ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Μελέτη και ανάλυση παραβιάσεων ιδιωτικότητας σε περιβάλλοντας έξυπνων σπιτιών και έξυπνων πόλεων

Διπλωματική Εργασία

Της

Τσανή Π. Σοφίας

Θεσσαλονίκη,23/04/2021

Μελέτη και ανάλυση παραβιάσεων ιδιωτικότητας σε περιβάλλοντα έξυπνων σπιτιών και έξυπνων πόλεων

Σοφία Π. Τσανή

Πτυχίο Νομικής, ΑΠΘ 2006

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής

Παπαδημητρίου Παναγιώτης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ηη/μμ/εεεε

Ονοματεπώνυμο 1	Ονοματεπώνυμο 2	Ονοματεπώνυμο 3
.....	.....	.....

ΠΕΡΙΛΗΨΗ

Το Διαδίκτυο των Πραγμάτων (Internet of Things-IOT) είναι μία από τις κορυφαίες τεχνολογικές εξελίξεις, θεωρούμενο από πολλούς ότι αποτελεί την 4η Βιομηχανική Επανάσταση. Δεδομένου ότι η παρουσία του στην καθημερινότητα θα γίνεται συνεχώς πιο έντονη, καθώς η χρήση των έξυπνων συσκευών, αυξάνεται με ιλιγγιώδη ταχύτητα σε όλες τις πτυχές της καθημερινότητας, η παρούσα διπλωματική εργασία έχει ως στόχο τη μελέτη των ζητημάτων και παραβιάσεων ιδιωτικότητας στα έξυπνα περιβάλλοντα, καθώς η ίδια τους η αρχιτεκτονική, δηλαδή η συλλογή, επεξεργασία και διαμοιρασμός τεράστιου όγκου δεδομένων μέσα από τη διασύνδεση αναρίθμητων συσκευών εγείρει μεγάλα ζητήματα ασφαλείας.

Λέξεις Κλειδιά: Διαδίκτυο των Πραγμάτων (Internet of Things- IOT), έξυπνες συσκευές, έξυπνες πόλεις, έξυπνο σπίτι, νέφος, δεδομένα μεγάλης κλίμακας, εξόρυξη δεδομένων, δρομολόγηση, ασφάλεια, κίνδυνοι

ABSTRACT

Internet of Things-IOT is one of the most significant technological evolutions, as it is considered to be the 4th Industrial Revolution. Considering that its use in everyday life is constantly more intense, due to the increasing use of smart devices in all aspects of life, this thesis aims at studying the issues and violations of privacy in smart environments. These issues essentially stem from the collection, processing and sharing of large amounts of data through the interaction and interconnection of a vast number of devices.

Keywords: Internet of Things-IOT, smart devices, smart cities, smart home, cloud, Big Data, Data Mining, Routing, security, risks

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. ΕΙΣΑΓΩΓΗ

Το Διαδίκτυο των Πραγμάτων (Internet of Things-IOT) είναι η τεχνολογία του μέλλοντος, που θα επιτρέψει τη βελτίωση της καθημερινότητας των ανθρώπων και των κοινωνιών με τη βελτίωση των παρεχόμενων υπηρεσιών σε κρίσιμους τομείς, όπως υγεία, ενέργεια, επιχειρηματικότητα, εκπαίδευση κ.λ.π, μέσω της συλλογής πληροφορ ιών σε πραγματικό χρόνο και της αλληλεπίδρασης συσκευών, ανθρώπων και οντοτήτων.

Η ετερογένεια όμως του έξυπνου συστήματος και των συσκευών, η υπολογιστική τους ικανότητα που επιτρέπει την αυτόνομη και διαρκή προσαρμογή τους στις αλλαγές των συνθηκών και ερεθισμάτων, η ευαισθησία των αισθητήρων και η διαρκής συλλογή τεραστίου αριθμού δεδομένων σε πραγματικό χρόνο, καθιστά το έξυπνο σύστημα ευάλωτο σε κακόβουλες επιθέσεις, καθώς κάθε μέρος του συστήματος διαθέτει και διαφορετικές αδυναμίες. Επίσης, λόγω της αλληλεπίδρασης των μερών μεταξύ τους, η παραβίαση ενός εξ αυτών οδηγεί μοιραία σε παραβίαση όλου του έξυπνου συστήματος.

Εκτός των ανωτέρω, δημιουργούνται και πολλά ζητήματα ασφαλείας όσον αφορά την εν αγνοία των τελικών χρηστών συλλογή δεδομένων, την αυθεντικοποίηση/εμπιστοσύνη των διασυνδεδεμένων συσκευών και άρα της γνησιότητας των συλλεχθέντων πληροφοριών, τον κίνδυνο παρακολούθησης, ειδικά των έξυπνων σπιτιών, αλλά και την ασφάλεια και ιδιωτικότητα των συλλεχθέντων δεδομένων (πού και πώς αυτά αποθηκεύονται και χρησιμοποιούνται). Επιπρόσθετα, με τη χρήση σύγχρονων τεχνικών, όπως της εξόρυξης δεδομένων, όχι μόνο υπάρχει δυνατότητα ταυτοποίησης και δημιουργίας μοτίβων συμπεριφοράς των χρηστών, αλλά επιπλέον και ανακάλυψης πληροφοριών για πρόσωπα που ούτε τα ίδια γνωρίζουν. Άλλοι κίνδυνοι που δημιουργούνται, είναι ο χρήστης να πέσει θύμα ανέλεγκτων αυτοματοποιημένων αποφάσεων και δημοσιοποίησης ευαίσθητων προσωπικών του δεδομένων.

Βάσει όλων των ανωτέρω κινδύνων, είναι κρίσιμη η δημιουργία υποχρεωτικών προτύπων ασφαλείας έτσι ώστε να επιτευχθεί η ασφάλεια εκ κατασκευής καθώς και η προσπάθεια αποτελεσματικής πρόβλεψης των αδυναμιών του συστήματος και πρόληψης των επιθέσεων. Επιπλέον, όλα αυτά θα πρέπει να συνοδεύονται από αποτελεσματικές νομοθετικές ενέργειες και πολιτικές προστασίας. Μόνο έτσι, μπορεί

να διασφαλιστεί μία αποτελεσματική θωράκιση του διάχυτου έξυπνου συστήματος παράλληλα με τη ραγδαία τεχνολογική εξέλιξη [1].

1.1. ΣΤΟΧΟΙ ΤΗΣ ΠΑΡΟΥΣΑΣ ΔΙΠΛΩΜΑΤΙΚΗΣ

Στην παρούσα διπλωματική εργασία, παρουσιάζονται και αναλύονται οι επιθέσεις, οι κίνδυνοι ασφαλείας και ιδιωτικότητας που ελλοχεύουν σε διάφορα επίπεδα του έξυπνου δικτύου, από τη βάση, ήτοι τις έξυπνες συσκευές, τα πρωτόκολλα που χρησιμοποιούνται, τη δρομολόγηση των δεδομένων, μέχρι και το νέφος. Ειδικότερα αναλύονται ζητήματα ασφαλείας και ιδιωτικότητας στις έξυπνες πόλεις και το έξυπνο σπίτι και επισημαίνονται πρακτικές των κατασκευαστών, αλλά και των ίδιων των χρηστών που προσελκύουν κινδύνους και καθιστούν το έξυπνο δίκτυο ευάλωτο. Επιπλέον, γίνεται αναφορά στις απειλές ασφαλείας που δημιουργούνται λόγω της χρήσης των τεχνολογιών του νέφους, των μεγάλων δεδομένων και της εξόρυξης αυτών, καθώς και της χρήσης της υπολογιστικής ομίχλης ή άκρου (fog/edge computing). Τέλος, γίνεται μελέτη διάφορων μεθόδων, τεχνολογιών και πρακτικών για την επίτευξη ασφαλείας σε διάφορα επίπεδα του έξυπνου συστήματος.

1.2. ΔΟΜΗ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η παρούσα διπλωματική εργασία έχει την ακόλουθη δομή:

Στο κεφάλαιο 2 της παρούσας διπλωματικής γίνεται μία παρουσίαση της έννοιας και της πυραμίδας τεχνολογίας του διαδικτύου των πραγμάτων. Στο κεφάλαιο 3 παρουσιάζονται τα χαρακτηριστικά, τα συστατικά, καθώς και τα μοντέλα διασύνδεσης των έξυπνων συσκευών. Στο κεφάλαιο 4 γίνεται περιγραφή των διαφόρων πρωτοκόλλων στο διαδίκτυο των πραγμάτων (επικοινωνίας, διασύνδεσης, ασφαλείας) και των ζητημάτων ασφαλείας που σχετίζονται με αυτά και ειδικότερα αναλύεται η τεχνολογία ταυτοποίησης μέσω ραδιοσυχνοτήτων (RFID), τα ζητήματα ασφαλείας που δημιουργούνται με τη χρήση της και οι επιθέσεις κατά των ετικετών. Το κεφάλαιο 5 πραγματεύεται τη δρομολόγηση στο διαδίκτυο των πραγμάτων, την έννοια και τα πρωτόκολλά της, τους κινδύνους και διάφορους τρόπους επίτευξης της ασφαλούς δρομολόγησης. Στο κεφάλαιο 6 περιγράφεται η αρχιτεκτονική, τα χαρακτηριστικά και οι εφαρμογές της έξυπνης πόλης και γίνεται ειδική αναφορά στη δομή του έξυπνου

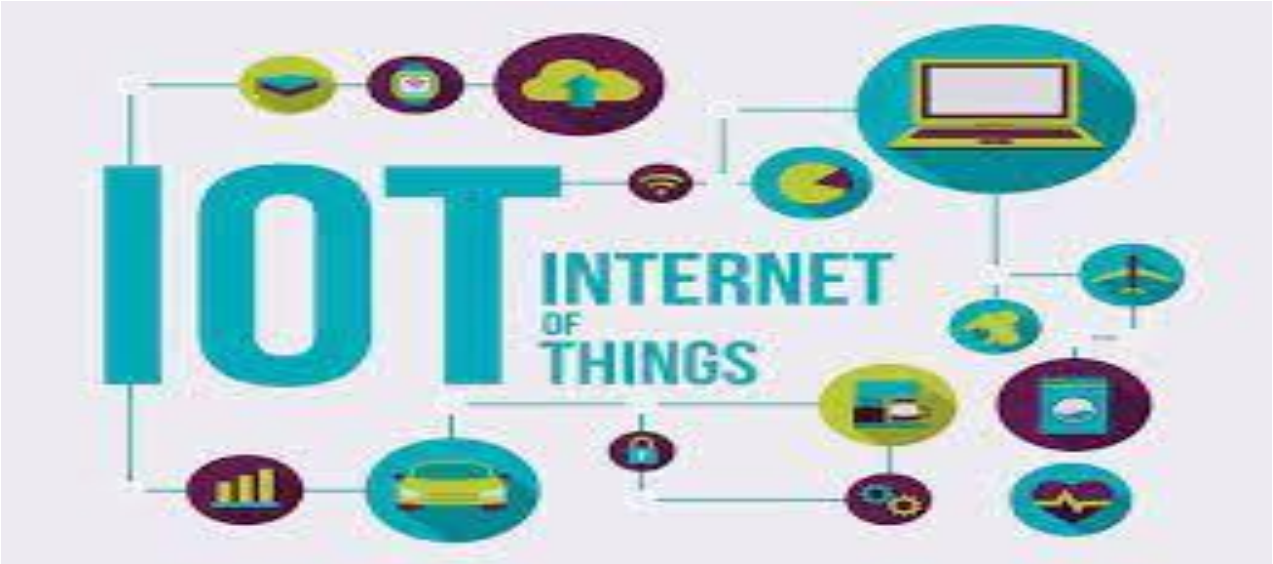
[1] https://securityreport.gr/magazine-archive/etos-2020/item/8271-internet-of-things, (πρόσβαση, 05/02/2021)

σπιτιού και τους κινδύνους ασφαλείας και ιδιωτικότητας που σχετίζονται με αυτό. Στο κεφάλαιο 7 γίνεται ανάλυση όλων των γενικών και ειδικών ζητημάτων ασφαλείας ανά επίπεδο στο Διαδίκτυο των Πραγμάτων, της ασφάλειας των δεδομένων και περιγραφή επικίνδυνων πρακτικών κατασκευαστών και χρηστών αλλά και των κινδύνων που δημιουργούνται από τα κοινά μέσα εισόδου σε όλες τις έξυπνες συσκευές.

Στο κεφάλαιο 8 περιγράφονται οι αδυναμίες ασφαλείας των έξυπνων πόλεων και οι κίνδυνοι του έξυπνου σπιτιού. Το κεφάλαιο 9 πραγματεύεται τις επιθέσεις σε διαφορετικά επίπεδα του Διαδικτύου των Πραγμάτων και τα είδη επιθέσεων στις έξυπνες πόλεις και το έξυπνο σπίτι. Στο κεφάλαιο 10 περιγράφονται οι τριάδες ασφαλείας των έξυπνων συσκευών, προτείνονται λύσεις ασφαλείας σε διάφορα επίπεδα του έξυπνου δικτύου και γίνεται μελέτη των πρακτικών αντιμετώπισης των ευπαθειών των έξυπνων δικτύων και των μεθοδολογιών μέτρησης ασφαλείας πληροφοριών. Επιπρόσθετα, γίνεται ανάλυση των διάφορων μηχανισμών και τεχνολογιών ασφαλείας των έξυπνων δικτύων (κρυπτογράφηση, τεχνολογία κατανεμημένης εγγραφής-Blockchain κ.λ.π.) και προτείνονται λύσεις επίτευξης της ασφάλειας από τη βάση μέχρι το νέφος.

Στο κεφάλαιο 11 δίνεται ο ορισμός του νέφους και του νέφους των πραγμάτων, αναλύονται οι κίνδυνοι και πρακτικές ασφαλείας του νέφους και ειδικά η κυριότητα, αποθήκευση και έλεγχος των δεδομένων, περιγράφονται οι επιθέσεις που δέχεται και προτείνονται τρόποι αντιμετώπισης των κινδύνων. Στο κεφάλαιο 12 δίνεται ο ορισμός των μεγάλων δεδομένων και περιγράφεται η αρχιτεκτονική, επεξεργασία και ανάλυσή τους, καθώς και τα ζητήματα ασφαλείας που σχετίζονται με αυτά. Στο κεφάλαιο 13 περιγράφεται η έννοια, η διαδικασία και οι κατάλληλες τεχνικές της εξόρυξης δεδομένων στο διαδίκτυο των πραγμάτων καθώς και τα ζητήματα ασφαλείας αυτών. Στο κεφάλαιο 14 αναλύεται η υπολογιστική ομίχλης ή άκρου, η αρχιτεκτονική, τα βασικά χαρακτηριστικά και τα ζητήματα ασφαλείας της. Στο κεφάλαιο 15 γίνεται αναφορά της συμβολής του Κανονισμού 2016/679 στην προστασία των προσωπικών δεδομένων καθώς και η σημασία της συναίνεσης στο Διαδίκτυο των Πραγμάτων. Τέλος, το κεφάλαιο 16 επισημαίνει τα συμπεράσματα της παρούσας εργασίας και τις μελλοντικές κατευθύνσεις.

2.ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (INTERNET OF THINGS/IOT)



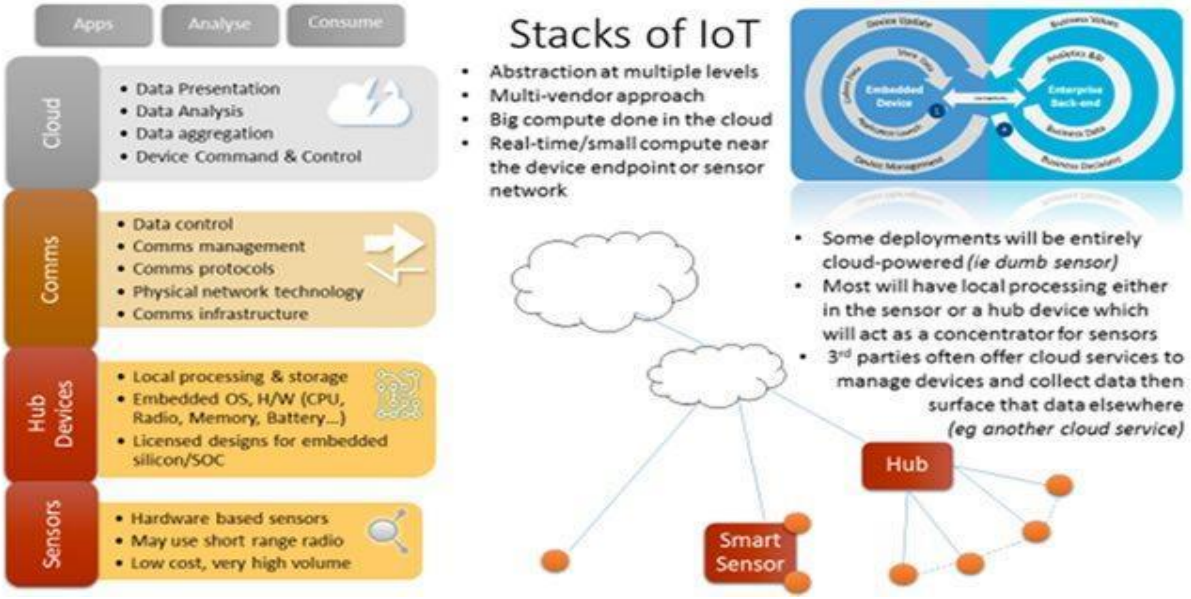
Εικόνα 1: Διαδίκτυο των Πραγμάτων [2]

Το **Διαδίκτυο των Πραγμάτων** (**Internet of Things**) αποτελεί το δίκτυο επικοινωνίας των συσκευών καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Βασικό χαρακτηριστικό του είναι η διασύνδεση των μερών/συσκευών (τοπικό δίκτυο ή σύνδεση στο διαδίκτυο), με στόχο να ελέγχονται από τον χρήστη μέσω υπολογιστή ή έξυπνου τηλεφώνου.

Θα πρέπει να σημειωθεί ότι δεν υπάρχει ακόμα συγκεκριμένο αρχιτεκτονικό μοντέλο ικανό να μοντελοποιήσει το έξυπνο περιβάλλον. Έτσι, έξυπνη συσκευή είναι κάθε τύπος εξοπλισμού, εργαλείου ή μηχανήματος που έχει υπολογιστική ικανότητα,[3] δηλαδή μπορεί να λειτουργήσει σε κάποιο βαθμό διαδραστικά και αυτόνομα[4]. Τα δεδομένα από και προς τις συσκευές συλλέγονται, ενσωματώνονται από έναν αθροιστή (λογισμικό ή ιστός), υπόκεινται σε επεξεργασία και είτε αποθηκεύονται, είτε προωθούνται στις συσκευές, είτε ανταλλάσσονται μεταξύ των συσκευών (Peer to Peer) (Florian Metzger, et al., 2019).

[2] https://www.i-scoop.eu/internet-of-things-guide/iot-technology-stack-devices-gateways-platforms/, (πρόσβαση, 15/01/2021)
[3] https://whatis.techtarget.com/definitions/S/page/11 , (Πρόσβαση, 23/01/2021)
[4] https://link.springer.com/article/10.1186/s40327-018-0063-8, (Πρόσβαση,23/01/2021)

2.1. ΠΥΡΑΜΙΔΑ ΤΕΧΝΟΛΟΓΙΑΣ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (IOT TECHNOLOGY STACK)



Εικόνα 2: Πυραμίσα Τεχνολογίας Διαδικτύου των Πραγμάτων [5]

Το διαδίκτυο των πραγμάτων (Internet of Things-IOT) είναι ένα δίκτυο η λειτουργία του οποίου εξαρτάται από πολλά επίπεδα, τα οποία είναι (Boris & Thomas, 2017):

<u>1ο επίπεδο Υλικό (Hardware):</u> Πρόκειται για τις συσκευές, αισθητήρες, ενεργοποιητές κλπ με τις οποίες επιτυγχάνεται η διασύνδεση, επιτρέποντας τη συλλογή πληροφοριών.

<u>2ο επίπεδο Λογισμικό (Software):</u> Πρόκειται για το σύστημα που μετατρέπει τις συσκευές σε έξυπνες, επιτρέποντας την επικοινωνία είτε των συσκευών μεταξύ τους είτε με ένα νέφος, μέσω της συλλογής, του ελέγχου και γενικώς της επεξεργασίας των δεδομένων. Το λογισμικό αποτελείται από το Λειτουργικό Σύστημα των συσκευών (OS) και τις εφαρμογές (Applications).

<u>3ο επίπεδο Επικοινωνία:</u> Αυτό το επίπεδο είναι πολύ σημαντικό καθώς καθορίζει τον τρόπο λήψης των δεδομένων από τα μέρη/συσκευές του έξυπνου δικτύου αλλά και την αλληλεπίδραση τους με το νέφος ή τρίτες συσκευές. Επίσης, αυτό το

[5] https://docs.microsoft.com/el-gr/archive/blogs/uktechnet/what-is-the-internet-of-things-and-where-does-microsoft-sit ,(πρόσβαση, 12/01/2021)

επίπεδο σχετίζεται και με τον τρόπο με τον οποίο γίνεται η ανταλλαγή των πληροφοριών μέσω των δικτύων και των πρωτοκόλλων που χρησιμοποιούνται.

4ο επίπεδο Πλατφόρμα Νέφους: Αυτό το επίπεδο αποτελεί τη ραχοκοκκαλιά όλου του έξυπνου συστήματος, καθώς το νέφος σχετίζεται με τη συλλογή και διαχείριση των δεδομένων, καθορίζοντας την ποσότητα και το είδος των δεδομένων που συλλέγονται σε καθημερινή βάση, με τη χρήση της αναλυτικής και της διασύνδεσης προγραμματισμού εφαρμογών του νέφους (API). Η αναλυτική έχει την ικανότητα να διαμοιράζει τα δεδομένα, να ανακαλύπτει μοτίβα, να κάνει προβλέψεις, να αφομοιώνει τη γνώση λειτουργίας των συσκευών κ.λ.π. ενώ με τη χρήση της διασύνδεσης προγραμματισμού εφαρμογών του νέφους (API), επιτυγχάνεται η διασύνδεση των συσκευών, ο διαμοιρασμός δεδομένων και η χρήση τους από τους τελικούς χρήστες.

5ο επίπεδο Εφαρμογές Νέφους: Πρόκειται για εφαρμογές που απευθύνονται απευθείας στον τελικό χρήστη, όπως είναι το έξυπνο σπίτι, η έξυπνη ενέργεια, τα έξυπνα αυτοκίνητα κλπ.

3.ΕΞΥΠΝΕΣ ΣΥΣΚΕΥΕΣ

Οι έξυπνες συσκευές, διαθέτουν μικροεπεξεργαστή και έχουν την ικανότητα να διαμοιράζονται πληροφορίες με άλλες συσκευές και συστήματα και να αφομοιώνουν εφαρμογές, χρησιμοποιώντας εξελιγμένες διασυνδέσεις προγραμματισμού εφαρμογών του νέφους (APIs). Η χρήση των έξυπνων συσκευών στοχεύει στην αξιολόγηση των διαφόρων συνθηκών και τη μετάδοσή τους στον χρήστη.

Οι έξυπνες συσκευές διασυνδέονται συνήθως ασύρματα. Διαθέτουν αισθητήρες οι οποίοι χρησιμοποιούνται για να συλλέξουν δεδομένα, μετρώντας θερμοκρασία, υγρασία, κινήσεις κλπ. Εν συνεχεία αφού οι συσκευές συλλέξουν τα δεδομένα από τους αισθητήρες, διαθέτουν ένα σύστημα το οποίο τα αποστέλλει σε έναν κεντρικό διακομιστή νέφους, ο οποίος τα επεξεργάζεται και διαμοιράζει τα αποτελέσματα σε συνδεδεμένες κινητές εφαρμογές. Οι αισθητήρες χρησιμοποιούνται για τη μέτρηση διάφορων μεγεθών με τη χρήση ενός πίνακα μικροελέγχου (MCU), ο οποίος αποτελείται από έναν επεξεργαστή, μία μνήμη και μερικές άλλες ενσωματωμένες μεταξύ τους συσκευές.

