/%CE%94%CE%B9%CF%80%CE%BB%CF%89%CE%BC%CE%B1%CF%84%CE%B9%CE%BA%CE%AE%20%CE%B5%CF%81%CE%B3%CE%B1%CF%83%CE%AF%CE%B1%20%CE%A3%CF%84%CE%B1%CE%BC%CE%B1%CF%84%CF%8C%CF%80%CE%BF%CF%85%CE%BB%CE%BF%CF%82%20%CE%94%CE%B7%CE%BC%CE%AE%CF%84%CF%81%CE%B9

%CE%BF%CF%82%20Final!.pdf?language=el

61. ΤΖΑΝΑΚΟΣ, Δ., 2020. *ΜΕΛΕΤΗ ΑΠΟΔΟΣΗΣ MACHINE LEARNING ΑΛΓΟΡΙΘΜΩΝ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΜΙΜΟ ΣΤΑ ΚΙΝΗΤΑ ΔΙΚΤΥΑ 5ΗΣ ΓΕΝΙΑΣ.* [Online]. ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ. ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ. [ημερομηνία πρόσβασης 3 Νοεμβρίου]. Διαθέσιμο στο: https://nemertes.library.upatras.gr/jspui/bitstream/10889/13529/1/%CE%A0%CF%84%CF%85%CF%87%CE%B9%CE%B1%CE%BA%CE%AE_%CE%A4%CE%B6%CE%B1%CE%BD%CE%AC%CE%BA%CE%BF%CF%82_%CF%84%CE%B5%CE%BB%CE%B9%CE%BA%CF%8C-converted.pdf

62. TSIATSIS, V., KARNOUSKOS, S., HOLLER, J., BOYLE, D., MULIGAN, C., 2018. *Internet of Things: Technologies and Applications for a New Age of Intelligence*, 2nd Edition, Academic Press.