3.1. ΣΥΣΤΑΤΙΚΑ & ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΕΞΥΠΝΩΝ ΣΥΣΚΕΥΩΝ

Οι έξυπνες συσκευές αποτελούνται από τα εξής στοιχεία (Boris & Thomas, 2017):

α. Συνδεδεμένες συσκευές: Πρόκειται για τα φυσικά αντικείμενα που είναι συνδεδεμένα στο έξυπνο δίκτυο, όπως είναι οι αισθητήρες οι οποίοι συλλέγουν συνεχώς δεδομένα από το περιβάλλον και μεταδίδουν τις πληροφορίες στο επόμενο επίπεδο.

β. Πίνακας Ελέγχου: Ο πίνακας ελέγχου διαχειρίζεται την κυκλοφορία δεδομένων μεταξύ διαφορετικών δικτύων και πρωτοκόλλων, μεταφράζει τα διαφορετικά πρωτόκολλα δικτύου και διασφαλίζει τη διαλειτουργικότητα των συσκευών.

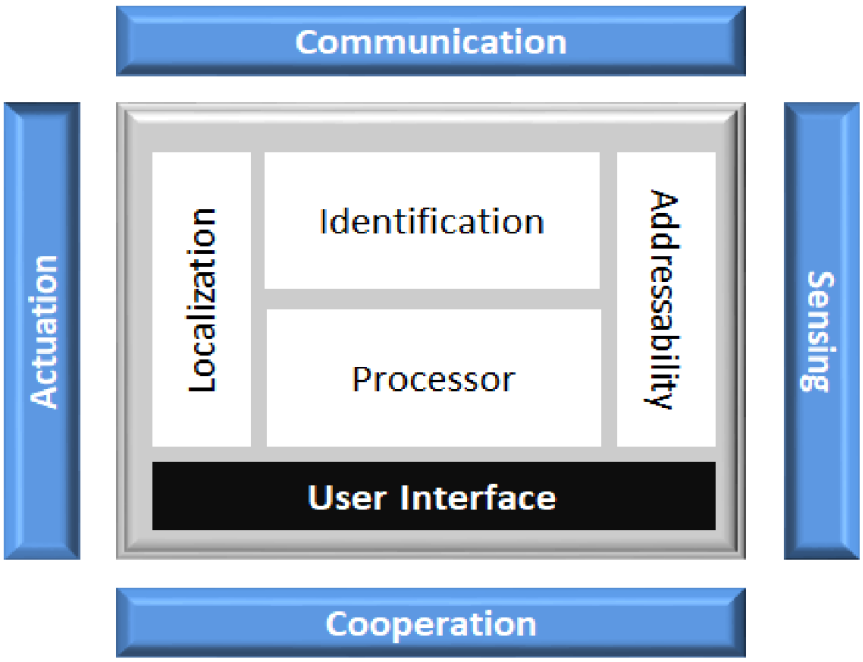
γ. Νέφος Δεδομένων: Το νέφος στο Διαδίκτυο των Πραγμάτων προσφέρει τα κατάλληλα εργαλεία για τη συλλογή, επεξεργασία, διαχείριση και αποθήκευση τεράστιου όγκου δεδομένων σε πραγματικό χρόνο. Οι βιομηχανίες και οι υπηρεσίες μπορούν εύκολα να έχουν πρόσβαση σε αυτά τα δεδομένα από απομακρυσμένη απόσταση και να λαμβάνουν κρίσιμες αποφάσεις όταν είναι απαραίτητο. Τα κατανεμημένα συστήματα διαχείρισης βάσεων δεδομένων είναι από τα απαραίτητα συστατικά του νέφους.

δ. Διεπαφή χρήστη: Πρόκειται για το ορατό, απτό μέρος του έξυπνου δικτύου το οποίο είναι προσβάσιμο και χρησιμοποιείται απευθείας από τους χρήστες.

ε. Διασύνδεση δικτύου: Πρόκειται για τις διάφορες ασύρματες ή ενσύρματες τεχνολογίες που χρησιμοποιούνται για τη διασύνδεση των συσκευών.

στ. Ασφάλεια: Η ασφάλεια είναι βασικό στοιχείο για τη διασφάλιση της λειτουργίας του έξυπνου συστήματος και επιτυγχάνεται με τον εντοπισμό και διόρθωση των αδυναμιών των συσκευών και πρωτοκόλλων του διαδικτύου των πραγμάτων.

ζ. Αναλυτική: Είναι η διαδικασία μετατροπής αναλογικών δεδομένων από διασυνδεδεμένες έξυπνες συσκευές και αισθητήρες σε χρήσιμες πληροφορίες που μπορούν να υποστούν επεξεργασία, να μεταφραστούν και να χρησιμοποιηθούν για λεπτομερή ανάλυση.



Εικόνα 3: Βασικά Χαρακτηριστικά των Έξυπνων Συσκευών *(Filho, 2020)*

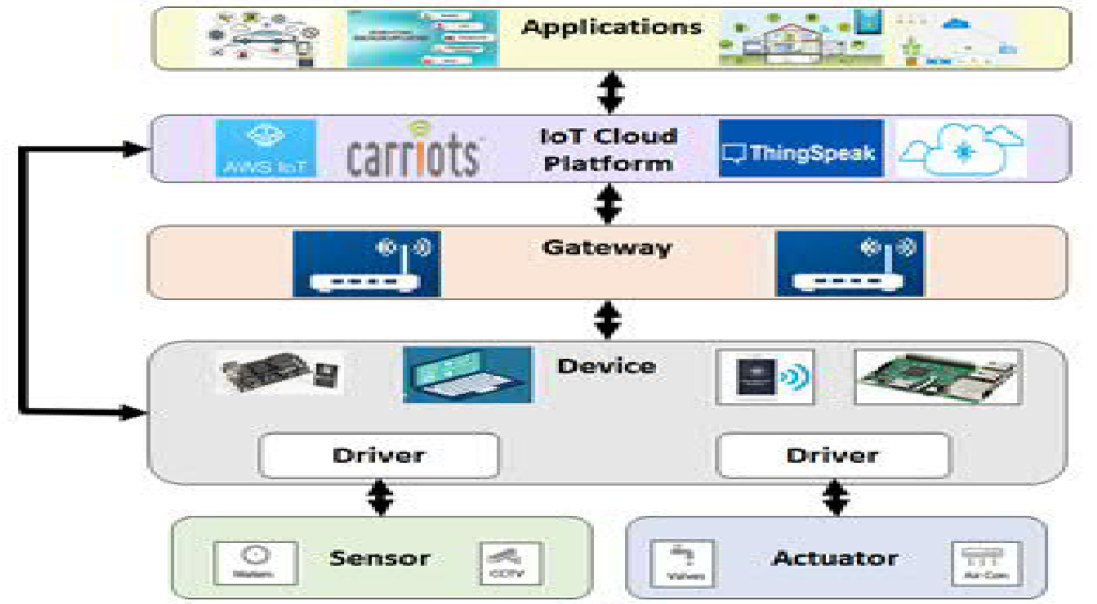
Τα βασικά στοιχεία που χαρακτηρίζουν τη λειτουργία των έξυπνων συσκευών είναι:

α. Η αυτονομία, η οποία συνίσταται στην ικανότητα αυτών να εκτελούν εργασίες ανεξάρτητα και χωρίς την άμεση εντολή του χρήστη.

β. Η συνδεσιμότητα, η οποία σχετίζεται με την δυνατότητα σύνδεσης στο διαδίκτυο καθώς και διασύνδεσης με άλλες συσκευές ανταλλάσσοντας δεδομένα.

γ. Η επίγνωση του περιβάλλοντος, που είναι η ικανότητα των έξυπνων συσκευών να λαμβάνουν πληροφορίες από το περιβάλλον μέσω αισθητήρων, όπως κάμερες, μικρόφωνα, GPS κ.λ.π. και να προσαρμόζονται αναλόγως.

δ. Τέλος, η αλληλεπίδραση των έξυπνων συσκευών με τον χρήστη, έστω και σε κάποιο βαθμό, συλλέγοντας δεδομένα και η κινητικότητα και αποθήκευση αυτών των δεδομένων είναι επίσης μοναδικά στοιχεία των έξυπνων συσκευών που τις χαρακτηρίζουν, καθώς σχετίζονται με την μοναδική ικανότητα τους να εκτελούν αυτόνομους υπολογισμούς.

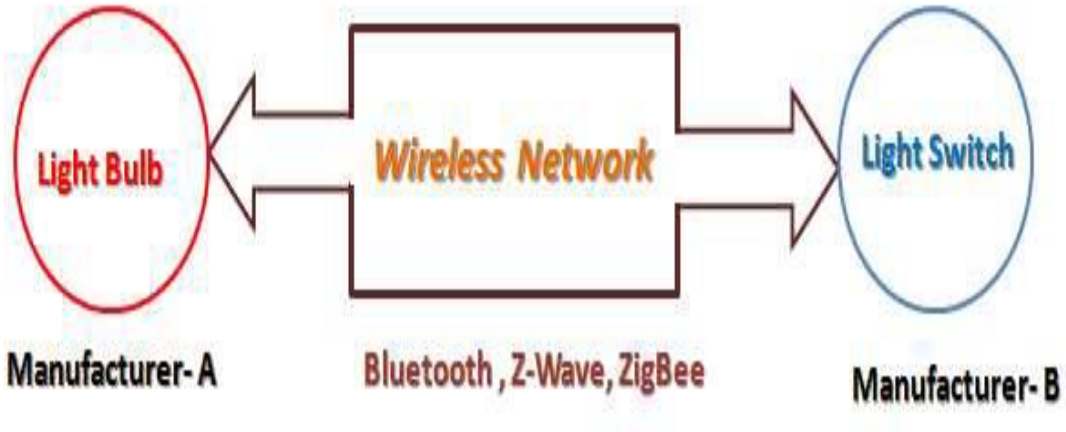


Εικόνα 4: Γενική Αρχιτεκτονική του Έξυπνου Δικτύου (Preeti Agarwal & Mansaf Alam, 2018)

3.2. ΜΟΝΤΕΛΑ ΔΙΑΣΥΝΔΕΣΗΣ ΣΥΣΚΕΥΩΝ

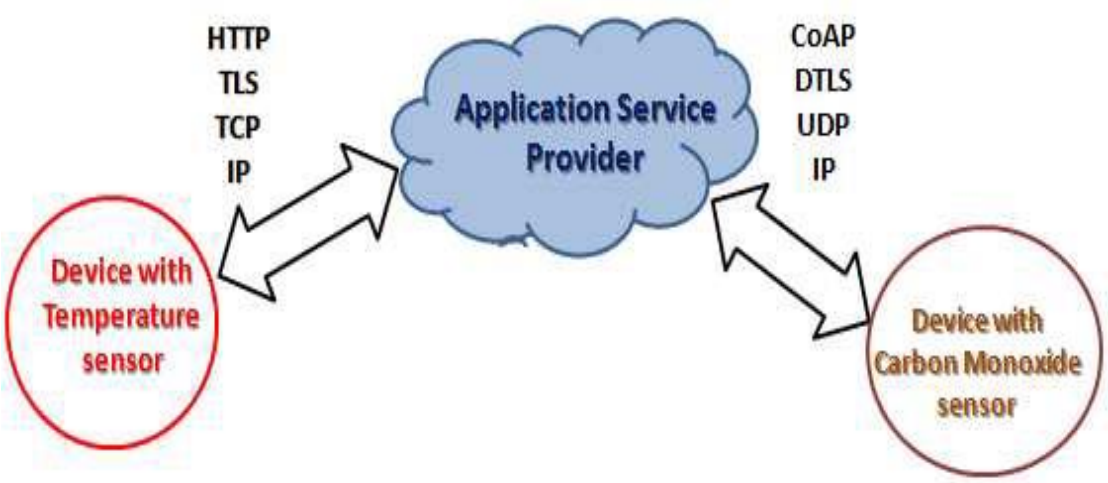
Οι έξυπνες συσκευές συνδέονται και επικοινωνούν κάνοντας χρήση προκαθορισμένων πρωτοκόλλων επικοινωνίας. Το 2015 το Συμβούλιο Αρχιτεκτονικής του Διαδικτύου (IAB), εξέδωσε έναν κατευθυντήριο οδηγό για την διασύνδεση των έξυπνων συσκευών, ο οποίος περιλαμβάνει το γενικό πλαίσιο αρχιτεκτονικής μοντέλων επικοινωνίας που χρησιμοποιείται από έξυπνες συσκευές. Τα βασικά χαρακτηριστικά του κάθε μοντέλου είναι (Santosh Kulkarni, 2017):

α. Μοντέλο Διασύνδεσης συσκευή με συσκευή (Device-to-Device): Το μοντέλο διασύνδεσης Συσκευή με Συσκευή (Device-to-Device) αναπαριστά την άμεση σύνδεση και επικοινωνία μεταξύ δύο συσκευών, χωρίς την χρήση κάποιου ενδιάμεσου διακομιστή. Οι συσκευές που διασυνδέονται χρησιμοποιούν πρωτόκολλα επικοινωνίας όπως το Bluetooth, το Z-Wave και το ZigBee. Αυτές οι συσκευές επικοινωνούν μέσω πολλών διευθύνσεων διαδικτυακού πρωτοκόλλου (IP) ή το διαδίκτυο (Nawazuddin Mohd1, 2018).



Εικόνα 5: Μοντέλο Διασύνδεσης Συσκευή με Συσκευή (Device to Device) (Nawazuddin Mohd1, 2018)

β. Μοντέλο Διασύνδεσης Συσκευή με Νέφος (Device-to-Cloud): Το μοντέλο διασύνδεσης Συσκευή με Νέφος (Device-to-Cloud), επιτρέπει την σύνδεση έξυπνων συσκευών μέσα από μια διαδικτυακή υπηρεσία νέφους η οποία ελέγχει την διαδρομή των μηνυμάτων και επιβλέπει όλη τη διαδικασία. Σε αυτό το πρωτόκολλο επικοινωνίας χρησιμοποιούνται πρωτόκολλα επικοινωνίας, όπως το Ethernet ή το Wi-fi. ((ENISA), 2017).

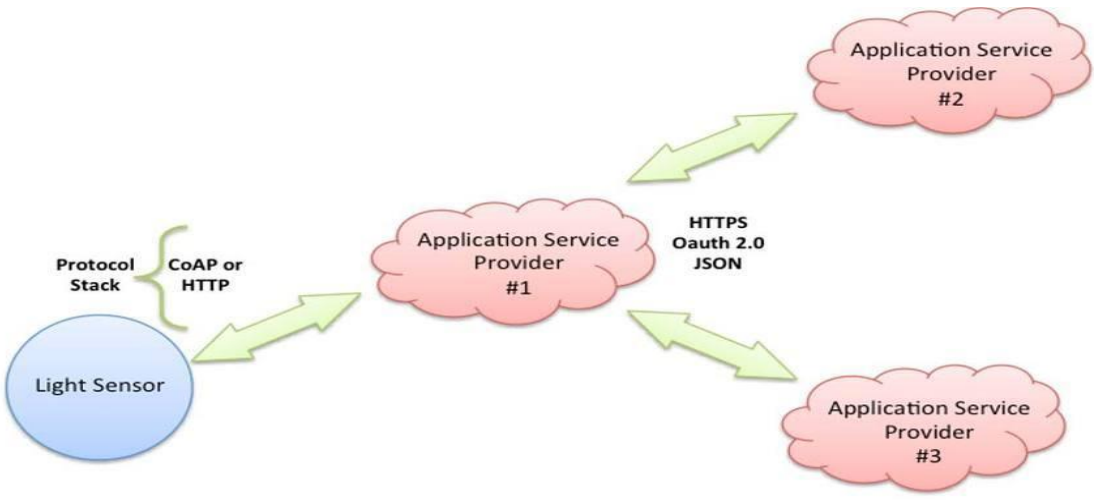


Εικόνα 6: Μοντέλο Διασύνδεσης Συσκευή με Νέφος *(Nawazuddin Mohd1, 2018)*

γ. Μοντέλο Διασύνδεσης Συσκευής με Πύλη (Device-to-Gateway): Σε αυτό το μοντέλο διασύνδεσης, χρησιμοποιείται μία ενδιάμεση συσκευή προκειμένου εν συνεχεία οι έξυπνες συσκευές να συνδεθούν σε μία υπηρεσία νέφους.

Εικόνα 7: Μοντέλο Διασύνδεσης Συσκευής με Πύλη (Nawazuddin Mohd1, 2018)

δ. Μοντέλο Διασύνδεσης του Επιπέδου Πρόσβασης και Διαμοιρασμού Δεδομένων (Back-End Data Sharing): Σε αυτό το μοντέλο διασύνδεσης, οι χρήστες μπορούν να εξάγουν και να αναλύσουν δεδομένα έξυπνων αντικειμένων σε συνδυασμό με δεδομένα και από άλλες πηγές από μια υπηρεσία νέφους. Το μοντέλο διασύνδεσης επιπέδου πρόσβασης και διαμοιρασμού δεδομένων (Back-End Data Sharing), επιτρέπει στα δεδομένα που συλλέγονται από μια έξυπνη συσκευή να συγκεντρώνονται και να αναλύονται.



Εικόνα 8: Μοντέλο Διασύνδεσης Επιπέδου Πρόσβασης και Διαμοιρασμού Δεδομένων (Md Husamuddin & Mohammed Qayyum, 2017)

4.ΠΡΩΤΟΚΟΛΛΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Το διαδίκτυο των πραγμάτων καλύπτει μία μεγάλη ποικιλία ενσωματωμένων τεχνολογιών, πόρων, πλατφορμών και συστημάτων νέφους, τα οποία επικοινωνούν και διασυνδέονται μεταξύ τους σε πραγματικό χρόνο. Για το συνδυασμό όλων των ανωτέρω, χρησιμοποιούνται υφιστάμενα και αναπτυσσόμενα πρωτόκολλα επικοινωνίας που επιτρέπουν στις συσκευές και στους διακομιστές, να αλληλεπιδρούν όλο και πιο αποτελεσματικά, με στόχο να ενοποιήσουν το ετερογενές έξυπνο περιβάλλον. Έτσι, το έξυπνο δίκτυο είναι σχεδιασμένο για να ενδυναμώνει την επικοινωνία μεταξύ συσκευών (D2D), ανθρώπων με συσκευές (H2D), ανθρώπων μεταξύ τους (H2H) και συσκευών με ανθρώπους (D2H).

Η διαδρομή του έξυπνου δικτύου από άκρο σε άκρο αποτελείται από τις ενσω ματωμένες συσκευές, τις θύρες και τις εφαρμογές τελικών σημείων. Οι ενσωματωμέν ες συσκευές συνδέονται με την τοπική θύρα, μέσω των πρωτοκόλλων (6LowPan, Zig Bee, Zwave, Thread, Bluetooth, WiFi κλπ). Στη συνέχεια, οι θύρες συνδέονται με το διαδίκτυο χρησιμοποιώντας διάφορες συνδέσεις, όπως ενσύρματη τοπική ή κινητή δικτύωση.

4.1.ΔΟΜΗ ΠΡΩΤΟΚΟΛΛΩΝ

Ακριβώς λόγω της μεγάλης ανομοιομορφίας του έξυπνου δικτύου δεν υπάρχει μία συγκεκριμένη δομή πρωτοκόλλων που χρησιμοποιούνται σε αυτό. Ανάλογα με τον τομέα δραστηριότητας, τις χρήσεις και τις εφαρμογές, τα χαρακτηριστικά και οι ιδιαιτερότητες της δομής των έξυπνων πρωτοκόλλων διαφέρουν, γι αυτό και είναι πολύ δύσκολη η σύγκριση μεταξύ τους (Jonathan Tournier, et al., 2020). Τα πρωτόκολλα που χρησιμοποιεί το έξυπνο δίκτυο κατηγοριοποιούνται στα διάφορα επίπεδα λειτουργίας του έξυπνου δικτύου[6]. Έτσι υπάρχουν τα πρωτόκολλα:

- Υποδομής (π.χ. LowPAN, IPv4/IPv6, RPL)
- Αναγνώρισης (π.χ. EPC, uCode, IPv6, URIs)
- Επικοινωνίας/Μεταφοράς (π.χ.Wifi, Bluetooth, LPWAN)
- Αναζήτησης (π.χ. υλικό δίκτυο, mDNS, DNS-SD)

[6] https://www.postscapes.com/internet-of-things-protocols/#protocols, (πρόσβαση 15/01/2021)

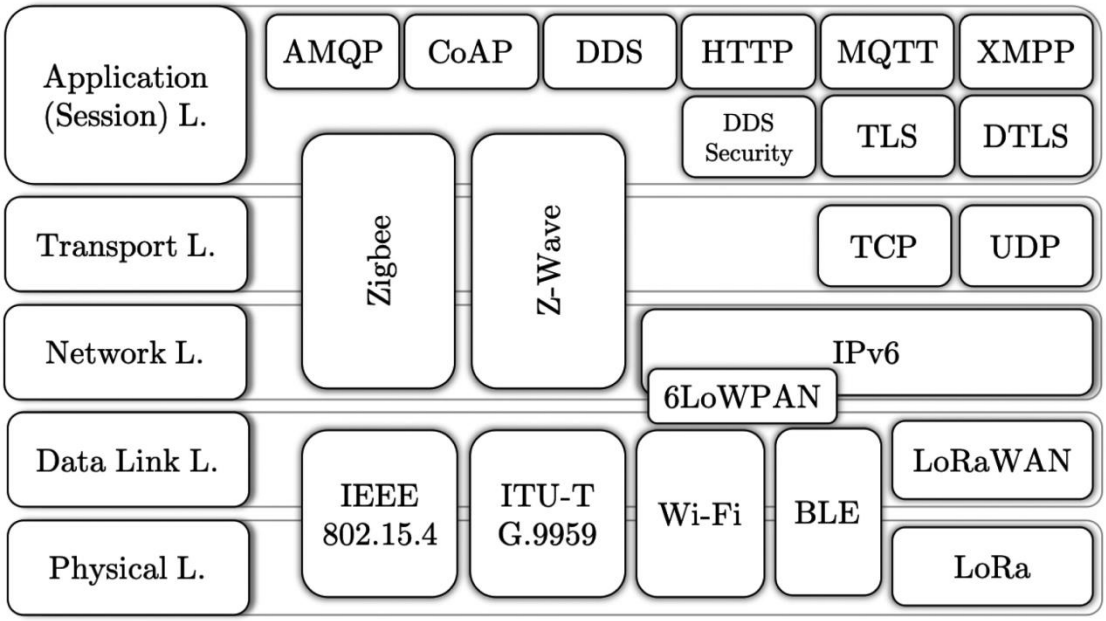
- Πρωτόκολλα δεδομένων (π.χ. MQTT, CoAP, AMQP, Websocket, Κόμβος)
- Διαχείρισης Συσκευής (π.χ. TR-069, OMA-DM)
- Σημασιολογίας (π.χ. JSON-LD, Web Thing Model) και
- Πολυεπίπεδων Συστημάτων (π.χ. Alljoyn, IoTivity,Weave, Homekit).

Οι έξυπνες συσκευές, επικοινωνούν και διασυνδέονται με τη χρήση πρωτοκόλλων επικοινωνίας, τα οποία είναι μέθοδοι επικοινωνίας που παρέχουν εχέγγυα ασφαλείας των δεδομένων που ανταλλάσσονται μεταξύ των διασυνδεδεμένων συσκευών. Στην ασύρματη σύνδεση, χρησιμοποιούνται διάφορες τεχνολογίες και πρωτόκολλα επικοινωνίας που προτυποποιούνται από σχετικούς οργανισμούς (π.χ. IEEE, IETF και W3C).

Από αυτά τα πρωτόκολλα τα πιο εύχρηστα είναι τα Zigbee, Bluetooth και Wi-Fi, ενώ τα πιο γνωστά πρωτόκολλα επικοινωνίας που χρησιμοποιούν οι έξυπνες συσκευές είναι (Sylvia, 2016) (Boris & Thomas, 2017), (Dan Dragomir∗, n.d.): το Bluetooth-BLE**,** το Zigbee, το Z-Wave, το 6LowPAN, το Thread, το Wi-Fi, το NFC, το Sigfox, το IEEE 802.15.4, το LoRaWAN (Long-RangeWAN), τα κυψελοειδή δίκτυα (GSM/ 3G/ 4G/ 5G) και το RFID (radio frequency identification). Τα πρωτόκολλα αυτά χρησιμοποιούνται ανάλογα με τις ανάγκες που θέλει να εξυπηρετήσει το κάθε έξυπνο δίκτυο.

Εκτός των ανωτέρω, πολύ σημαντικά για τη λειτουργία του έξυπνου δικτύου είναι και τα πρωτόκολλα διασύνδεσης (Interaction Protocols), τα οποία είναι αναγκαία για τη διασύνδεση των συσκευών και εφαρμογών (protocol suites). Ορισμένα από τα πιο γνωστά από αυτά είναι (Sylvia, 2016): το MQTT, το CoAP, το XMPP και το WAMP[7].

[7] https://www.postscapes.com/internet-of-things-protocols (πρόσβαση 30/12/2020)



Εικόνα 9: Πρωτόκολλα ανά Επίπεδο του Διαδικτύου των Πραγμάτων(ADRIAN PEKAR, 2020)

4.2.ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Με την συνεχή αύξηση των έξυπνων συσκευών που βασίζονται στο λογισμικό ανοιχτού κώδικα (open source software), δημιουργούνται νέες ανάγκες κατά την επικοινωνία στο έξυπνο δίκτυο και για τον λόγο αυτό τα πρωτόκολλα θα πρέπει να είναι σε θέση να καλύψουν τις νέες προκλήσεις, ήτοι την φορητότητα, την ασφάλεια, τις μεγάλες αποστάσεις και την διακοπτόμενη συνδεσιμότητα. Παρά την πληθώρα των πρωτοκόλλων του έξυπνου διαδικτύου, αυτά μοιράζονται τις ίδιες αφηρημένες αρχές και είναι ευάλωτα στους ίδιους τύπους επιθέσεων, παροτι κάθε είδος επίθεσης απευθύνεται σε συγκεκριμένο πρωτόκολλο κάθε φορά, λαμβάνοντας υπόψη τις ιδιαιτερότητές του.

Όλες οι απειλές ασφαλείας στα πρωτόκολλα του έξυπνου δικτύου πηγάζουν από την αυθεντικοποίηση, εξουσιοδότηση και κρυπτογράφηση πακέτων (Alin ZAMFIROIU, et al., 2020). Από προεπιλογή, τα μηνύματα που μεταφέρονται στο δίκτυο δεν είναι ασφαλή, καθώς αποστέλλονται ως απλά κείμενα. Συγκεκριμένα, οι κοινές επιθέσεις (Jonathan Tournier, et al., 2020) σε όλα τα πρωτόκολλα του έξυπνου δικτύου αφορούν την ασφάλεια των πακέτων δεδομένων, από τα οποία είτε εξάγονται ευαίσθητα δεδομένα (λαθρακοή/eavesdropping) είτε τροποποιούνται τα μεταφερόμενα δεδομένα αλλοιώνοντας όλη τη ροή. Αυτό μπορεί να συμβεί, καθώς πολλά έξυπνα

δίκτυα δεν χρησιμοποιούν κρυπτογράφηση κατά την επικοινωνία και έτσι είναι εύκολο για τον εισβολέα, εξετάζοντας απλώς το ασύρματο δίκτυο να εξάγει τις πληροφορίες που θέλει χωρίς να αναγκαστεί να προβεί σε περίπλοκες υπολογιστικές ενέργειες. Άλλα έξυπνα δίκτυα είναι ευπαθή είτε επειδή χρησιμοποιείται αδύναμη κρυπτογράφηση με παλαιούς αλγόριθμους ή μικρά κλειδιά είτε επειδή χρησιμοποιούνται μη ευέλικτοι (ad hoc) και μη ανταποκρινόμενοι σε όλες τις επιθέσεις αλγόριθμοι κρυπτογράφησης. Σε κάθε περίπτωση ακόμα και ένας δυνατός αλγόριθμος κρυπτογράφησης μπορεί να παραβιαστεί,εάν ο εισβολέας αναγνωρίσει κάποια μοτίβα. Η χρήση πιστοποιητικών δημοσίου κλειδιού από μία αξιόπιστη αρχή πιστοποιητικών, η ενεργοποίηση εξουσιοδότησης κάθε κόμβου και η εξουσιοδοτημένη πρόσβαση στα ευαίσθητα δεδομένα, είναι συνεπώς σημεία κλειδιά για την ασφάλεια.

Όμως, πέραν των κοινών κινδύνων, λόγω της μεγάλης ετερογένειας των πρωτοκόλλων των έξυπνων δικτύων, προκύπτουν ιδιαίτερα ζητήματα ασφαλείας για κάθε πρωτόκολλο ξεχωριστά. Στα περισσότερα πρωτόκολλα επικοικοινωνίας, οι κίνδυνοι σχετίζονται με αδυναμίες του λογισμικού και λανθασμένη διαμόρφωση ρυθμίσεων ασφαλείας, ειδικά των ενδιάμεσων πόρων. Έτσι συνήθως δεν γίνεται σωστή αυθεντικοποίηση, παροχή εξουσιοδότησης, επιβεβαίωση, παράδοση και κρυπτογράφ ηση μηνυμάτων. Γι αυτό τον λόγο οι επιθέσεις που δέχονται αυτά τα πρωτόκολλα σχετίζονται με άρνηση υπηρεσιών (DoS,DDoS) (Giuseppe Nebbione & Maria Carla Calzarossa, 2020).

Εκτός των ανωτέρω, υπάρχει μεγάλη διαφοροποίηση ως προς την παροχή υπηρεσιών ασφαλείας μεταξύ των πρωτοκόλλων. Γενικά τα πρωτόκολλα επικοινωνίας υποστηρίζουν ένα ελάχιστο επίπεδο ασφαλείας καθώς και υπηρεσίες ασφαλείας προς τον χρήστη, με τη χρήση μηχανισμών κρυπτογράφησης. Αντιθέτως, τα πρωτόκολλα αναζήτησης υπηρεσιών δεν διαθέτουν εγγενώς υπηρεσίες ασφαλείας. Γι αυτό και η ενσωμάτωση των κατάλληλων λύσεων ασφαλείας έχει αφεθεί στην ευχέρεια του προγραμματιστή (Giuseppe Nebbione & Maria Carla Calzarossa, 2020). Θα πρέπει να τονιστεί η έλλειψη εχέγγυων ασφαλείας από τον σχεδιασμό των πρωτοκόλλων.Οι υπηρεσίες ασφαλείας θεωρούνται προαιρετικές και πρέπει να ενεργοποιηθούν από τους προγραμματιστές, οι οποίοι όμως τείνουν να τις παραμελούν κατά την ενσωμάτωση και παραμετροποίηση των εφαρμογών. Σε αυτό παίζει ρόλο το γεγονός ότι η κρυπτογράφηση από άκρο σε άκρο είναι κοστοβόρα δεδομένων των περιορισμών των έξυπνων συσκευών και του συστήματος.

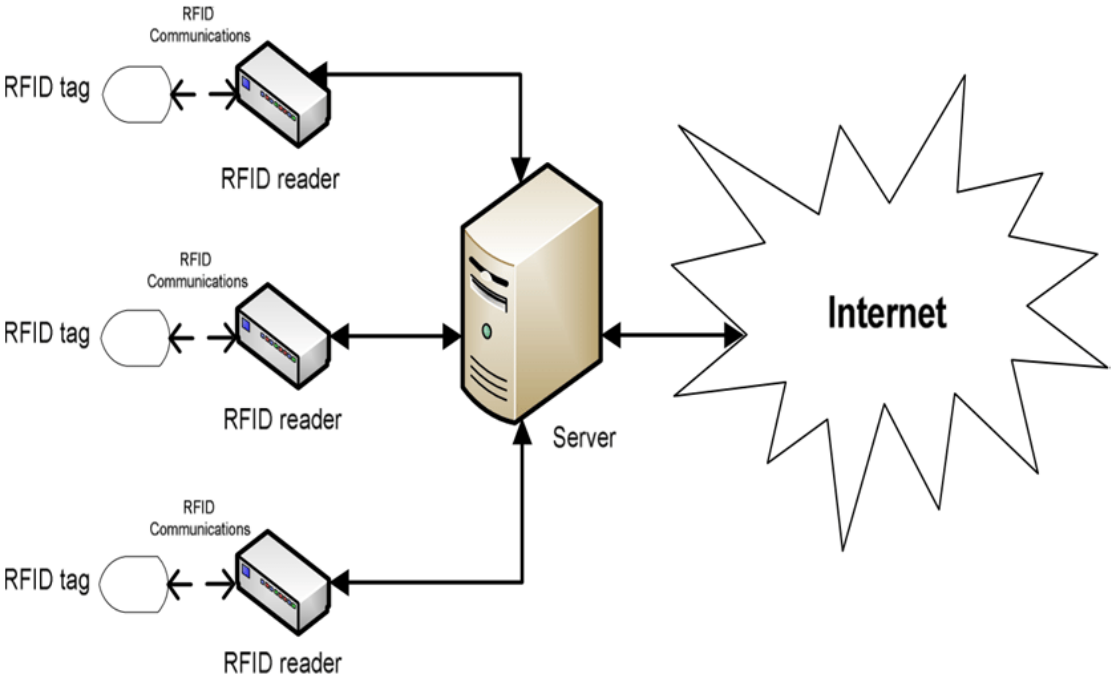
Επίσης, ειδικά κατά την επικοινωνία δεν είναι δυνατόν να εφαρμοστούν παραδοσιακές μέθοδοι ασφαλείας, λόγω της μεγάλης ποικιλίας των συσκευών και μηχανισμών. Επιπλέον, δεν είναι εφικτή η λειτουργία του συστήματος κάτω από ένα ελεγχόμενο τείχος ασφαλείας, καθώς οι εισβολείς μπορεί να αποκτήσουν πρόσβαση στο δίκτυο εμμέσως και με την παραβίαση ενός μόνο κόμβου. Εξάλλου, η ξαφνική ανάγκη αύξησης του ρυθμού μεταφοράς δεδομένων λόγω του τεράστιου όγκου πληροφοριών (από το έξυπνο δίκτυο και τα μέσα κοινωνικής δικτύωσης), κάνει το σύστημα πιο ευπαθές σε άρνηση υπηρεσίας (DoS), ενώ η ασύρματη επικοινωνία μεταξύ των κόμβων επιτρέπει τόσο ενεργητικές όσο και παθητικές επιθέσεις (J. Cynthia, et al., 2019).

Με βάση τα ανωτέρω και συνοψίζοντας, έχει προκύψει ότι οι κίνδυνοι ασφαλείας των πρωτοκόλλων του έξυπνου δικτύου οφείλονται αρχικά τόσο στη μεγάλη ετερογένεια των πρωτοκόλλων που δεν καθιστά εύκολη τη δημιουργία κοινών αρχών ασφαλείας, όσο και στο γεγονός ότι το διαδίκτυο των πραγμάτων είναι σχετικά καινούργιο και έχει ως αποτέλεσμα τα βασικά του πρωτόκολλα λειτουργίας να είναι συνεχώς εξελισσσόμενα. Άλλωστε, εκ κατασκευής πολλές συσκευές δεν μπορούν να αναβαθμιστούν ή όσες από αυτές μπορούν, παρέχονται από τις κατασκευάστριες εταιρίες περιορισμένες αναβαθμίσεις ασφαλείας. Εκτός των ανωτέρω, οι επιταγές της αγοράς, η οποία προκρίνει το κέρδος από την ασφάλεια, δεν επιτρέπουν την απόσυρση των παλαιάς τεχνολογίας πόρων και τεχνολογιών και η προσπάθεια συμβατότητάς τους με νέους και πιο εξελιγμένους πόρους δημιουργεί μεγάλους περιορισμούς ασφαλείας. Τέλος, ενώ κάποιες συσκευές μπορεί να είναι εκ κατασκευής ασφαλείς, εντάσσονται σε έξυπνα περιβάλλοντα με άλλες μη ασφαλείς συσκευές και λόγω της αναγκαίας αλληλεπίδρασης τους δημιουργούνται κίνδυνοι ασφαλείας.

4.3.ΕΙΔΙΚΑ Η ΤΕΧΝΟΛΟΓΙΑ ΤΑΥΤΟΠΟΙΗΣΗΣ ΜΕΣΩ ΡΑΔΙΟΣΥΧΝΟΤΗΤΩΝ (RFID) ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Μία πολύ σημαντική τεχνολογία που προτιμάται στο διαδίκτυο των πραγμάτων, για λόγους οικονομίας και ενέργειας, είναι η ταυτοποίηση μέσω ραδιοσυχνοτήτων (RFID), η οποία αποτελείται από ετικέτες και ηλεκτρονικούς αναγνώστες. Οι ετικέτες είτε είναι ενσωματωμένες στις έξυπνες συσκευές είτε επισυνάπτονται σε αυτές και διακρίνονται σε ενεργητικές και παθητικές. Πρόκειται για μία αυτόματη, ανέπαφη τεχνολογία αναγνώρισης η οποία μπορεί να αναγνωρίσει το σήμα της στοχευμένης ετικέτας με

στόχο την απόκτηση δεδομένων, χωρίς χειροκίνητες παρεμβάσεις (Qi Jing, et al., 2014).



Εικόνα 10: Χρήση Τεχνολογίας RFID στο Διαδίκτυο των Πραγμάτων *(Shamsi, et al., 2018)*

4.3.1. ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΜΕΣΩ ΡΑΔΙΟΣΥΧΝΟΤΗΤΩΝ (RFID)

Τα ζητήματα ασφαλείας που σχετίζονται με την τεχνολογία ταυτοποίησης μέσω ραδιοσυχνοτήτων (RFID), είναι καταρχήν ο περιορισμένος αποθηκευτικός χώρος και οι περιορισμένες υπολογιστικές ικανότητες που διαθέτουν οι ετικέτες, με αποτέλεσμα να μην μπορούν να ενσωματωθούν σε αυτές γνωστά και δοκιμασμένα πρωτόκολλα ασφαλείας. Γι αυτό τον λόγο πρέπει να χρησιμοποιούνται διαφορετικά και ελαφριά πρωτόκολλα ασφαλείας, ανάλογα με τον σκοπό για τον οποίο πρόκειται να χρησιμοποιηθεί κάθε φορά η εν λόγω τεχνολογία. Επιπλέον, δεν έχει καθιερωθεί ένα ενιαίο, διεθνές πρότυπο κωδικοποίησης χαρακτήρων για τις ετικέτες, με αποτέλεσμα πολλές φορές ο αναγνώστης (reader) να μην μπορεί να αποκτήσει πρόσβαση στις πληροφορίες της ετικέτας ή να υπάρχουν σφάλματα κατά τη διαδικασία ανάγνωσης. Ένα άλλο πρόβλημα που μπορεί να δημιουργηθεί είναι όταν πολλές ετικέτες μεταδίδουν ταυτόχρονα πληροφορίες δεδομένων στον αναγνώστη, με αποτέλεσμα αυτός να μην μπορεί να λάβει σωστά τα δεδομένα (Qi Jing, et al., 2014). Τέλος, οι

ταυτότητες (ID) των ετικετών, μπορούν να χρησιμοποιηθούν από εισβολείς για τον εντοπισμό της τοποθεσίας του χρήση.

4.3.2. ΕΠΙΘΕΣΕΙΣ ΚΑΤΑ ΤΩΝ ΕΤΙΚΕΤΩΝ

Οι πιο συνήθεις επιθέσεις κατά των ετικετών (Den ver BraganRAGANza & B. Tulasi, 2017) είναι οι επιθέσεις παρεμβολών ή παρακώλυσης επικοινωνιών (jamming), που σκόπιμα ή μη προκαλούνται μεταξύ του αναγνώστη και της ετικέτας, με αποτέλεσμα να εμποδίζεται η επικοινωνία μεταξύ τους. Άλλες πρόσφορες επιθέσεις είναι η Λαθρακρόαση (Eavesdropping), με την οποία ο εισβολέας χρησιμοποιεί έναν ψεύτικο αναγνώστη μεταξύ του γνήσιου και της ετικέτας, με αποτέλεσμα να υποκλέπτει πληροφορίες και η επίθεση επανάληψης (Replay Attack) με την οποία ο εισβολέας αποκτά πρόσβαση στις πληροφορίες ενός συστήματος ταυτοποίησης μέσω ραδιοσυχνοτήτων (RFID) και αντιγράφει τα δεδομένα παριστάνοντας τον γνήσιο αναγνώστη ή ετικέτα. Επιπλέον, με την επίθεση απενεργοποίησης (Deactivation), το σύστημα καθίσταται άχρηστο, καθώς ο εισβολέας αποστέλλει μη ισχύουσες εντολές στην ετικέτα και έτσι ο αναγνώστης δεν μπορεί να την αναγνωρίσει. Με την επίθεση αποεπισύναψης της ετικέτας ο εισβολέας αντικαθιστά το επισυναπτόμενο αντικείμενο με άλλο, παριστάνοντας στον αναγνώστη ότι είναι το γνήσιο. Με την επίθεση πλαστογράφησης (spoofing), ο εισβολέας ουσιαστικά αντιγράφει τις ετικέτες, με στόχο να τροποποιηθούν τα δεδομένα τα οποία δεν έχουν επικυρωθεί από τον αναγνώστη. Με την επίθεση του παρεμβαλλόμενου (Man in the middle), κατά τη μετάδοση των πληροφοριών παρεμβάλλεται ένας ψεύτικος αναγνώστης μεταξύ του γνήσιου και της ετικέτας, με αποτέλεσμα να χειραγωγούνται τα δεδομένα μεταξύ τους. Τέλος, με την επίθεση κλωνοποίησης (cloning) ο εισβολέας αντιγράφει τα δεδομένα σε μία νέα ετικέτα την οποία κατέχει ο ίδιος.

4.4. ΣΥΓΧΡΟΝΑ ΠΡΩΤΟΚΟΛΛΑ ΓΙΑ ΑΣΦΑΛΕΙΑ ΣΤΟ ΕΞΥΠΝΟ ΔΙΚΤΥΟ

Η ασφάλεια αφορά όλα τα επίπεδα του έξυπνου δικτύου. Τα γνωστά πρωτόκολλα επικοινωνίας προσφέρουν μερική μόνο ασφάλεια. Τα έξυπνα πρωτόκολλα έχουν να αντιμετωπίσουν από τη μία πλευρά παραβιάσεις ασφαλείας των πλατφορμών των παρόχων νέφους και από την άλλη πλευρά ζητήματα ιδιωτικότητας δεδομένων, αυθεντικοποίησης, εξουσιοδότησης και σωστής διαχείρισης σε ένα διάχυτο ετερογενές

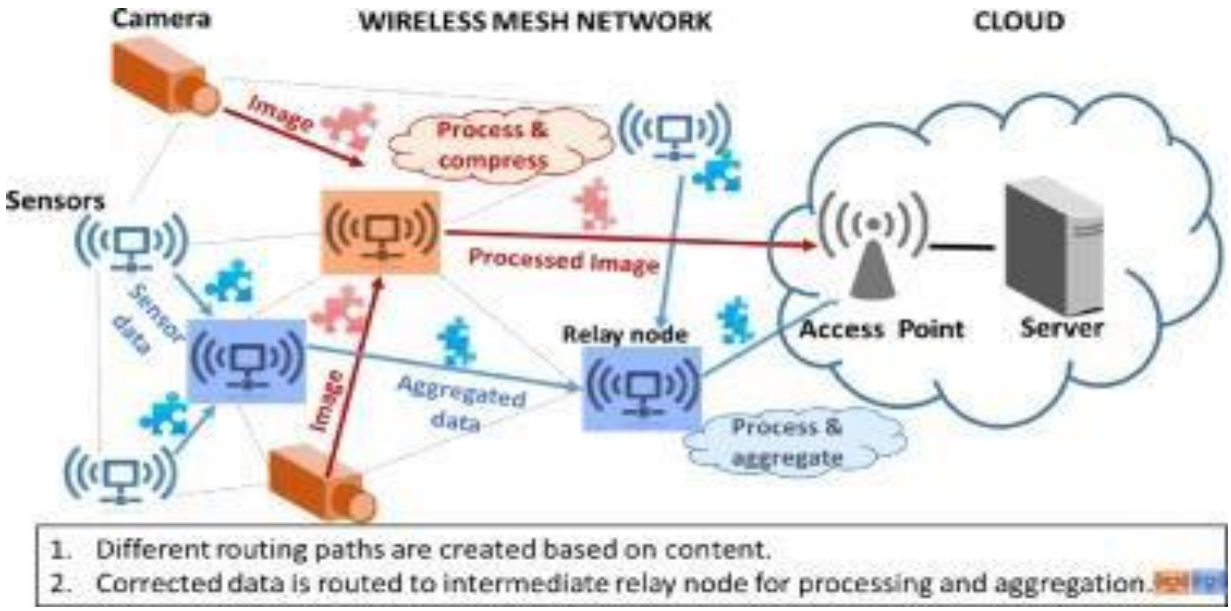
περιβάλλον. Γι αυτό είναι σημαντική η εφαρμογή πρωτοκόλλων ασφαλείας σε όλα τα επίπεδα του έξυπνου δικτύου.

Έτσι, έχουν αναπτυχθεί νέα πρότυπα με ελαφρά σχέδια ασφαλείας τα οποία ενδεικτικά είναι (Gilchrist, 2017),(Tara Salman, 2017): τα TLS/DTLS, τα οποία χρησιμοποιούνται στο επίπεδο μεταφοράς και εξασφαλίζουν αυθεντικοποίηση, ακεραιότητα και απορρητο. Το MAC 802.15.4e που παρέχει ασφάλεια δεδομένων, το OAuth 2.0, το οποίο επιτρέπει στους διακομιστές τρίτων μερών να ελέγχουν τα δικαιώματα πρόσβασης και άδειες στις πηγές. Το WirelessHART χρησιμοποιεί πρόσφατες τεχνικές κρυπτογράφησης, αυθεντικοποίησης κλπ. Το RPL που προσφέρει ασφάλεια της πληροφορίας και τα TCG, SASL, ACE.

5. ΔΡΟΜΟΛΟΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (IoT routing)*(Saleem, 2016)*

Η δρομολόγηση (Routing) (Boris & Thomas, 2017) είναι μία βασική υπηρεσία στο διαδίκτυο των πραγμάτων, καθώς επιτρέπει την ανταλλαγή πληροφοριών μεταξύ των αντικειμένων, κατευθύνοντας αποτελεσματικά και διαμοιράζοντας αξιόπιστα τα δεδομένα στο δίκτυο, από τις πηγές στους προορισμούς τους μέσω ενδιάμεσων κόμβων (που λέγονται δρομολογητές).

Η διαδικασία της δρομολόγησης κατευθύνει τα δεδομένα προωθώντας τα με βάση πίνακες δρομολόγησης που βρίσκονται στους δρομολογητές, οι οποίοι αποθηκεύουν μια εγγραφή για την καλύτερη διαδρομή προς διάφορες κατευθύνσεις στο δίκτυο. Κατά συνέπεια, η κατασκευή των πινάκων δρομολόγησης είναι πολύ σημαντική για την αποτελεσματική δρομολόγηση, γιατί εκτός των άλλων, η διαδρομή που ακολουθούν τα δεδομένα από την πηγή στον προορισμό, επιδρά και στην κατανάλωση ενέργειας των ενδιάμεσων κόμβων (Sriram Sankaran, 2015).



Εικόνα 11: Δρομολόγηση στο Διαδίκτυο των Πραγμάτων (Yichao Jin, et al., 2016)

5.1. ΠΡΩΤΟΚΟΛΛΑ ΔΡΟΜΟΛΟΓΗΣΗΣ

Τα πρωτόκολλα δρομολόγησης (Tara Salman, 2017) είναι πολύ σημαντικά στο διαδίκτυο των πραγμάτων, καθώς καθορίζουν τη μεταφορά των πακέτων από την πηγή στον προορισμό, αντιμετωπίζουν τους περιορισμούς του έξυπνου συστήματος, καθορίζουν την ταχύτητα μετάδοσης των πακέτων δεδομένων, εξοικονομούν ενέργεια και μνήμη και ανταποκρίνονται στις συνεχείς αλλαγές τοποθεσίας που χαρακτηρίζει το έξυπνο δίκτυο. Τα πιο γνωστά πρωτόκολλα δρομολόγησης είναι το RPL, το CORPL και το CARP.

Υπάρχουν πολλοί παράγοντες που επηρεάζουν τη δρομολόγηση,οι οποίοι είναι:

α. Περιορισμένοι Πόροι: Ένα σοβαρό πρόβλημα είναι η ύπαρξη περιορισμών των έξυπνων πόρων και πηγών, όπως είναι η τροφοδοσία ενέργειας, οι δυνατότητες μνήμης, οι επιλογές ασύρματης επικοινωνίας κ.λ.π.

β. Δυναμική Τοπολογία Δρομολόγησης: Δηλαδή η σχεδόν αυτόνομη λειτουργία του δικτύου με σκοπό να αποφεύγει βλάβες και μπλοκαρίσματα. Οι αιτίες της δυναμικότητας της τοπολογίας είναι πολλές, μεταξύ των οποίων οι ενεργειακοί περιορισμοί των συσκευών, η φορητότητα των έξυπνων συσκευών, η σύνδεση/αποσύνδεση τους κατά βούληση, οι συχνές δυσλειτουργίες των κόμβων, η αναξιοπιστία των ασύρματων συνδέσεων.

γ. Κλιμάκωση (Scalability): Σχετίζεται με τον μεγάλο αριθμό κόμβων αλλά και με τη γεωγραφική έκταση που μπορεί αυτοί να καλύπτουν, η οποία δυσκολεύει τη

δρομολόγηση, καθώς την καθιστά πιο περίπλοκη και κοστοβόρα, δεδομένου οτι πρέπει παράλληλα να διατηρηθεί η λειτουργικότητα του συστήματος.

δ. Αποσυνδέσεις(partitions) και κενά(voids) του δικτυου: Ένα άλλο μεγάλο πρόβλημα είναι οι αποσυνδέσεις (partitions) κόμβων κατά τέτοιο τρόπο ώστε να μην μπορούν να ανταλλάζουν δεδομένα με τους άλλους κόμβους καθώς και τα τμήματα εκείνα που δεν καλύπτονται από το δίκτυο (voids).

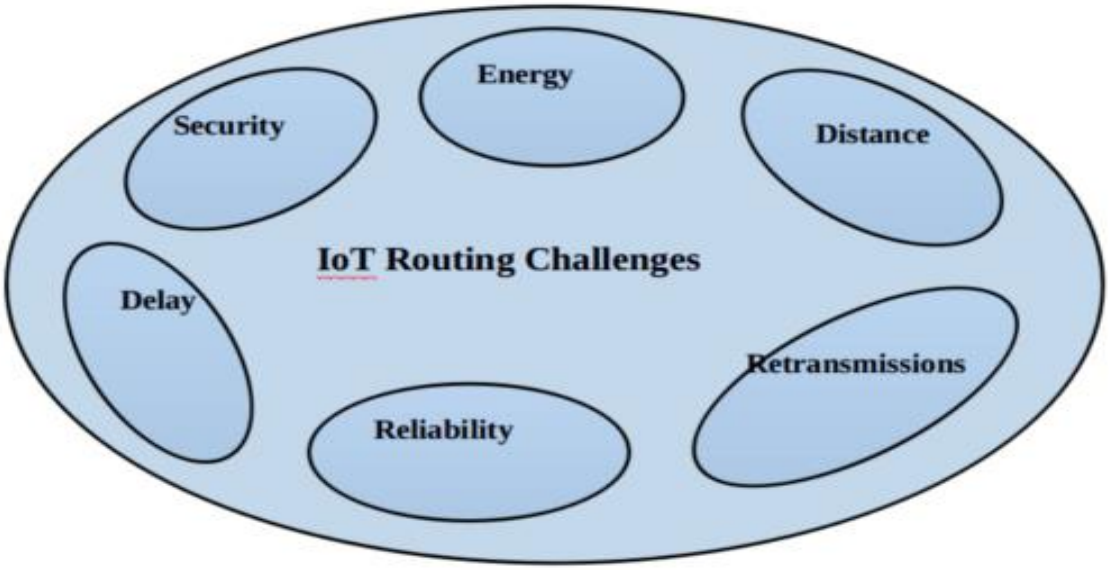
5.2. ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΟΥΣ ΔΡΟΜΟΛΟΓΗΣΗΣ

Κάθε συσκευή που συνδέεται στο διαδίκτυο είναι πολύ εύκολο να δεχτεί επίθεση. Γι αυτό, τα πρωτόκολλα δρομολόγησης και οι διάφοροι μηχανισμοί του δικτύου πρέπει να διασφαλίζουν ότι τα δεδομένα είναι ασφαλή και ότι οι κόμβοι δεν έχουν υποστεί επίθεση. Όσο πιο πολλές συσκευές συνδέονται στο έξυπνο δίκτυο τόσο πιο πολύ αυξάνεται η κίνηση δεδομένων στο δίκτυο. Αυτό μπορεί να οδηγήσει αφενός στην αποστολή πακέτων δεδομένων σε λάθος προορισμούς και αφετέρου σε μη εξουσιοδοτημένη πρόσβαση στο δίκτυο, εάν δεν εφαρμοστούν σωστά πρωτόκολλα παροχής εξουσιοδότησης.

Οι κόμβοι είναι ευάλωτοι σε επιθέσεις, γεγονός που οφείλεται σε υλικές αδυναμίες τους, σε κοινή χρήση ασύρματων συνδέσεων και σε εφαρμογές μάχης (battlefield applications). Η διασφάλιση της ασφαλούς σύνδεσης μεταξύ των κόμβων του δικτύου συνήθως επιτυγχάνεται με τη χρήση πρωτοκόλλων ασφαλείας που έχουν ως βάση την εμπιστοσύνη και τα οποία χρησιμοποιούν αλγορίθμους που κατηγοριοποιούν τους κόμβους σε έμπιστους ή μη. Εάν ένας κόμβος χαρακτηριστεί έμπιστος, καταγράφεται σε λίστα και θεωρείται πλέον ασφαλής.

Υπάρχουν διαφόρων ειδών επιθέσεις κατά των πρωτοκόλλων δρομολόγησης, (Rhitabrat Pokharel, et al., 2018), όπως η επίθεση τροποποίησης συμπεριφοράς (modification attack), η οποία σχετίζεται με επίθεση στον σταθμό μεταφοράς των δεδομένων (δρομολογητές και τροποποιητές), όπου τα δεδομένα τροποποιούνται και μεταφέρονται σε επόμενους κόμβους. Στην επίθεση εντός και εκτός (on-off attack), ο κακόβουλος κόμβος επιλεκτικά λειτουργεί ως καλός ή κακός, καθώς ο επιτιθέμενος θέλει να διασφαλίσει ότι ο κακόβουλος κόμβος δεν θα ανιχνευθεί. Η επίθεση κακού στόματος (bad mouth attack) αποστέλλει ψευδείς πληροφορίες σχετικά με κόμβο προορισμού για να μειώσει την αξιοπιστία του. Στην επίθεση συνωμοσίας (collusion attack), πολλοί κόμβοι σχηματίζουν μία ομάδα με σκοπό να αυξήσουν την αξιοπιστία

τους, έτσι ώστε να μην ανιχνεύονται ως κακόβουλοι. Τέλος, στην επίθεση λογισμικής και υλισμικής ευπάθειας, το υλικό και λογισμικό είναι υπεύθυνα για την αδυναμία εφαρμογής μεθόδων κρυπτογράφησης δεδομένων.



Εικόνα 12: Κίνδυνοι Ασφαλείας Δρομολόγησης [8]

5.3. ΕΠΙΤΕΥΞΗ ΑΣΦΑΛΟΥΣ ΔΡΟΜΟΛΟΓΗΣΗΣ

Υπάρχουν διάφορες λύσεις για την επίτευξη ασφαλούς δρομολόγησης. Αυτές είναι (Sufian Hameed, et al., 2019)**:**

α. Ένα από τα μεγαλύτερα κλειδιά για την επίτευξη ασφαλούς δρομολόγησης είναι η εφαρμογή ενός ασφαλούς πρωτοκόλλου δρομολόγησης για τη μεταφορά των δεδομένων στο έξυπνο δίκτυο. Ένα τέτοιο πρωτόκολλο θα πρέπει να είναι σε θέση αφενός να ανευρίσκει μία ασφαλή διαδρομή και αφετέρου να ασφαλίζει τη διαδρομή μεταξύ των επικοινωνούντων κόμβων.

β. Μία άλλη μεγάλη πρόκληση είναι ο γρήγορος εντοπισμός των κακόβουλων κόμβων και η απομόνωσή τους, με την ανάπτυξη των κατάλληλων πρωτοκόλλων και τεχνικών.

[8] https://slogix.in/iot-blog/what-are-the-pitfalls-in-the-design-of-iot-routing-protocols/index.html,πρόσβαση 15/02/2021

γ. Επίσης, είναι πολύ σημαντική η αυτοσταθεροποίηση του πρωτοκόλλου, δηλαδή η ικανότητά του να επανέρχεται αυτομάτως μετά από προβλήματα κατά τη λειτουργία του χωρίς ανθρώπινη παρέμβαση.

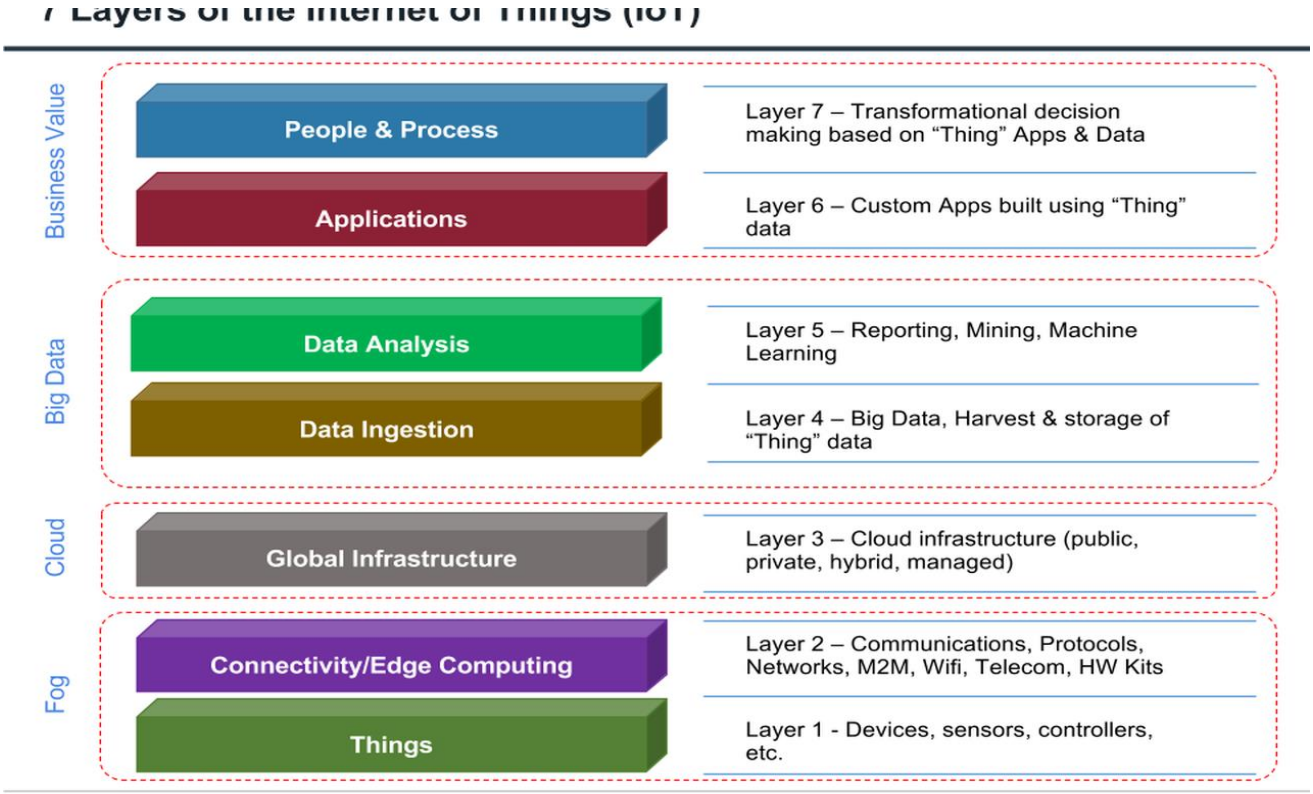
δ. Τέλος, ένα ασφαλές πρωτόκολλο δρομολόγησης θα πρέπει να μπορεί να διατηρεί την ιδιωτικότητα της τοποθεσίας των συσκευών που είναι σημαντική για την αποτροπή κακόβουλων επιθέσεων.

6. ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Έχει επιχειρηθεί να δοθούν πολλοί ορισμοί για την έξυπνη πόλη, ωστόσο δεν υπάρχει ένας ενιαίος ορισμός (Vito Albino, 2015), καθώς οι κυβερνήσεις κάθε χώρας αποφασίζουν μόνες τους ανάλογα και με τα τεχνολογικά και οικονομικά μέσα που διαθέτουν, πόσο θα προχωρήσουν στην υλοποίηση της. Πρόκειται στην ουσία για μια πόλη που χρησιμοποιώντας την τεχνολογία πληροφοριών και επικοινωνιών (ΤΠΕ), διάφορες υλικές συσκευές συνδεδεμένες στο έξυπνο δίκτυο και αισθητήρες, συλλέγει συνεχώς σε πραγματικό χρόνο, δεδομένα από πολίτες, συσκευές, κτίρια κ.λ.π. Εν συνεχεία, τα συλλεχθέντα δεδομένα υπόκεινται σε επεξεργασία και χρησιμοποιούνται για την αποτελεσματική διαχείριση των υπηρεσιών και λειτουργιών της πόλης, όπως τα συστήματα μεταφοράς, ενέργειας, βιβλιοθήκες κλπ. Με αυτόν τον τρόπο υπάρχει μία διαρκής βελτίωση των παρεχόμενων υπηρεσιών και του τρόπου ζωής, καθώς υπάρχει δυνατότητα των αρχών να ενημερώνονται σε ζωντανό χρόνο για τα προβλήματα της καθημερινότητας των πολιτών και να προβαίνουν διαρκώς σε αλλαγές.

Το οικοσύστημα της έξυπνης πόλης, αποτελείται άλλοτε από τρία, άλλοτε από πέντε και άλλοτε από επτά επίπεδα. Σύμφωνα με το μοντέλο των επτά επιπέδων (Tara Salman, 2017), η έξυπνη πόλη στη βάση της αποτελείται από διάφορες έξυπνες εφαρμογές όπως έξυπνη πόλη, έξυπνη ενέργεια κλπ. Στο δεύτερο επίπεδο βρίσκονται οι αισθητήρες και οι έξυπνες συσκευές (αισθητήρες θερμοκρασίας, υγρασίας, κάμερες κ.λ.π). Στο τρίτο επίπεδο γίνεται η διασύνδεση των αισθητήρων με ένα κέντρο δεδομένων ή νέφος, στο τέταρτο επίπεδο εκτελείται η ενσωμάτωση και ο συνδυασμός των δεδομένων, στο πέμπτο επίπεδο βρίσκεται η αναλυτική, δηλαδή ο έλεγχος των δεδομένων με τη χρήση διάφορων τεχνικών (εξόρυξη δεδομένων, μηχανική μάθηση κλ.π). Στο έκτο επίπεδο βρίσκεται το λογισμικό που είναι αναγκαίο για τη λειτουργία των εφαρμογών και τέλος το τελευταίο επίπεδο αποτελείται από υπηρεσίες που

λειτουργούν με τη χρήση όλης αυτής της τεχνολογίας, όπως διαχείριση ενέργειας, υγείας, εκπαίδευση κ.λ.π. Η ασφάλεια και η διαχείριση απαιτούνται για κάθε ένα από τα επτά επίπεδα/στρώματα καθώς αυτά αλληλεξαρτώνται .

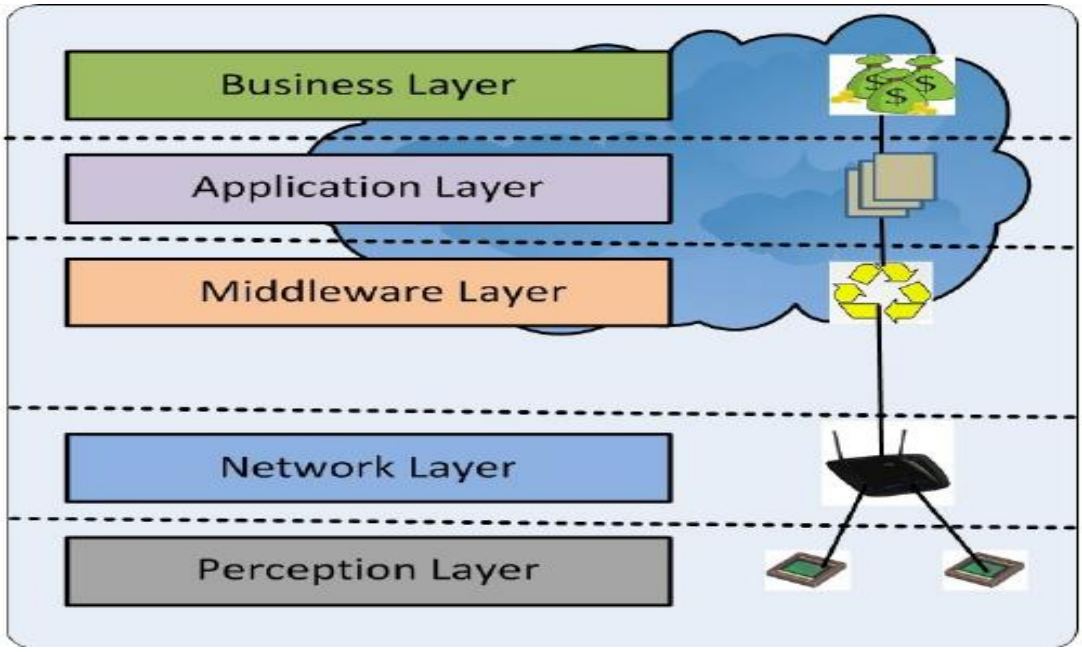


Εικόνα 13: Τα επτά επίπεδα του συστήματος των έξυπνων πόλεων [9]

6.1. ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Οι εφαρμογές της έξυπνης πόλης στηρίζονται στη συλλογή δεδομένων από αισθητήρες, που συλλέγουν διαρκώς δεδοδομένα. Στη συνέχεια, αυτά τα δεδομένα μεταφέρονται στο νέφος μέσω του επιπέδου ενσωμάτωσης, το οποίο διαχειρίζεται την ετερογένεια των αισθητήρων, συσκευών και δικτύων. Γι αυτό τον λόγο η αρχιτεκτονική της έξυπνης πόλης αποτελείται από τα επίπεδα Συλλογής, Ενσωμάτωσης, Νέφους, Εφαρμογής και Επιχειρηματικότητας, ενώ η ασφάλεια και διαχείριση απαιτούνται σε όλα τα στρώματα (Anna Triantafyllou, 2018),(Afzaal, 2019). Συγκεκριμένα:

[9] https://www.quora.com/What-are-the-different-layers-of-IoT-model, (πρόσβαση 15/01/2021)



Εικόνα 14: Επίπεδα Έξυπνης Πόλης*(Mohammad Aazam, et al., 2014)*

α. Επίπεδο Συλλογής (perception layer): Το επίπεδο αυτό αποτελείται από το σύνολο των αισθητήρων και έχει ως κύριο στόχο την συναίσθηση του περιβάλλοντος και την αναγνώριση αντικειμένων/πραγμάτων για τη συλλογή δεδομένων. Το επίπεδο αυτό αποτελείται από δύο μέρη, ήτοι τους κόμβους συλλογής (αισθητήρες, ελεγκτές κλπ) και το δίκτυο συλλογής το οποίο επικοινωνεί με ένα δίκτυο μεταφοράς. Οι κόμβοι χρησιμοποιούνται για τη συλλογή και έλεγχο των δεδομένων ενώ το δίκτυο στέλνει τα συλλεχθέντα δεδομένα σε μία θύρα ή στέλνει οδηγίες ελέγχου στον ελεγκτή. Σε αυτό το επίπεδο χρησιμοποιούνται διάφορες τεχνολογίες (RFID, WSN, RSN, GPS κλπ).

β. Επίπεδο ενσωμάτωσης (Integration Layer): Σε αυτό το επίπεδο συγκεντρώνονται όλα τα προηγουμένως συλλεχθέντα δεδομένα με σκοπό την αφομοίωση όλων των ετερογενών μηχανισμών, δικτύων και συσκευών με το νέφος. Σε αυτό το επίπεδο γίνεται η συλλογή των μεταδιδόμενων πληροφοριών και η αποθήκευσή τους. Εδώ υπάρχει το δίκτυο πρόσβασης (access network), που παρέχει ένα συνεχές περιβάλλον πρόσβασης στο επίπεδο συλλογής και περιλαμβάνει ασύρματα δίκτυα (WiFi), αποκεντρωμένα ασύρματα δίκτυα (ad hoc) κ.λ.π., το βασικό δίκτυο (core network) το οποίο είναι υπεύθυνο για τη μεταφορά των δεδομένων και το τοπικό δίκτυο (Local Area).

γ. Επίπεδο Νέφους (Cloud Layer): Σε αυτό το επίπεδο γίνονται κυρίως εργασίες όπως αποθήκευση, υπολογισμός και ανάλυση των συλλεχθέντων δεδομένων.

Εδώ μεταφέρονται τα δεδομένα που αποκτώνται από τα προηγούμενα στρώματα και αποθηκεύονται έτσι ώστε να χρησιμοποιηθούν από τις εφαρμογές της Έξυπνης πόλης. Για τη διαχείριση όλου αυτού του μεγάλου όγκου πληροφοριών χρησιμοποιούνται οι τεχνολογίες των δεδομένων μεγάλης κλίμακας.

δ. Επίπεδο Εφαρμογών (Application layer): Αυτό το επίπεδο υποστηρίζει όλες τις εφαρμογές της έξυπνης πόλης με τη χρήση του κατάλληλου για τη λειτουργία τους λογισμικού και υλοποιεί την έξυπνη υπολογιστική και την κατανομή πόρων με τον έλεγχο, διαλογή, παραγωγή και επεξεργασία δεδομένων. Αυτό το επίπεδο έχει την ικανότητα να αναγνωρίζει αξιόπιστα, ανεπιθύμητα, ακόμα και κακόβουλα δεδομένα και να τα φλιτράρει.

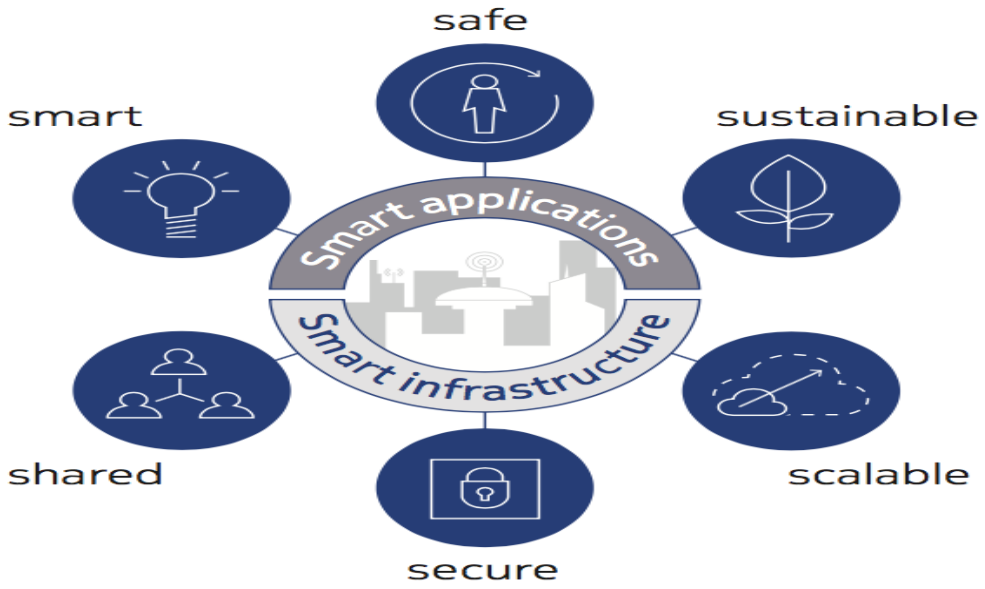
ε. Επίπεδο Επιχειρηματικότητας (Business layer): Σε αυτό το επίπεδο, δίνεται η δυνατότητα να δημιουργούνται συνεχώς διάφορα επιχειρηματικά μοντέλα για την αξιοποίηση των υπηρεσιών της έξυπνης πόλης, με τη χρήση των διαρκώς συλλεχθέντων δεδομένων.

Θα πρέπει να σημειωθεί ότι πολύ σημαντικό ρόλο παίζει και το λεγόμενο **ενδιάμεσο λογισμικό (Middleware),** δηλαδή το επίπεδο εκείνο που βασίζεται κυρίως σε υπηρεσίες λογισμικού, οι οποίες συνδέουν όλα τα μέρη μεταξύ τους. Αυτό το επίπεδο ενσωματώνει τη ροή των δεδομένων ενώ τα καταγράφει, τα επεξεργάζεται και διαχειρίζεται τα ψηφιακά αιτήματα από άλλες υπηρεσίες ή από τον τελικό χρήστη (Alin ZAMFIROIU, et al., 2020).

6.2. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ ΕΞΥΠΝΩΝ ΠΟΛΕΩΝ

Η έξυπνη πόλη διαθέτει πολλά ιδιαίτερα χαρακτηριστικά (Youyang Qu, 2017) όπως είναι αρχικά η ετερογένεια, δηλαδή η ύπαρξη μεγάλου αριθμού και ποικιλίας χρηστών, συσκευών, δικτύων, τεχνολογιών και πρωτοκόλλων. Μία ακόμα ιδιαιτερότητα των έξυπνων πόλεων είναι το γεγονός ότι οι έξυπνες συσκευές και δίκτυα που χρησιμοποιούνται σε αυτές έχουν πολλούς περιορισμούς και χαρακτηρίζονται από περιορισμένη μνήμη, διάρκεια μπαταρίας και ικανότητες επεξεργασίας αλλά και αρκετούς περιορισμούς διασύνδεσης δικτύου. Ακόμα, συναντάται η κινητικότητα, δηλαδή η εύκολη μεταφορά πληροφοριών, δεδομένων και αγαθών μέσα στην πόλη αλλά και η ανοιχτή επικοινωνία και παρακολούθηση σε πραγματικό χρόνο. Ένα άλλο χαρακτηριστικό της έξυπνης πόλης, είναι η συνδεσιμοτητα, δηλαδή η ικανότητα σύνδεσης οποιασδήποτε συσκευής και η κλιμάκωση (scalability), η οποία σχετίζεται

με την ικανότητα διαχείρισης και επεξεργασίας των διαρκώς αυξανόμενων δεδομένων και διακινούμενων μηνυμάτων. Τέλος, ένα άλλο χαρακτηριστικό των έξυπνων πόλεων είναι η διαρκής αλληλεπίδραση των συσκευών με τον άνθρωπο και η χρήση πολλών εφαρμογών απευθείας από τον τελικό χρήστη.

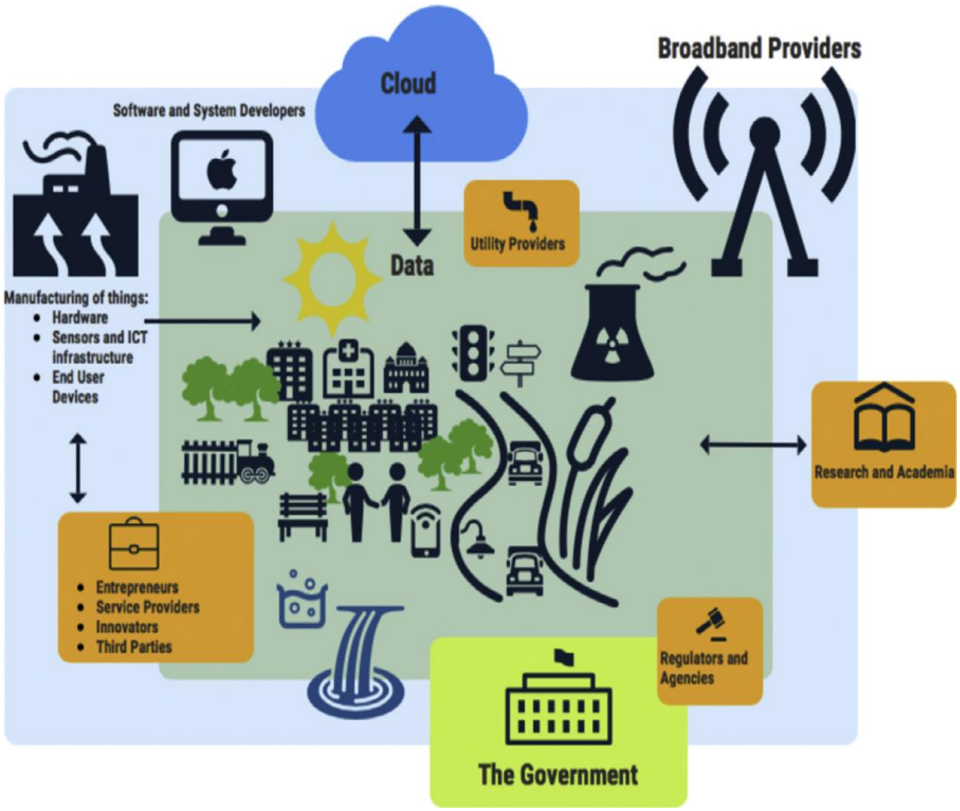


Εικόνα 15: Χαρακτηριστικά των έξυπνων πόλεων [10]

6.3. ΕΦΑΡΜΟΓΕΣ ΕΞΥΠΝΗΣ ΠΟΛΗΣ

Οι εφαρμογές της έξυπνης πόλης είναι (Anna Triantafyllou, 2018): Η έξυπνη Κινητικότητα και ο έξυπνος τουρισμός, η Δημόσια Ασφάλεια και η περιβαλλοντική παρακολούθηση, το Έξυπνο Σπίτι, το Έξυπνο Δίκτυο, η Έξυπνη Επιχειρηματικότητα, η Έξυπνη Γεωργία, τα Logistics και η διαχείριση χρόνου ζωής των προϊόντων, η Έξυπνη Υγεία και ο Έξυπνος-ανεξάρτητος τρόπος ζωής. Δεδομένης της ευρείας χρήσης του διαδικτύου των πραγμάτων στην καθημερινότητα του πολίτη της έξυπνης πόλης, είναι μεγάλο στοίχημα η ισοστάθμιση της ευχρηστότητας των υπηρεσιών από τους πολίτες έναντι της ασφάλειας, της ιδιωτικότητας και της προστασίας των ευαίσθητων προσωπικών δεδομένων.

[10] https://cities-today.com/industry/six-ss-for-smart-city-successes/ (πρόσβαση 15/01/2021)



Εικόνα 16: Το οικοσύστημα της Έξυπνης Πόλης (Morta Vitunskaite, 2019)

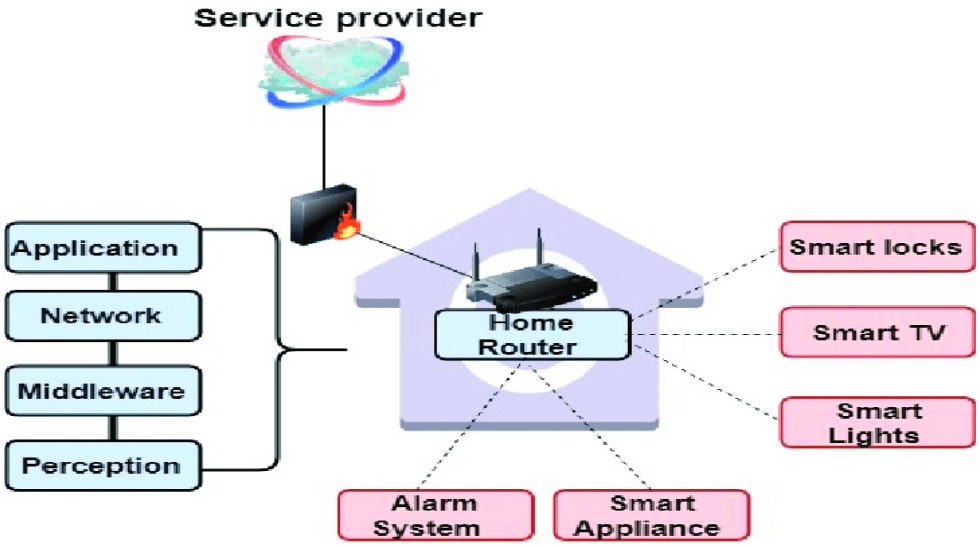
6.3.1. ΕΞΥΠΝΟ ΣΠΙΤΙ

Το έξυπνο σπίτι ή οικιακός αυτοματισμός είναι ένας οργανικός συνδυασμός από διάφορες τεχνολογίες και υποσυστήματα, τα οποία χρησιμοποιούνται στο σπίτι με στόχο την παροχή ασφάλειας, ευκολίας και άνεσης στους χρήστες. Το έξυπνο σπίτι χρησιμοποιεί τις τεχνολογίες υπολογιστικής, ελέγχου, παρουσίασης εικόνων και επικ οινωνίας μέσω της σύνδεσης στο διαδίκτυο, προσφέροντας τη δυνατότητα ελέγχου και διαχείρισης διαφόρων αυτόματων ενεργειών μέσα στο οικιακό περιβάλλον. Η χρήση του διαδικτύου των πραγμάτων στο έξυπνο σπίτι, με εφαρμογή διαφορετικών ασύρματων τεχνολογιών που υποστηρίζουν την απομακρυσμένη μεταφορά δεδομένων, τον έλεγχο και συστήματα ανίχνευσης (RFID, WiFi, Bluetooth κ.λ.π.), έχει εξελίξει τις λειτουργίες του έξυπνου σπιτιού ένα βήμα παρακάτω (Hannah, 2020).

Οι συσκευές στο έξυπνο σπίτι συνδέονται ενσύρματα ή ασύρματα με το διαδίκτυο, μέσα από το οποίο επικοινωνούν με τις βάσεις δεδομένων του νέφους τους. Το νέφος φιλοξενεί τα δεδομένα που αποθηκεύουν οι συσκευές που είναι αναγκαία για τη λειτουργία που θέλει να επιτελέσει. Στις περισσότερες περιπτώσεις ο χρήστης αλληλεπιδρά με τις συσκευές μέσω του έξυπνου τηλεφώνου του που συνδέεται επίσης στο διαδίκτυο.

Οι τεχνολογίες του έξυπνου σπιτιού πρέπει να έχουν την ικανότητα να συνδέονται ψηφιακά με διάφορες συσκευές και πηγές πληροφοριών με σκοπό να παρέχουν στους χρήστες πιο εξατομικευμένες υπηρεσίες. Επίσης, οι τεχνολογίες θα πρέπει να συνδέονται και με τον εξωτερικό κόσμο μέσω του απομακρυσμένου ελέγχου και τη σύνδεση με υπηρεσίες νέφους (Benjamin K. Sovacool, et al., 2021). Το έξυπνο σπίτι περιλαμβάνει τέσσερις τύπους συστημάτων έξυπνου σπιτιού (Georgios Mantas, et al., 2010):

- Το σύστημα ελέγχου οικιακού φωτισμού,κλίματος και ηλεκτρικών συσκευών
- Το σύστημα οικιακής διασκέδασης
- Το σύστημα οικιακής επικοινωνίας και
- Το σύστημα οικιακής ασφαλείας.



Εικόνα 17: Αρχιτεκτονική Έξυπνου Σπιτιού (Jose Sicato, et al., 2019)

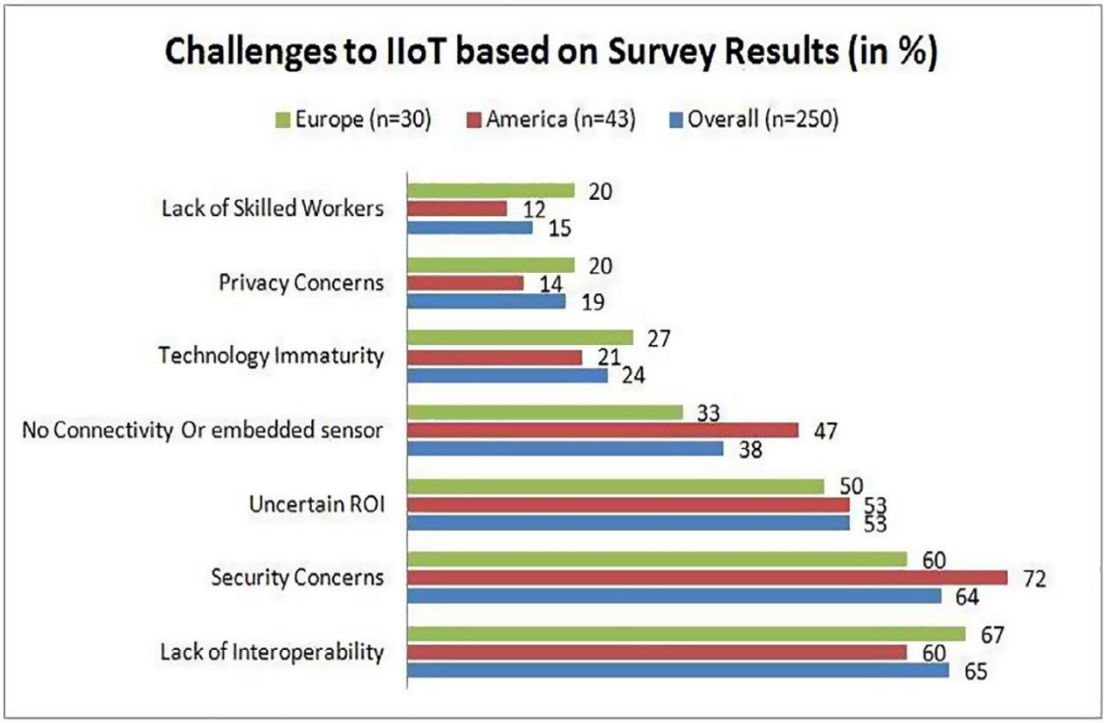
Ένα σύστημα οικιακού αυτοματισμού συνδέει συνήθως ελεγχόμενες συσκευές με έναν κεντρικό κόμβο ή "πύλη". Η διεπαφή χρήστη για τον έλεγχο του συστήματος χρησιμοποιεί είτε επιτοίχια τερματικά, επιτραπέζιους υπολογιστές, μια εφαρμογή κινητού τηλεφώνου ή μια διεπαφή Ιστού που μπορεί επίσης να είναι προσβάσιμη μέσω του Διαδικτύου. Το έξυπνο σπίτι αποτελείται από τρία μέρη: ένα εσωτερικό δίκτυο, που αποτελείται από πολλά και διαφορετικά μέσα και πρωτόκολλα επικοινωνίας, ένα εξωτερικό δίκτυο που αποτελεί το διαδίκτυο και τον πάροχο υπηρεσιών και μία οικιακή

θύρα που είναι ένας μικρός δρομολογητής που παρέχει πρόσβαση δικτύου και συνδέει το οικιακό δίκτυο με τον εξωτερικό κόσμο.

7. ΚΙΝΔΥΝΟΙ & ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Παρά τα πλεονεκτήματά του, υπάρχουν πολλά προβλήματα που σχετίζονται με το έξυπνο δίκτυο και τα οποία σχετίζονται κυρίως με την ασφάλεια, την ιδιωτικότητα και τη διαχείριση των δεδομένων μεγάλης κλίμακας. Το Διαδίκτυο των Πραγμάτων (IoT), δεν αποτελεί μία μεμονωμένη τεχνολογία, αλλά είναι ένας συνδυασμός πολλών τεχνολογιών (τεχνολογία επικοινωνίας, πληροφοριών κλπ), γεγονός που δημιουργεί διάφορα σύνθετα ζητήματα όταν πρόκειται για διασύνδεση πολλών έξυπνων συσκευών σε περιβάλλοντα με μεγάλες γεωγραφικές αποστάσεις. Σε αυτή την περίπτωση υπάρχει ένας κεντρικός διακομιστής (server), ο οποίος υποχρεωτικά ταυτοποιεί όλες τις συσκευές.

Όμως, υπάρχει μεγάλος κίνδυνος κατά τη διασύνδεση των συσκευών να υπάρξει διαρροή των δεδομένων με ψεύτικες ταυτοποιήσεις ή με άλλους τρόπους παραπλάνησης των συσκευών. Οι πιθανότητες αυτές αυξάνονται συνεχώς καθώς στο μέλλον θα υπάρχει δυνατότητα διασύνδεσης ενός τεράστιου αριθμού έξυπνων συσκευών, σε ένα Δίκτυο πολλών συσκευών (NPT), όπου θα παρέχεται η δυνατότητα ηλεκτρονικής πρόσβασης. Σε αυτές τις περιπτώσεις οι συσκευές αυτού του δικτύου θα έχουν πρόσβαση σε έναν τεράστιο όγκο πληροφοριών οι οποίες θα αποθηκεύονται σε έναν κεντρικό διακομιστή (Centralized Data Management Servers-CDMS). Εδώ είναι που ανακύπτουν ζητήματα ασφάλειας του τεράστιου όγκου δεδομένων.



***Εικόνα 18: Ζητήματα από την εφαρμογή του Διαδικτύου των Πραγμάτων (*world economic forum industrial internet survey 2014 (Abhishek Raghuvanshi a, 2020))**

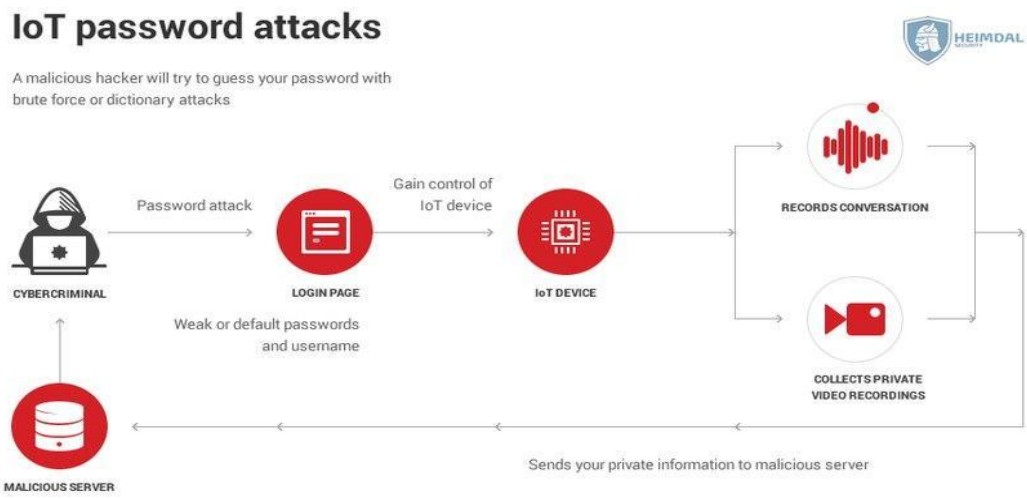
7.1. ΕΙΔΙΚΑ ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Η ασφάλεια αποτελεί μεγάλο πρόβλημα στο Διαδίκτυο των Πραγμάτων, λαμβάνοντας υπόψη τα χαρακτηριστικά των έξυπνων συσκευών. Γι αυτό τον λόγο εφαρμογές ασφαλείας και ιδιωτικότητας θα πρέπει να ενσωματώνονται κατά τον σχεδιασμό των συσκευών και επιπλέον τα δεδομένα θα πρέπει μεν να είναι ανοιχτά και διασυνδεδεμένα, όμως η αποθήκευση και χρήση τους θα πρέπει να γίνονται με τήρηση των αρχών ασφάλειας και ιδιωτικότητας. Επιπλέον, οι συσκευές χρειάζονται μία ταυτότητα και σωστή διαχείριση αυτής, έτσι ώστε να παρέχεται ταυτόχρονα ευχρηστότητα των ψηφιακών υπηρεσιών, δικαιώματα και άδειες πρόσβασης στο έξυπνο δίκτυο (Anon., 2017).

Σύμφωνα με την Κοινότητα Ασφάλειας Εφαρμογών Ανοιχτού Ιστού (OWASP για το 2018[11], οι κορυφαίες αδυναμίες των έξυπνων συσκευών είναι[12] (Sylvia, 2016):

[11] https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html, πρόσβαση (15/03/2021)
[12] https://securityboulevard.com/2020/10/the-top-iot-vulnerabilities-in-your-devices-keyfactor/, (πρόσβαση,15/03/2021)

α. Κωδικοί Πρόσβασης: Μία από τις βασικότερες αδυναμίες των έξυπνων συσκευών είναι οι αδύναμοι ή προβλέψιμοι κωδικοί πρόσβασης όπως και η εφαρμογή σκληρής κωδικοποίησης. Οι δημόσιοι κωδικοί πρόσβασης, η πρακτική της μη συχνής αλλαγής τους και οι εξωτερικές θύρες υλικού ή λογισμικού, επιτρέπουν τη μη εξουσιοδοτημένη πρόσβαση στα έξυπνα συστήματα. Οι εισβολείς μέσω των έξυπνων συσκευών μπορούν να εγκαταστήσουν κακόβουλο λογισμικό, χειραγωγώντας τις αδυναμίες του υλικολογισμικού και έτσι αποκτούν πρόσβαση σε αυτό. Αυτό συμβαίνει καθώς, εκ κατασκευής συνήθως οι συσκευές δεν περιέχουν ασφαλές υλικολογισμικό. Έτσι, είναι αναγκαίο οι εταιρίες να αναβαθμίζουν συνεχώς την ασφάλεια του υλικολογισμικού των έξυπνων συσκευών, καθώς έστω και από μία μόνο συσκευή οι εισβολείς μπορούν να διεισδύσουν σε όλο το έξυπνο δίκτυο. Επίσης, θα πρέπει οι διαχειριστές δικτύου να εφαρμόσουν νέες πολιτικές σύνδεσης που απαιτούν από τους χρήστες και τους διαχειριστές τόσο να αλλάζουν τους προεπιλεγμένους κωδικούς των συσκευών, όσο και να εισάγουν ειδικούς και περίπλοκους συνδυασμούς χαρακτήρων σε διάφορα επίπεδα του έξυπνου περιβάλλοντος.



Εικόνα 19: Επιθέσεις κατά των κωδικών πρόσβασης [13]

β. Μη ασφαλείς Υπηρεσίες Δικτύου: Υπηρεσίες δικτύου που είναι εγκατεστημένες στις ίδιες τις έξυπνες συσκευές και που είτε δεν είναι αναγκαίες, είτε δεν είναι ασφαλείς, θέτουν σε κίνδυνο την ακεραιότητα, αυθεντικότητα, εμπιστευτικό

[13] https://www.gov1.com/technology/articles/iot-security-basics-every-device-owner-needs-now-ArSrjx3DYxLZAQaQ/, (πρόσβαση 18/04/2021)

τητα και διαθεσιμότητα των πληροφοριών καθώς επιτρέπουν εκτός των άλλων και μη εξουσιοδοτημένη πρόσβαση. Οι μη ασφαλείς υπηρεσίες δικτύου μπορούν να αποκαλυφθούν στους εισβολείς[14] εάν θύρες που δεν είναι απαραίτητες για την εκτέλεση υπηρεσιών, είναι ανοιχτές σε έναν διακομιστή ιστού. Ένας εισβολέας μπορεί να σαρώσει τον διακομιστή για ανοιχτές θύρες και να βρει πιθανώς ευάλωτες υπηρεσίες στον διακομιστή, οι οποίες τότε γίνονται αντικείμενο εκμετάλλευσης. Αυτό μπορεί να οδηγήσει σε παραβιασμένο διακομιστή ιστού που δεν λειτουργεί πλήρως. Για τον λόγο αυτό πρέπει να καταργείται η εγκατάσταση μη αναγκαίων υπηρεσιών και να κλείνουν οι θύρες που δεν χρησιμοποιούνται με τη δημιουργία τείχους προστασίας.

γ. Μη ασφαλείς επιφάνειες διασύνδεσης του έξυπνου συστήματος: Οι διάφορες επιφάνειες διασύνδεσης (όπως το μη ασφαλές δίκτυο, η διασύνδεση προγραμματισμού εφαρμογών, το νέφος κ.λ.π.) δημιουργούν ζητήματα ασφαλείας που σχετίζονται με την ανεπαρκή ή παντελή απουσία αυθεντικοποίησης/εξουσιοδοτημένης πρόσβασης, αδυναμίες κρυπτογράφησης και ελέγχου εισερχόμενων και εξερχόμενων πληροφοριών. Συχνά οι εταιρίες παραβλέπουν τις πολιτικές ασφαλείας κατά τη διεπαφή προγραμματισμού εφαρμογών (back-end API), η οποία προσφέρει μία νέα είσοδο πρόσβασης στους εισβολείς. Ένα πρόβλημα είναι ότι οι προγραμματιστές συχνά θεωρούν ότι οι συσκευές προστατεύονται από μόνες τους, ενώ θα πρέπει να σχεδιάζουν πιο ασφαλείς εφαρμογές με τη χρήση τειχών προστασίας, αντιικών, εντοπισμό εισβολών και σχεδιασμό συστημάτων αποτροπής επιθέσεων.

δ. Έλλειψη μηχανισμών ασφαλούς αναβάθμισης και ενημερώσεων: Αυτό οφείλεται στο γεγονός ότι οι κατασκευαστές δεν μεριμνούν για τη μελλοντική λειτουργία των έξυπνων συσκευών, αλλά και γιατί ανάλογα με την γεωγραφική τοποθεσία τους μπορεί να δυσχεραίνονται οι αναβαθμίσεις. Η έλλειψη μηχανισμών ασφαλούς αναβάθμισης σχετίζεται με την αδυναμία επαλήθευσης του λογισμικού της συσκευής,την απουσία κρυπτογράφησης κατά τον διαμοιρασμό της πληροφορίας, την απουσία μηχανισμού αποτροπής υποβάθμισης της συσκευής σε παλαιότερη έκδοση του λογισμικού της που έχει καταργηθεί λόγω προβλημάτων ασφαλείας και την έλλειψη ενημερώσεων για αλλαγές ασφαλείας εξαιτίας αναβαθμίσεων. Ορισμένες συσκευές, παροτι υπάρχει διαθέσιμη αναβάθμιση δεν ειδοποιούν σχετικώς τον χρήστη, ενώ άλλες συσκευές παρότι εγκαθιστούν αυτόματα τις αναβαθμίσεις, μπορεί να

[14] https://wiki.crashtest-security.com/insecure-network-services-open-port-scanner, (πρόσβαση 11/03/2021)

χρειάζονται μία επανεκκίνηση του υλισμικού για να εφαρμοστούν, διαδικασία η οποία όμως καθιστά το σύστημα ευάλωτο και μη διαθέσιμο μέχρι την εφαρμογή των ενημερώσεων. Εξάλλου πολλές διαθέσιμες ενημερώσεις, στερούνται εχεγγύων ακεραιότητας, καθιστώντας τις συσκευές επιρρεπείς σε επιθέσεις. Για τον λόγο αυτό είναι αναγκαίος ο έλεγχος της προέλευσης κάθε ενημέρωσης και η χρήση μόνο των έγκυρων από αυτές.

ε. Χρήση μη ασφαλών ή παλαιάς τεχνολογίας μερών: Η χρήση ελαττωματικών ή μη ασφαλών συστατικών μερών υλικού, λογισμικού και βιβλιοθηκών δημιουργεί μεγάλους κινδύνους. Συστήματα που χρησιμοποιούν παραδοσιακά πρωτόκολλα αναβάθμισης λογισμικού, άλλοτε αδυνατούν να αναγνωρίσουν τις συσκευές και το προφιλ ασφαλείας τους ή να εντοπίσουν και ασφαλίσουν το έξυπνο δίκτυο σε όλη του την έκταση. Οι εταιρίες θα πρέπει να δίνουν μεγαλύτερη βάση στα ψηφιακά πιστοποιητικά και την ύπαρξη ταυτότητας κάθε μέρους που διασυνδέεται.

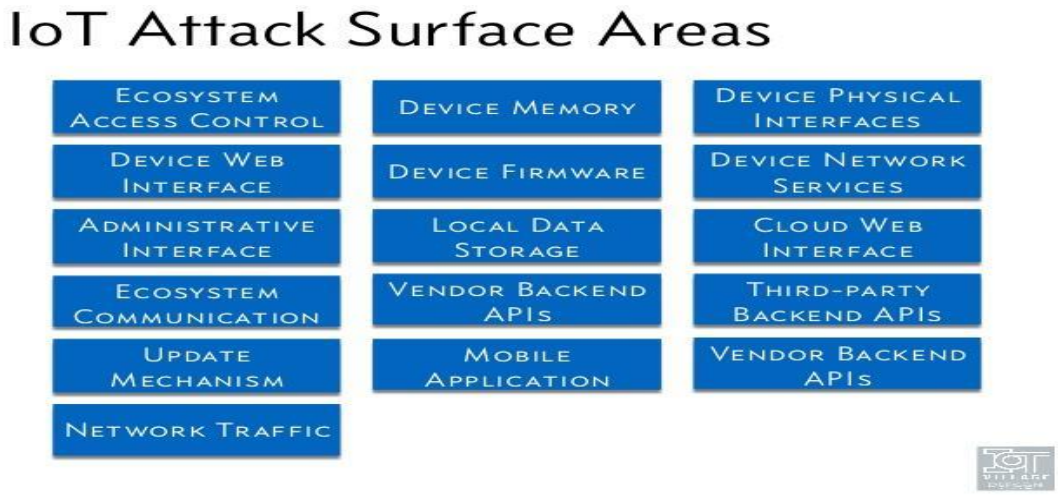
στ. Ανεπαρκής προστασία ιδιωτικότητας: Σχετίζεται με την χωρίς άδεια πρόσβαση και χρήση των απόρρητων πληροφοριών του χρήστη, η οποία διευκολύνεται λόγω της αυτόνομης ανταλλαγής των δεδομένων μεταξύ των συσκευών. Ενώ η μεταφορά δεδομένων από άκρο σε άκρο θεωρείται σχετικά ασφαλής, δεν συμβαίνει το ίδιο και κατά την επικοινωνία η οποία γίνεται μέσα από μία μεγάλη ποικιλία κόμβων και αισθητήρων (Usman, 2020).

ζ. Μη ασφαλής μεταφορά και αποθήκευση δεδομένων: Υπάρχουν μεγαλύτερα εχέγγυα ασφαλείας που σχετίζονται με την ασφαλή αποθήκευση των δεδομένων παρά με τη μεταφορά τους. Η έλλειψη ασφάλειας σχετίζεται με την αδύναμη κρυπτογράφηση ή με την έλλειψη ελέγχου πρόσβασης σε ευαίσθητα δεδομένα οπουδήποτε σε κάθε επίπεδο του έξυπνου συστήματος. Ενώ η ασφάλεια του έξυπνου δικτύου επιδιώκεται με την από τον σχεδιασμό χρήση πρωτοκόλλων ασφαλείας για τον έλεγχο πρόσβασης των διασυνδεδεμένων συσκευών, αυτή η δυνατότητα δεν έχει επεκταθεί και σε άλλα επίπεδα του έξυπνου δικτύου.

η. Έλλειψη διαχείρισης Συσκευών: Σχετίζεται με την πρόληψη, διαχείριση και αναβάθμιση των συσκευών και πυλών. Η αναγνώριση των διασυνδεδεμένων συσκευών είναι ένα πρώτο βήμα για την ασφάλεια. Η χρήση της παραδοσιακής αναγνώρισης των συσκευών με τη χρήση διευθύνσεων δικτύου και βασικών λειτουργικών συστημάτων δεν αποδίδει στα έξυπνα δίκτυα. Οι περισσότεροι οργανισμοί δεν γνωρίζουν τις αδυναμίες των έξυπνων συσκευών, γεγονός που αποδίδεται στην υποτίμηση της σημασίας ελέγχου και παρατήρησης της συμπεριφοράς

των διασυνδεδεμένων συσκευών που οδηγεί στην δημιουργία προφιλ ασφαλείας και ρίσκου κάθε μίας από αυτές.

θ. Μη ασφαλείς προεπιλεγμένες ρυθμίσεις: Οι συσκευές συνήθως έχουν εγκατεστημένες ανασφαλείς εργοστασιακές ρυθμίσεις. Μάλιστα,ορισμένες από αυτές δεν έχουν την ικανότητα να κάνουν το σύστημα πιο ασφαλές, αφού εμποδίζουν τους χρήστες να τροποποιούν τις παραμέτρους.



Εικόνα 20: Επιφάνειες Επιθέσεων κατά του έξυπνου δικτύου [15]

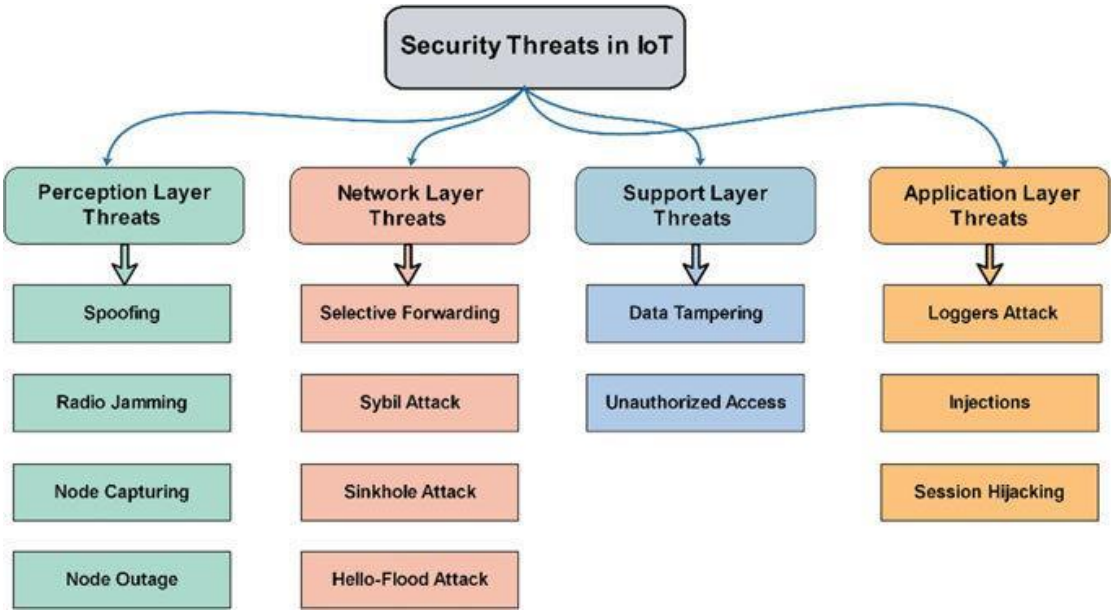
ι. Έλλειψη μέτρων φυσικής προστασίας των έξυπνων συσκευών: Αυτή σχετίζεται με την απόκτηση τοπικού ελέγχου της συσκευής ή απομακρυσμένη μελλοντική επίθεση της συσκευής. Έχει αποδειχθεί ότι οι συσκευές όχι μόνο μπορούν να ενσωματώνουν ελαττώματα αλλά επιπλέον και να αποτελούν σοβαρό παράγοντα κακόβουλης επίθεσης. Αυτό θα μπορούσε να αντιμετωπιστεί με τη διεξαγωγή ελέγχων των επιμέρους συστατικών των συσκευών, καθώς εκεί βρίσκονται συστήματα,κρυπτογραφημένες δυαδικές ακολουθίες, στοιχεία αποθήκευσης κλειδιών, μνήμη φλάς και άλλα στοιχεία ελέγχου των συσκευών. Επομένως, εάν αυτά τα στοιχεία ελέγχου δεν είναι αξιόπιστα, τα υψηλότερα επίπεδα ασφαλείας του έξυπνου δικτύου θα είναι ευάλωτα. Τέλος, στην ασφάλεια των συσκευών μεγάλο ρόλο διαδραματίζει η αποτροπή μόλυνσης της αλυσίδα τροφοδοσίας με κακόβουλες ροές, καθώς και η χρήση εργαλείων ελέγχου αυτών των ροών (Anon., 2017).

[15] https://www.slideshare.net/danielmiessler/iot-attack-surfaces-defcon-2015, (πρόσβαση 23/04/2021)

7.2. ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΑΝΑ ΕΠΙΠΕΔΟ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Κάθε επίπεδο του διαδικτύου των πραγμάτων, αντιμετωπίζει ιδιαίτερους κινδύνους,οι οποίοι είναι (Qi Jing, et al., 2014) :

- **Στο επίπεδο συλλογής δεδομένων** τα ζητήματα ασφαλείας που εγείρονται σχετίζονται με τους περιορισμούς των πόρων, δηλαδή τις περιορισμένες υπολογιστικές ικανότητες, τους μικρούς χώρους αποθήκευσης και τη μικρή δυνατότητα ανιχνεύσεων κακόβουλων επιθέσεων. Οι πιο συνηθισμένες επιθέσεις που δέχεται αυτό το επίπεδο είναι η επίθεση της Λαθρακοής, οι κακόβουλες δρομολογήσεις και η παραβίαση/αλλοίωση των μηνυμάτων. Λόγω του ρόλου αυτού του επιπέδου στη συλλογή των δεδομένων, η ασφάλειά του επιτυγχάνεται μέσω της ασφάλειας των δεδομένων, με τη χρήση αλγορίθμων κρυπτογράφησης, διαχείρισης κλειδιού, ασφαλούς δρομολόγησης και εμπιστοσύνης των κόμβων.



Εικόνα 21: Απειλές Ασφαλείας ανά επίπεδο στο Διαδίκτυο των Πραγμάτων [16]

- **Στο επίπεδο του δικτύου πρόσβασης** κατά τη χρήση ασύρματου δικτύου (WiFi), δημιουργούνται ζητήματα ασφαλείας του δικτύου, καθώς οι χρήστες έχουν από τη μία πλευρά να αντιμετωπίσουν τις παγίδες του διαδικτύου (ιστοί ηλεκτρονικού ψαρέματος κλπ) και από την άλλη πλευρά τις κακόβουλες

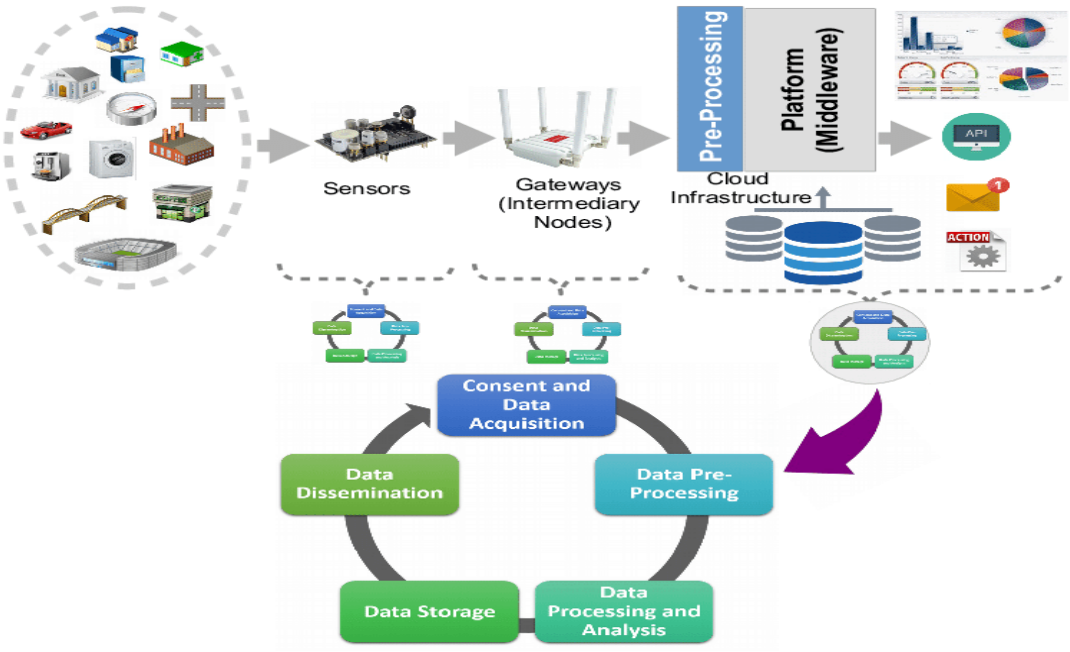
[16] https://www.researchgate.net/figure/Security-threats-at-different-layers-of-the-IoT architecture_fig2_337259162, (πρόσβαση 09/02/2021)

επιθέσεις,όπως επιθέσεις μη εξουσιοδοτημένης πρόσβασης, άρνησης υπηρεσίας κλπ. Στα αποκεντρωμένα ασύρματα δίκτυα (ad hoc) τα ζητήματα ασφαλείας σχετίζονται με την πρόσβαση στο δίκτυο κακόβουλων κόμβων, με την διαρροή ή παραβίαση των δεδομένων και την παραβίαση των δρομολογημένων πληροφοριών.

- **Στο επίπεδο των εφαρμογών**, οι μεγαλύτεροι κίνδυνοι σχετίζονται με την πλατφόρμα υπολογιστικής νέφους, καθώς αυτή κρυπτογραφεί τα δεδομένα και δημιουργεί αντίγραφα δεδομένων των χρηστών που διατηρούνται στο νέφος για ορισμένο χρονικό διάστημα. Άλλο σημαντικό ζήτημα σε αυτό το επίπεδο είναι ο κίνδυνος εντοπισμού της τοποθεσίας και των αναζητήσεων των χρηστών καθώς και της εξόρυξης των ευαίσθητων προσωπικών δεδομένων τους. Εκτός των ανωτέρω, σε αυτό το επίπεδο απαιτείται και η ασφάλεια του ενδιάμεσου λογισμικού (middleware) κατά την συλλογή και ανάλυση των δεδομένων, η οποία επιτυγχάνεται με σωστούς ελέγχους πρόσβασης, προστασία της ιδιωτικότητας, παροχή εξουσιοδότησης χρήστη, διατήρησης ακεραιότητας των δεδομένων, διαθεσιμότητας των δεδομένων σε ζωντανό χρόνο κλπ .

7.2.1. ΕΙΔΙΚΟΤΕΡΑ Η ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ

Ένα από τα σπουδαιότερα ζητήματα στο διαδίκτυο των πραγμάτων είναι η ασφαλής μεταφορά δεδομένων, η οποία προσλαμβάνει δύο μορφές: ασφάλεια εφαρμογών και ασφάλεια του χρήστη. Η πρώτη επικεντρώνεται στην ασφάλεια του χρήστη κατά τη χρήση μίας συγκεκριμένης εφαρμογής, ενώ η δεύτερη στην διασφάλιση των πληροφοριών αλλά και των ευαίσθητων προσωπικών δεδομένων του χρήστη. Για την επίτευξη της ασφάλειας πρέπει να επιτυγχάνεται η απορρητότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριών, παράλληλα με την ιδιωτικότητα του χρήστη κατά την μεταφορά δεδομένων, μέσα σε ένα αξιόπιστο συνεχώς μεταβαλλόμενο έξυπνο δίκτυο. Γι αυτό τον λόγο η αυθεντικοποίηση μεταξύ των διασυνδεδεμένων πόρων αλλά και η ανωνυμοποίηση του χρήστη, προκειμένου να αποφευχθεί η παρακολούθησή του από μη εξουσιοδοτημένους εισβολείς είναι πολύ βασικά εργαλεία. Παράλληλα θα πρέπει να επιλύονται τα ζητήματα της διαλειτουργικότητας, της ετερογένειας και της κλιμάκωσης του έξυπνου δικτύου (Sarada Prasad Gochhayat, et al., 2020).



Εικόνα 22: Τυπική Ροή Δεδομένων στο Διαδίκτυο των Πραγμάτων (Charith Perera, et al., 2019)

7.2.2. ΚΙΝΔΥΝΟΙ ΑΣΦΑΛΕΙΑΣ ΑΠΟ ΤΑ ΚΟΙΝΑ ΜΕΣΑ ΕΙΣΟΔΟΥ ΣΕ ΟΛΕΣ ΤΙΣ ΕΞΥΠΝΕΣ ΣΥΣΚΕΥΕΣ

Ένας πολύ σπουδαίος παράγοντας που θέτει σε κίνδυνο τις έξυπνες συσκευές και συνεπώς το έξυπνο δίκτυο είναι τα κοινά μέσα εξόδου των έξυπνων συσκευών. Οι κίνδυνοι ασφαλείας που σχετίζονται με αυτά είναι (Stylianos Kavalarisa, 2015) :

α. Η έλλειψη υλικής διασύνδεσης-ασύρματη σύνδεση: Επειδή οι έξυπνες συσκευές λειτουργούν χωρίς υλική διασύνδεση, υπάρχει ο κίνδυνος παρεμβολής, εξαιτίας άλλων ασύρματων συσκευών που λειτουργούν στην ίδια συχνότητα, όπως ασύρματα τηλέφωνα ή δόλια παρεμβολή με συνέπεια την απώλεια σήματος.

β. Η παραβίαση των πρωτοκόλλων ονοματοδοσίας διαδικτύου ή ονομάτων τομέων, Χώρων ή Περιοχών (**DNS**), αυτόματης διαμόρφωσης (**DHCP**) και ελέγχου και διαχείρισης (**ARP**), τα οποία χρησιμοποιούνται τόσο για τη διασύνδεση των συσκευών όσο και για την ευκολότερη εγκατάσταση τους από τον τελικό χρήστη, περιορίζοντας την χειροκίνητη εφαρμογή στο ελάχιστο, δημιουργεί κινδύνους για την ακεραιότητα του δικτύου.

γ. Η παραβίαση της καθολικής τεχνολογίας άμεσης σύνδεσης συσκευών (Αρχιτεκτονική UPnP), με την οποία παρέχεται η εύκολη και αποτελεσματική δυνατότητα διασύνδεσης διαφορετικών ηλεκτρονικών συσκευών, καθώς χρησιμοποιούνται κοινές τεχνολογίες και πρωτόκολλα για σύνδεση σε δίκτυο και ιστό,

επιτυγχάνοντας μεταξύ συσκευών ευέλικτη συνδεσιμότητα, έλεγχο και μεταφορά δεδομένων, δημιουργεί κινδύνους.

δ. Οι μέθοδοι διαμοιρασμού αρχείων (CIFS, SMB) και οι συσκευές αποθήκευσης είναι από τα πρώτα μέσα που δέχονται επίθεση, με τη χρήση ενός τροποποιημένου προγράμματος λογισμικού της μνήμης μόνο για ανάγνωση (ROM), ενός κακόβουλου λογισμικού ή οποιαδήποτε άλλης μορφής παραβίασης.

ε. Τα σφάλματα σχεδιασμού της κονσόλας διασύνδεσης, που αποτελεί το μέσο αλληλεπίδρασης μεταξύ του χρήστη και των συσκευών, δημιουργούν ζητήματα ιδιωτικότητας σε σχέση με τη μετάδοση μη κρυπτογραφημένων προσωπικών πληροφοριών.

Στ. Τα μη ενημερωμένα συστήματα διαχείρισης (Android OS, Linux, Windows, Apple, iOS), είναι εξαιρετικά ευάλωτα σε παραβιάσεις. Επιπλέον, λόγω και της πολυπλοκότητάς τους συνήθως αναπτύσσουν ιούς και αδυναμίες που οφείλονται σε εσφαλμένες εφαρμογές, εκτελέσεις ή ευάλωτες βιβλιοθήκες.

ζ. Τέλος, η πρακτική κατά την οποία δεν χρησιμοποιούνται μόνο τα παραδοσιακά διαδικτυακά πρωτόκολλα αλλά γίνεται μετασχηματισμός παλαιότερων μεθόδων, με τη χρήση λογισμικών (html ή java), δημιουργεί προβληματισμούς για τη δημιουργία εφαρμογών που δεν έχουν ελεγχθεί διεξοδικά για ελαττώματα ασφαλείας ή για λογισμικό αβέβαιης προέλευσης (SOUP) που δημιουργεί ζητήματα ασφαλείας της συσκευής.

7.3. ΠΡΑΚΤΙΚΕΣ ΠΟΥ ΚΑΘΙΣΤΟΥΝ ΜΗ ΑΣΦΑΛΕΙΣ ΤΙΣ ΕΞΥΠΝΕΣ ΣΥΣΚΕΥΕΣ (SOHO)

Οι αδυναμίες των έξυπνων οικιακών και συσκευών γραφείων (SOHO), οφείλονται σε μεγάλο βαθμό στον μεγάλο αριθμό των διασυνδεδεμένων ετερογενών συσκευών, στην ύπαρξη μεγάλου αριθμού πυλών εισόδου καθώς και στην πρακτική των κατασκευαστών να τις καταστήσουν ευκολόχρηστες και προσβάσιμες στο ευρύ κοινό εις βάρος όμως της ασφάλειας. Επίσης η εξαγωγή, ανάλυση, μεταφορά, αποθήκευση και επεξεργασία μεγάλων ποσοτήτων δεδομένων μπορούν να οδηγήσουν σε παρακολο ύθηση, ανάλυση συμπεριφοράς, δημιουργίας προφιλ και φωτογράφισης των προσώπων που αφορούν.

Η ασφάλεια των έξυπνων συσκευών περιλαμβάνει την ιδιωτικότητα, την ακε-ραιότητα, τη διαθεσιμότητα και την κρυπτογράφηση των δεδομένων. Οι περισσότερες

έξυπνες συσκευές δεν μπορούν να επεξεργαστούν δεδομένα με ασφαλή τρόπο. Αυτό πολλές τις καθιστά στόχο παραβιάσεων, με αποτέλεσμα την απώλεια δεδομένων, την εγκατάσταση κακόβουλου λογισμικού, την μη εξουσιοδοτημένη πρόσβαση σε αυτές, την παρακολούθηση, τον εντοπισμό τοποθεσίας κ.λ.π . Εκτός των ανωτέρω, δημιουργούνται κίνδυνοι παρακολούθησης και ασφάλειας των ίδιων των δεδομένων με τη δημιουργία διάφορων νομικών προκλήσεων για την προστασία τους. Τέλος, οι ανωτέρω παραβιάσεις επιτρέπουν συχνά σε διαφημιστές και άλλα τρίτα πρόσωπα να αποκτούν πληροφορίες και να δημιουργούν διαφημιστικά προφίλ των χρηστών, σε σχέση με την τοποθεσία, τις προτιμήσεις και τις επιλογές τους.

Ειδικά, οι αιτίες και οι πρακτικές που ακολουθούνται από τις κατασκευάστριες εταιρίες, από τους πωλητές και τους χρήστες και που καθιστούν ευάλωτες τις έξυπνες συσκευές είναι (Boris & Thomas, 2017),(Pal & Purushothaman, 2017):

- **Όσον αφορά το επίπεδο ασφαλείας**, υπάρχει έλλειψη δεδομένων και μετρήσεων σε σχέση με γνωστές ευπάθειες, με αποτέλεσμα να μην είναι ευχερής η μελλοντική αναγνώριση των αδυναμιών των έξυπνων συσκευών. Επιπλέον, υπάρχουν ανεπαρκείς πληροφορίες σχετικά με ζητήματα αναβάθμισης και συντήρησης των έξυπνων συσκευών, λόγω του μικρού χρόνου ζωής τους στο έξυπνο δίκτυο. Οι κατασκευάστριες εταιρίες προχωρούν σε κατασκευή έξυπνων συσκευών ή ανάπτυξης λογισμικού, χωρίς τις αναγκαίες δικλείδες ασφαλείας, καθώς τους ενδιαφέρει να προωθούν οικονομικές συσκευές. Τέλος, πολλές φορές στα έξυπνα δίκτυα χρησιμοποιούνται απαρχαιωμένες συσκευές, καθώς υπάρχει περιορισμένη αντικατάσταση των παλαιών και ανεπιθύμητων συσκευών, με αποτέλεσμα το σύστημα να καθίσταται ευάλωτο.
- **Όσον αφορά την ιδιωτικότητα**, υπάρχει απουσία αυστηρών κανόνων ενάντια στη συλλογή και χρήση των ευαίσθητων δεδομένων των χρηστών. Ακόμα, οι εταιρίες δεν έχουν αναπτύξει μοντέλα προστασίας ιδιωτικότητας για τα έξυπνα δίκτυα και τέλος υπάρχουν λίγοι πόροι κατά την ανάπτυξη των έξυπνων δικτύων που ενσωματώνουν τις αρχές της ιδιωτικότητας και της ταυτοποίησης.
- **Όσον αφορά τη διαλειτουργικότητα** των έξυπνων δικτύων, σοβαρά προβλήματα δημιουργούνται από την μεγάλη ανομοιογένεια του έξυπνου συστήματος, από την ύπαρξη μεγάλων περιορισμών των χρησιμοποιούμενων πόρων (ενέργεια, κ.λ.π), από την απουσία καταχωρημένων δεδομένων για καλύτερες σχεδιαστικές πρακτικές και από τη μικρή προσπάθεια ανάπτυξης

δεδομένων και πρωτοκόλλων. Τέλος, σοβαρό παράγοντα ασφαλείας αποτελεί και η έλλειψη προτύπων/προδιαγραφών, η οποία οφείλεται στην ανομοιογένεια των έξυπνων περιβαλλόντων.

Τέλος, θα πρέπει να σημειωθεί ότι σύμφωνα με την Κοινότητα Ασφάλειας Εφαρμογών Ανοιχτού Ιστού (OWASP), σημαντική αιτία όλων των κινδύνων ασφαλείας των έξυπνων δικτύων, είναι ότι οι κατασκευάστριες εταιρίες δεν δίνουν βάση στην προστασία της ιδιωτικότητας των ευαίσθητων δεδομένων των χρηστών και μάλιστα πολλές φορές τα χρησιμοποιούν χωρίς τη συναίνεσή τους. Επίσης, οι εταιρίες δεν ενσωματώνουν συνήθως στις συσκευές εργαλεία κρυπτογράφησης ή ελέγχου πρόσβασης και δεν παρέχουν υποστήριξη ασφαλείας σε ήδη υπάρχουσες συσκευές με συνεχείς αναβαθμίσεις, παρακολούθηση συστήματος,θωράκιση από δυσλειτουργίες και ικανότητες άμεσης ανταπόκρισης. Τέλος, οι συσκευές συνήθως διαθέτουν ανασφαλείς εργοστασιακές ρυθμίσεις, οι οποίες παραμένουν αμετάβλητες από τους καταναλωτές. [17]

8. ΑΔΥΝΑΜΙΕΣ ΑΣΦΑΛΕΙΑΣ ΕΞΥΠΝΩΝ ΠΟΛΕΩΝ

Στις έξυπνες πόλεις μεγεθύνονται οι κίνδυνοι ασφαλείας λόγω της ύπαρξης αισθητήρων που συλλέγουν διαρκώς δεδομένα σε δημόσια μέρη, της πολυπλοκότητας του δικτύου και της αλληλεξάρτησης των συσκευών, που τις καθιστούν εύκολο στόχο σε διάφορες επιθέσεις. Στις έξυπνες πόλεις απαιτείται η επίτευξη της ασφάλειας και ιδιωτικότητας με την έννοια της διατήρησης των αρχών της διαθεσιμότητας, ακεραιότητας, ιδιωτικότητας, ελέγχου πρόσβασης,του απορρήτου και της μη απόρριψης (non - repudiation). Αυτό αποτελεί μεγάλο στοίχημα για τις έξυπνες πόλεις, καθώς λόγω της αλληλεπίδρασης των συσκευών, η απόκτηση ελέγχου σε μία από αυτές, οδηγεί στο να αποκτηθεί ο έλεγχος σε όλο το δίκτυο, με αποτέλεσμα να κινδυνεύουν τα συλλεχθέντα ευαίσθητα δεδομένα των πολιτών.

Οι αιτίες που καθιστούν ευάλωτες σε επιθέσεις τις έξυπνες πόλεις είναι (Abhishek Raghuvanshi a, 2020),(Afzaal, 2019) καταρχήν η ύπαρξη συσκευών με πολλούς περιορισμούς στο επίπεδο συλλογής δεδομένων (Perception Layer). Οι συσκευές που χρησιμοποιούνται στο έξυπνο δίκτυο, όπως οι αισθητήρες και οι ετικέτες

[17] https://securityboulevard.com/2020/10/lack-of-security-in-iot-devices-explained-what-can-we-do-about-it/, (πρόσβαση 09/02/2021)

RFID, έχουν περιορισμένους πόρους/δυνατότητες με αποτέλεσμα να έχουν περιορισμένους μηχανισμούς ασφάλειας και ιδιωτικότητας.

Δεύτερον, οι έξυπνες πόλεις χρησιμοποιούν συστήματα που δεν διασφαλίζουν την κυβερνοασφάλεια, επειδή οι περισσότερες συσκευές που χρησιμοποιούνται δεν μπορούν να υποστηρίξουν βιώσιμες κρυπτογραφημένες συνδέσεις, οι οποίες άλλωστε και αυτές μπορούν να παραβιαστούν από τους επιτιθέμενους.

Τρίτον, οι τεχνολογίες επικοινωνίας που χρησιμοποιούνται στο επίπεδο ενσωμάτωσης (Integration layer) των έξυπνων συσκευών (RFID, NFC, Bluetooth, BLE κλπ) έχουν αδυναμίες που επιτρέπουν την παραβίασή τους.

Τέταρτον, στο επίπεδο νέφους (Cloud), τα ζητήματα ασφαλείας σχετίζονται με την χρήση εξωτερικής ανάθεσης σε τρίτα μέρη (Outsoursing) με απομακρυσμένη πρόσβαση, γεγονός που έχει ως αποτέλεσμα την αδυναμία αποτελεσματικού ελέγχου των δεδομένων, του πολυλειτουργικού λογισμικού (multi-tenancy) και των μεγάλων δεδομένων.

Πέμπτον, η πολυπλοκότητα του έξυπνου συστήματος και οι αλυσιδωτές επιπτώσεις, λόγω της ύπαρξης μεγάλου αριθμού ετερογενών συσκευών και δικτύων που α λληλεξαρτώνται, καθιστούν πολύ δύσκολη τη δυνατότητα έγκαιρου εντοπισμού του κινδύνου. Οι πολλαπλές συνδέσεις μεταξύ των συσκευών τις αφήνουν εκτεθειμένες σε κινδύνους που μπορούν να οδηγήσουν σε αλυσιδωτές αντιδράσεις και να επηρρεαστούν και άλλα συστήματα.

Έκτον, ιοί λογισμικού είναι πολύ εύκολο να εισχωρήσουν σε περίπλοκα συστήματα όπως αυτό των έξυπνων πόλεων αναλαμβάνοντας τον έλεγχο όλου του συστήματος και των διαθέσιμων δεδομένων.

Έβδομον, για τη χρήση των εφαρμογών της έξυπνης πόλης, οι χρήστες πολλές φορές χρησιμοποιούν τα κινητά τους τηλέφωνα τα οποία εύκολα μπορούν να παραβιαστούν. Επίσης, μπαίνοντας στις εφαρμογές μπορεί από απροσεξία να επιτρέψουν πρόσβαση σε κακόβουλες εφαρμογές.

Τέλος, στην έξυπνη πόλη το σύστημα αλληλεπιδρά με την ανθρώπινη πρωτοβουλία και έτσι τυχόν λάθη μπορεί να οδηγήσουν σε διαρροές δεδομένων ή δυσλειτουργίες.

8.1. ΚΙΝΔΥΝΟΙ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΕΞΥΠΝΟΥ ΣΠΙΤΙΟΥ

Οι συσκευές του έξυπνου σπιτιού θεωρούνται υπολογιστές που εκτελούν συγκεκριμένες εργασίες και όχι ειδικά μηχανήματα με ενσωματωμένη νοημοσύνη. Αποτελούνται δε από έναν μικροεπεξεργαστή που συνδέεται με το διαδίκτυο. Ωστόσο, σε αντίθεση με τους παραδοσιακούς υπολογιστές, σχεδιάζονται με λίγες ή χωρίς ρυθμίσεις ασφαλείας και δεν έχουν τη δυνατότητα ενημερώσεων και αναβαθμίσεων.

Οι αδυναμίες των έξυπνων οικιακών συσκευών προέρχονται κυρίως από την ίδια τη φύση τους, δηλαδή τη συνεχή αλληλεπίδραση και ανταλλαγή πληροφοριών. Έτσι, επειδή το δίκτυο προσαρμόζεται συνεχώς ανάλογα με τις συνεχείς αλλαγές των συνθηκών, απαιτεί μηχανισμούς ασφαλείας που προσαρμόζονται σε αυτές, κάτι που όμως είναι δύσκολο να επιτευθεί. Σύμφωνα με πολλές μελέτες (Enisa.europa.eu, 2020) η πιο σημαντική αδυναμία των έξυπνων συσκευών είναι οι λανθασμένοι ή αδύναμοι κωδικοί, οι οποίοι υιοθετούνται από τους χρήστες είτε λόγω άγνοιας των απαιτήσεων ασφαλείας, είτε λόγω ευκολίας είτε λόγω παράκαμψης των περιορισμών των κωδικών (μήκος, χαρακτήρες κλπ). Οι εισβολείς αποκτούν πρόσβαση σε αυτούς χρησιμοποιών τας διαδικτυακές βάσεις δεδομένων ή μαντεύοντας τους αδύναμους κωδικούς. Επίσης, οι ίδιοι οι οικιακοί χρήστες συνήθως επιτρέπουν άθελά τους τις επιθέσεις πίσω πόρτας (backdoors), δηλαδή την εγκατάσταση κακόβουλου λογισμικού που αναιρεί τις κανονικές διαδικασίες ελέγχου ταυτότητας για πρόσβαση στο οικιακό σύστημα, όπως με την αυτόβουλη αλλαγή της διάταξης και διαμόρφωσης του δικτύου. Αυτό ενισχύεται ακόμα περισσότερο, από το γεγονός ότι δεν υπάρχει μία ορθή πολιτική προστασίας για ένα ασφαλές οικιακό περιβάλλον, καθώς κάθε οικιακός χρήστης, ακόμα και ανήλικοι μπορούν να χρησιμοποιήσουν κάθε συσκευή και υπηρεσία.

Επιπλέον, η χρήση μη κρυπτογραφημένου κειμένου κατά την επικοινωνία του δικτύου, μπορεί να οδηγήσει σε ενεργητικές και παθητικές επιθέσεις που αποκαλύπτουν ευαίσθητες πληροφορίες των συσκευών, καθώς η πλειοψηφία των οικιακών έξυπνων συσκευών είναι συστήματα που στηρίζονται στο νέφος, τα οποία εκθέτουν τις Διασυνδέσεις Προγραμματισμού Εφαρμογών. Ένας άλλος παράγοντας που καθιστά ευάλωτες τις οικιακές συσκευές είναι η χρήση φτηνού υλικο-λογισμικού, η οποία έχει ως αποτέλεσμα να εισάγονται στις έξυπνες οικιακές συσκευές αδυναμίες που είναι σχεδόν αδύνατον να εντοπιστούν από τους διαχειριστές και τους χρήστες. Αυτό σε συνδυασμό με το γεγονός ότι οι συσκευές είναι μονίμως συνδεδεμένες στο

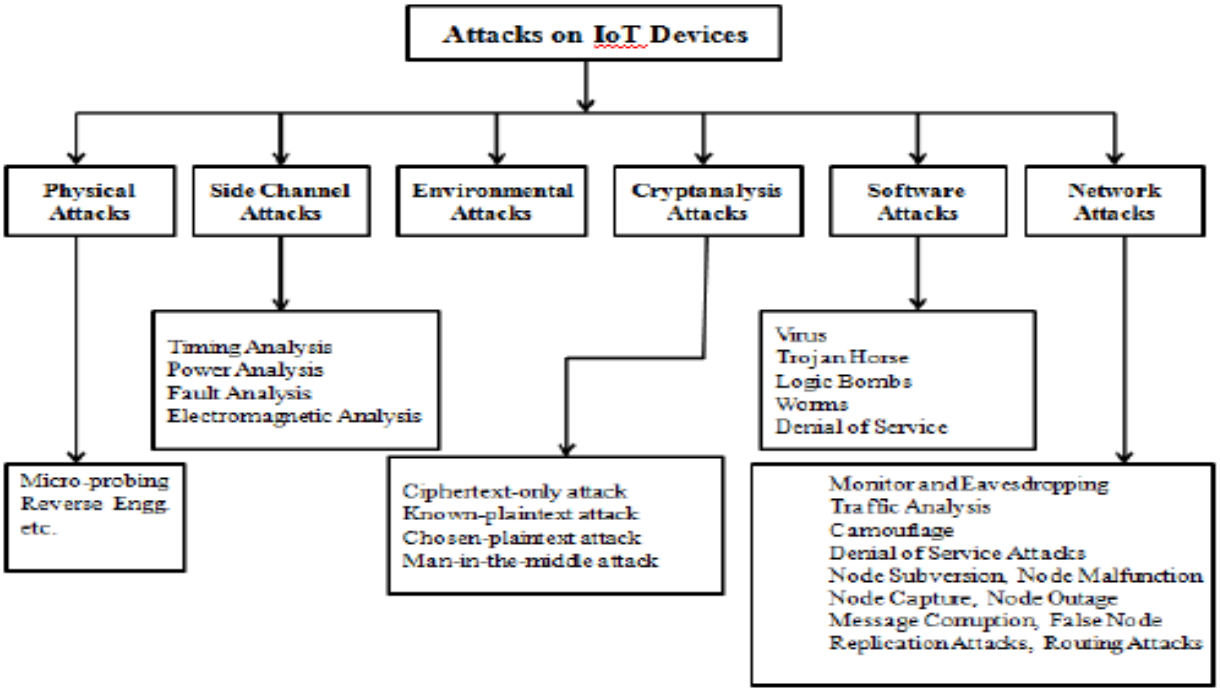
διαδίκτυο, έχει ως αποτέλεσμα να καθίστανται επιρρεπείς σε κακόβουλες επιθέσεις, οδηγώντας συχνά σε άρνηση υπηρεσίας (Agazzi, 2020).

Εκτός των ανωτέρω, οι έξυπνες οικιακές συσκευές εγείρουν και σημαντικά ζητήματα ιδιωτικότητας (Theodoros Aivaliotis, et al., 2020). Η είσοδος τρίτων μερών για την αποθήκευση δεδομένων στο νέφος, επιτρέπει την απομακρυσμένη πρόσβαση και παρακολούθηση και άρα την πρόσβαση στα δεδομένα από παντού. Έτσι με την απόκτηση ελέγχου σε προσωπικά δεδομένα από τρίτα μέρη εξάγονται μοτίβα δραστηριοτήτων των χρηστών. Επίσης, η συναίνεση για χρήση των δεδομένων για άλλους σκοπούς πέραν της χρήσης της συσκευής, μπορεί να οδηγήσει σε νέες παραβιάσεις ιδιωτικότητας. Το έξυπνο σπίτι είναι πολύ ευάλωτο σε εξυπνους ηθοποιούς λόγω του αριθμού των πιθανών σημείων εισόδου. Έτσι, εάν αποκτηθεί η πρόσβαση σε μία έξυπνη οικιακή συσκευή, θα υπάρχει μεγάλη πιθανότητα απόκτησης ελέγχου στο σύνολο του δικτύου με αποτέλεσμα τη διαρροή προσωπικών πληροφοριών και ευαίσθητων δεδομένων.

9. ΕΠΙΘΕΣΕΙΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

9.1. ΠΙΘΑΝΕΣ ΕΠΙΘΕΣΕΙΣ ΣΕ ΔΙΑΦΟΡΕΤΙΚΆ ΕΠΙΠΕΔΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Το έξυπνο δίκτυο μπορεί να δεχθεί επιθέσεις σε διάφορα επίπεδα (J. Cynthia, et al., 2019):



Εικόνα 23: Επιθέσεις στα διάφορα επίπεδα των έξυπνων συσκευών (Sachin Dilip Babar, et al., 2011)

α. Επιθέσεις σε Υλικό Μέσο: Πραγματοποιείται με μη εξουσιοδοτημένη πρόσβαση στους αισθητήρες, στους ενεργοποιητές και στα συστήματα ελέγχου. Το μικρό τους μέγεθος και η μικρή ικανότητα επεξεργασίας που διαθέτουν, δεν επιτρέπουν την εγκατάσταση λογισμικού αναβάθμισης. Επίσης, η απουσία προτύπων ασφαλείας,τους καθιστά ευάλωτους σε επιθέσεις.

β. Επιθέσεις στο λογισμικό: Πρόκειται για επιθέσεις στο λογισμικό, στο λειτουργικό σύστημα (Android, Tiny OS) και στο λογισμικό νέφους (Nimbis,Hadoop κ.λ.π.). Οι έξυπνες συσκευές διαθέτουν ενσωματωμένα λειτουργικά συστήματα ως λογισμικό. Αυτά τα λειτουργικά συστήματα δεν είναι σχεδιασμένα με προδιαγραφές ασφαλείας και για τον λόγο αυτό είναι ευάλωτα σε κακόβουλες επιθέσεις. Σε αυτή την κατηγορία περιλαμβάνονται διάφορες κακόβουλες επιθέσεις όπως ιοί, ο δούρειος ίππος, το σκουλήκι. Επίσης, εδώ εντάσσονται και η αυτοματοποιημένη διαδικασία για την εξεύρεση δυνητικά εκμεταλλεύσιμων σφαλμάτων λογισμικού, τροφοδοτώντας τυχαία με διαφορετικές παραλλαγές από δεδομένα σε ένα πρόγραμμα στόχο, έως ότου μία από αυτές τις παραλλαγές να αποκαλύψει μια ευπάθεια (fuzzing) όπως και η άρνηση υπηρεσίας (DDoS).

γ. Επιθέσεις Δικτύου: Αυτές σχετίζονται με την ασύρματη συνδεσιμότητα, που αποτελεί μία από πολλές ευπάθειες του έξυπνου δικτύου και αποτελεί πόλο έλξης διαφόρων επιθέσεων σε συσκευές ή κόμβους οι οποίοι επικοινωνούν με την πύλη που αποτελεί τον πυρήνα του δικτύου και συνδέει πολλές συσκευές με το νέφος. Αυτή η ευπάθεια οφείλεται στον μεγάλο αριθμό συσκευών και μηχανισμών του έξυπνου δικτύου, καθώς παραδοσιακοί μηχανισμοί ασφαλείας δεν είναι αποτελεσματικοί.

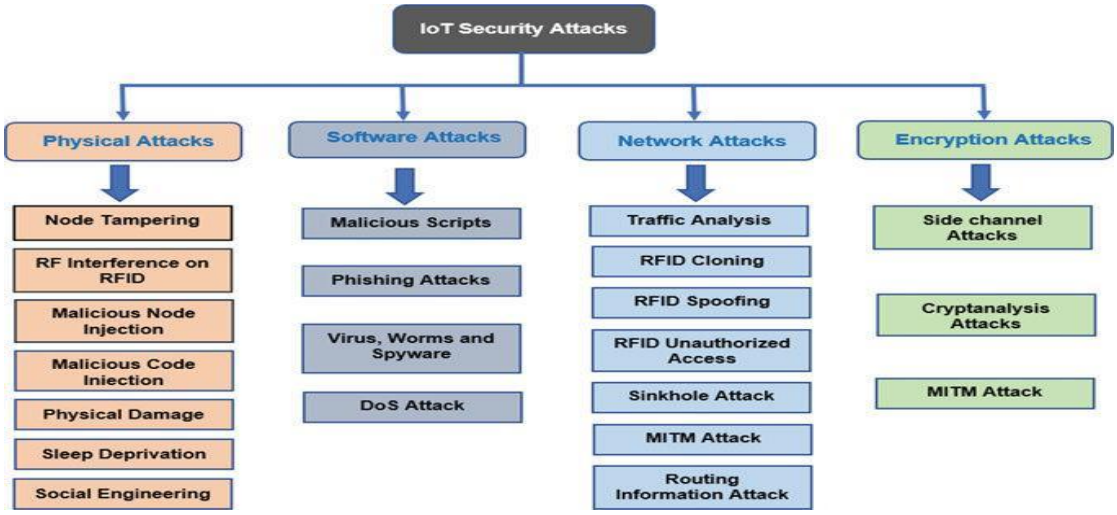
δ. Επιθέσεις Κρυπτανάλυσης: Σε αυτή την επίθεση ο επιτιθέμενος προσπαθεί να αποκτήσει πρόσβαση σε ένα κρυπτογραφημένο μήνυμα χωρίς να έχει πρόσβαση σε κλειδί κρυπτογράφησης, όπως οι επιθέσεις ωμής βίας (brute force attacks), η επίθεση απλού γνωστού κειμένου (known-plaintext attack) κ.λ.π.

ε. Επιθέσεις Δευτερεύοντος Καναλιού: Ο επιτιθέμενος αποκτώντας πληροφορίες από πολλές εφαρμογές του δικτύου (π.χ. ενέργεια, ραδιοσυχνότητες, ήχος κλπ.) αποκτά πρόσβαση στο σύστημα. Έτσι, οι επιθέσεις αυτές βασίζονται σε αδυναμίες του ίδιου του αλγόριθμου που υλοποιήθηκε (σφάλματα λογισμικού, κρυπτανάλυσης κ.λ.π). Οι επιθέσεις αυτές γίνονται ακόμα πιο επικίνδυνες σε ένα έξυπνο δίκτυο δεδομένου ότι αυτό είναι λιγότερο ασφαλές στα διάφορα επίπεδά του και χρησιμοποιεί πιο αδύναμες αυθεντικοποιήσεις.

Στ. Διαρροή Δεδομένων από το Νέφος: Τα δεδομένα αποθηκεύονται στο νέφος, προκειμένου εν συνεχεία να διαμοιραστούν. Η πρόσβαση σε αυτά θα πρέπει να αποκτάται μόνο με τη χρήση ισχυρής αυθεντικοποίησης στη Λίστα Ελέγχου Πρόσβασης. Ο πάροχος νέφους είναι υπεύθυνος για την διαρροή, καθώς μία λάθος ρύθμιση του νέφους μπορεί να οδηγήσει σε διαρροές. Για τον λόγο αυτό η εξωτερική πρόσβαση σε ευαίσθητα δεδομένα και σε αρχεία καταγραφών (logs) θα πρέπει να έχει περιορισμούς.

9.2. ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ ΣΤΟ ΕΞΥΠΝΟ ΔΙΚΤΥΟ

Οι επιθέσεις που μπορεί να δεχτεί το έξυπνο δίκτυο είναι (J. Cynthia, et al., 2019) :



Εικόνα 24: Επιθέσεις Ασφαλείας του Έξυπνου Δικτύου (Hany F. Atlam & Gary Wills, 2020)

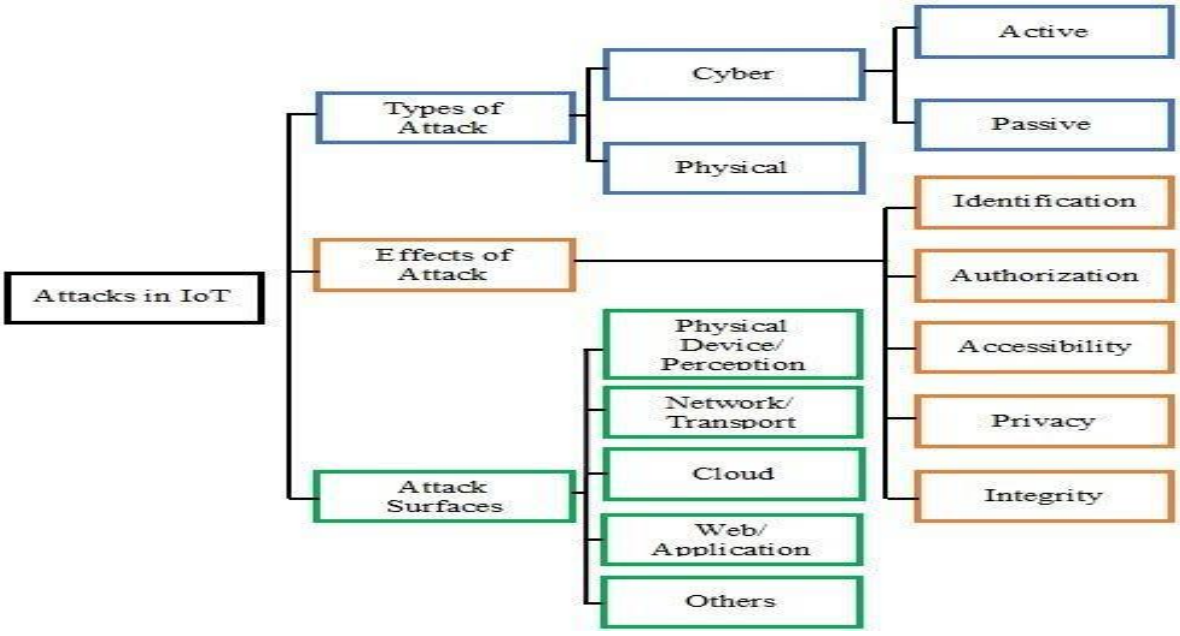
- **Η Άρνηση υπηρεσίας (Dos)** η οποία στοχεύει στο να εξαντλήσει τους πόρους των παρόχων υπηρεσιών και το εύρος ζώνης του δικτύου. Η Επίθεση παρεμβολής καναλιού είναι επίσης μία μορφή τέτοιας επίθεσης.
- **Η Λαθρακοή (Eavedropping)** είναι όταν οι παθητικοί επιτιθέμενοι στοχεύουν στην επικοινωνία, αποκτώντας πρόσβαση στα δεδομένα και εξάγοντας πληροφορίες από αυτά. Οι ενεργητικοί επιτιθέμενοι αιχμαλωτίζουν έναν εξωτερικό κόμβο για να αποκτήσουν πρόσβαση σε αποθηκευμένα δεδομένα.
- **Ο Έλεγχος έξυπνης οντότητας** είναι όταν ένας ενεργητικός επιτιθέμενος αποκτά τον έλεγχο μίας έξυπνης οντότητας μέσα από ένα μονοπάτι επίθεσης και οδηγεί στον έλεγχο τόσο των δεδομένων όσο και των υπηρεσιών που σχετίζονται με αυτά.
- **Η επίθεση στα δίκτυα που χρησιμοποιούν το πρωτόκολλο δικτύου δημοσίευσης- εγγραφής Μεταφοράς Τηλεμετρίας Ουράς Μηνυμάτων(MQTT) για τη μεταφορά μηνυμάτων μεταξύ των συσκευών**, οφείλεται σε έλλειψη αυθεντικοποίησης και κρυπτογράφησης της επικοινωνίας και μπορεί να οδηγήσει σε επιθέσεις αναβάθμισης του υλικολογισμικού με χρήση κακόβουλου κώδικα, έγχυσης της γλώσσας για πρόσβαση και χειρισμό βάσεων δεδομένων (SQL) και σε Διαδικτυακή δέσμη ενεργειών.
- **Η ζήτηση λύτρων (Ramsonware)** είναι η επίθεση με την οποία οι εισβολείς κλέβουν δεδομένα από οποιαδήποτε επιφάνεια, θύρα ή νέφος του έξυπνου

δικτύου και ζητούν λύτρα για να μην τα δημοσιοποιήσουν ή για να μη διακοπεί η πρόσβαση του θύματος σε αυτά.

- **Η πλαστογράφηση αιτήσεων του έξυπνου δικτύου (Iot Request Forgery)**, είναι όταν ο επιτιθέμενος επιτίθεται στις ίδιες τις έξυπνες συσκευές ενός δικτύου από το να προσπαθήσει να σπάσει πολλαπλά επίπεδα ασφαλείας.
- **Οι κακόβουλες φορητές συσκευές** χρησιμοποιούνται για την επίθεση σε έξυπνο δίκτυο, παρέχοντας πρόσβαση σε αυτό. Τέλος, οι εικονικές απειλές, είναι όταν ο κεντρικός διακομιστής εκτελεί εικονικό λογισμικό, δέχεται επίθεση σε εικονικό περιβάλλον και προσομοιάζει με την επίθεση άνθρωπος στη μέση (Man in the middle Attack) .

9.3. ΕΙΔΗ ΕΠΙΘΕΣΕΩΝ ΣΤΙΣ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Οι εισβολείς μπορούν να επιτεθούν σε μία έξυπνη πόλη (Gilchrist, 2017),(Anwaar AlDairi, 2017) με εργαλεία υποκλοπών-κοριούς (Eavesdropping) με τα οποία δύνανται να παρακολουθούν τα κανάλια επικοινωνίας, αιχμαλωτίζοντας την ροή της δρομολόγησης και αποκτώντας τον χάρτη δικτύου. Επίσης, με κλοπή (theft) μπορούν να υποκλέπτουν ευαίσθητα δεδομένα, πληροφορίες, κωδικούς, κλειδιά κρυπτογράφη σης αλλά και συσκευές. Με την Άρνηση Υπηρεσία (DoS) οι εισβολείς πλημμυρίζουν τις συνδέσεις μέχρι που υπηρεσίες και οι συσκευές μπλοκάρουν.



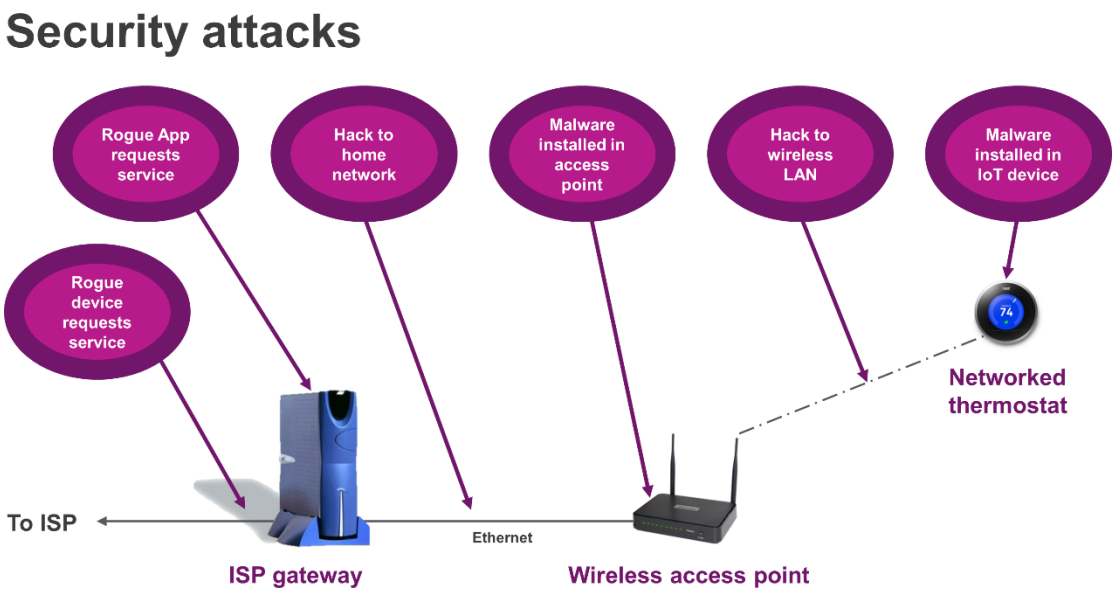
Εικόνα 25: Διάγραμμα της λίστας επιθέσεων ασφαλείας στο έξυπνο δίκτυο (Petros Spachos, et al., 2020)

Οι μεγάλοι κίνδυνοι ασφαλείας που ελλοχεύουν στις έξυπνες πόλεις καταδεικνύεται από πολλά παραδείγματα επιθέσεων. Έτσι, το 2015 σχεδόν 230 χιλιάδες πολίτες της Ουκρανίας, αντιμετώπισαν μία μεγάλη περίοδο χωρίς σύνδεση ρεύματος καθώς το σύστημα ηλεκτροδότησης δέχτηκε επίθεση από εισβολείς. Η Ατλάντα, πρωτεύουσα της Τζορτζια των ΗΠΑ, δέχτηκε επίθεση από έναν ιό (Samsam) που επηρέασε το 30% των εφαρμογών λογισμικού της για δύο βδομάδες. Ζητήθηκαν κρυπτονομίσματα (bitcoins) που αντιστοιχούν σε 55.000$ ως λύτρα, αλλά η πόλη αρνήθηκε να τα δώσει. Οι συνέπειες κόστισαν 12,2 εκατομμύρια δολλάρια. Ο Άγιος Μαρτίνος, ένα νησί της Καραϊβικής δέχθηκε επίθεση, με αποτέλεσμα όλες οι κυβερνητικές υπηρεσίες να είναι ανενεργές για μία εβδομάδα, όσο οι αρχές προσπαθούσαν να ανακτήσουν τον έλεγχο [18] . Τέλος, το 2016 χρησιμοποιήθηκε κακόβουλο λογισμικό (Mirai) για μια σειρά κατανεμημένων επιθέσεων άρνησης υπηρεσίας (επιθέσεις DDoS) στις 21 Οκτωβρίου 2016, στοχεύοντας συστήματα που λειτουργούν από τον παροχέα Dyn Name System (DNS). Η επίθεση προκάλεσε τις μεγάλες πλατφόρμες και υπηρεσίες Διαδικτύου να μην είναι διαθέσιμες σε μεγάλο αριθμό χρηστών στην Ευρώπη και τη Βόρεια Αμερική [19].

9.3.1. ΕΠΙΘΕΣΕΙΣ ΚΑΤΑ ΤΟΥ ΕΞΥΠΝΟΥ ΣΠΙΤΙΟΥ

Στο έξυπνο σπίτι, οι εισβολείς μπορούν να παρέμβουν και να αλλοιώσουν απομακρυσμένα τα μεταδιδόμενα μηνύματα του δικτύου, να προκαλέσουν άρνηση υπηρεσιών και να αποκτήσουν πρόσβαση σε απόρρητα δεδομένα των οικιακών χρηστών. Συγκεκριμένα, οι επιθέσεις στο έξυπνο σπίτι σχετίζονται με την πρόσβαση των δεδομένων από μη εξουσιοδοτημένους χρήστες ή οντότητες (παραβίαση εμπιστευτικότητας), με την παραβίαση της ακεραιότητας των δεδομένων και του συστήματος, την παραβίαση της διαθεσιμότητας του συστήματος, την έλλειψη ελέγχου της τοποθεσίας όπου αποθηκεύονται τα δεδομένα, την παραβίαση των κωδικών πρόσβασης ή και άλλων μηχανισμών ταυτοποίησης του χρήστη, την δημοσιοποίηση ευαίσθητων προσωπικών δεδομένων και την έλλειψη αυθεντικοποίησης/εμπιστοσύνης των διασυνδεδεμένων συσκευών και άρα της γνησιότητας των συλλεχθέντων πληροφοριών (Susan Y.L. Wakenshaw1*, 2018).

[18] https://www.dilitrust.com/en/blog/cyber-attacks-smart-cities/ (πρόσβαση 16/01/2021)
[19] https://en.wikipedia.org/wiki/2016_Dyn_cyberattack, (πρόσβαση 23/04/2021)



Εικόνα 26: Επιθέσεις Ασφαλείας κατά των έξυπνων συσκευών [20]

Οι απειλές μπορούν να προκληθούν αρχικά εσωτερικά, εξαιτίας τη μη κατάλληλης διαμόρφωσης και σύνδεσης του οικιακού δικτύου καθώς και τη μη σωστή διάταξη των διακομιστών, των συσκευών και των τειχών προστασίας. Η διαμόρφωση και σύνδεση του οικιακού δικτύου είναι εύκολο να διαρραγεί αφού οι χρήστες μπορούν εύκολα να αλλάξουν την διάταξη του δικτύου, αφαιρώντας ή μετακινώντας ή προσθέτοντας νέα μέρη.

Εκτός από τις εσωτερικές, υπάρχουν και οι εξωτερικές απειλές των οικιακών συστημάτων, οι οποίες διακρίνονται σε παθητικές και ενεργητικές:

α. Οι παθητικές επιθέσεις είναι δύσκολο να εντοπιστούν, καθώς με αυτές οι επιτιθέμενοι προσπαθούν να αποκτήσουν πρόσβαση στις μεταδιδόμενες πληροφορίες χωρίς να τις αλλοιώσουν (λαθρακοή και ανάλυση κίνησης):

- Με τη λαθρακοή, που είναι η πιο συχνή επίθεση ανοιχτών δικτύων, ο επιτιθέμενος παρακολουθεί την κίνηση των χρηστών μεταξύ του εσωτερικού οικιακού δικτύου και του εξωτερικού κόσμου χωρίς τη συναίνεσή τους, αποκτώντας μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα.
- Με την ανάλυση κίνησης, επιτρέπεται η εξαγωγή ευαίσθητων πληροφοριών από την παρατήρηση του μοτίβου ανταλλαγής μηνυμάτων ακόμα και όταν αυτά είναι κρυπτογραφημένα.

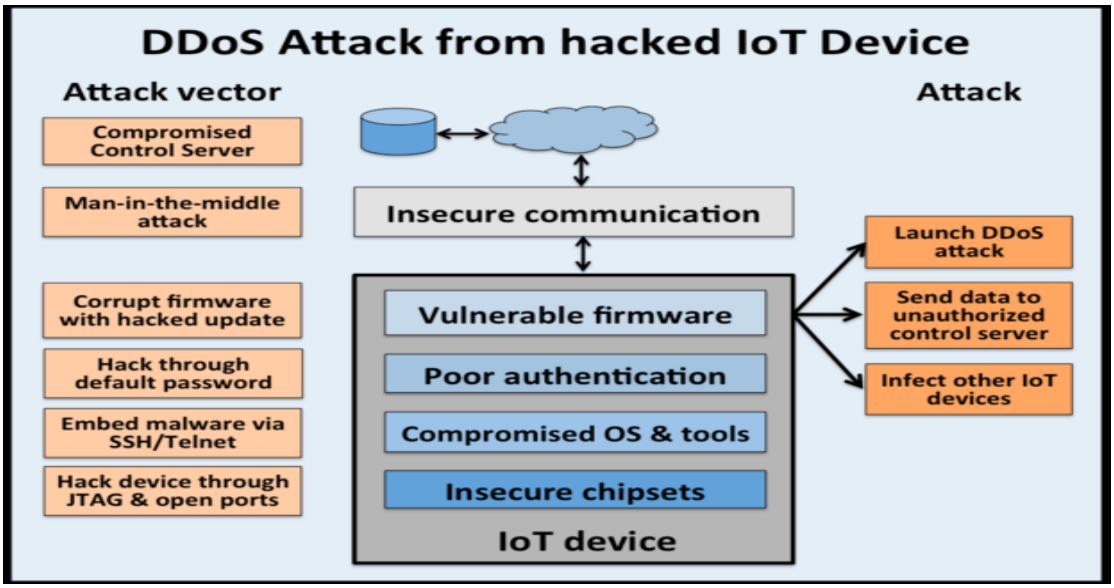
[20] https://wavecomp.ai/blog/security-in-iot-devices/, (πρόσβαση 23/04/2021)

β.Οι ενεργητικές επιθέσεις είναι αυτές με τις οποίες οι επιτιθέμενοι προσπαθούν να χειραγωγήσουν τις πληροφορίες ή να εισάγουν ψευδείς πληροφορίες στο οικιακό σύστημα. Οι κυριότεροι τύποι αυτών, είναι η μεταμφιεσμένη επίθεση (masquerading attack), η επανάληψη (replay), η αλλοίωση μηνυμάτων, η άρνηση υπηρεσίας και κακόβουλοι κώδικες.

- Με τη μεταμφιεσμένη επίθεση, ο εισβολέας αποκτά μη εξουσιοδοτημένα προνόμια στο οικιακό σύστημα παριστάνοντας ότι είναι ένα εξουσιοδοτημένο πρόσωπο ή οντότητα.
- Με την επίθεση επανάληψης, ο εισβολέας αιχμαλωτίζει ένα αντίγραφο ενός αιτήματος μίας έγκυρης υπηρεσίας που αποστέλλεται από μία συσκευή του οικιακού δικτύου, την αποθηκεύει και μετά την αναπαράγει, με σκοπό να αποκτήσει πρόσβαση της υπηρεσίας στην οποία ο χρήστης έχει πρόσβαση.
- Με την επίθεση αλλοίωσης των μηνυμάτων, ο εισβολέας παρεμβαίνει στην επικοινωνία μεταξύ δύο εξουσιοδοτημένων οντοτήτων, αλλάζοντας το λογισμικό έτσι ώστε να ενεργεί κακόβουλα ή τροποποιώντας τα δεδομένα.
- Με την άρνηση υπηρεσίας, ο εισβολέας είτε αποστέλλει άπειρα μηνύματα στο εσωτερικό δίκτυο του έξυπνου σπιτιού με αποτέλεσμα να υπερφορτωθούν οι πόροι με κίνηση είτε αποστέλλει τεράστιο αριθμό μηνυμάτων στους διακομιστές και συσκευές που συνδέονται στο διαδίκτυο έτσι ώστε να μπλοκάρει την εσωτερική κίνηση που μεταδίδεται μέσω ενσύρματου ή ασύρματου δικτύου μέσα στο έξυπνο σπίτι.
- Οι κακόβουλοι κώδικες, είναι απειλές λογισμικού του έξυπνου συστήματος, με τις οποίες οι εισβολείς τροποποιούν, καταστρέφουν ή κλέβουν δεδομένα και αποκτούν μη εξουσιοδοτημένη πρόσβαση. Εγκαθίστανται στο σύστημα με διάφορες επιθέσεις στην επικοινωνία του δικτύου μέσω ηλεκτρονικών μηνυμάτων, ιστοσελίδων κλπ.

Συνοψίζοντας, θα πρέπει να τονιστεί ότι το οικιακό σύστημα είναι πιο ευάλωτο όταν λειτουργεί ασύρματα. Η ασφάλεια σε αυτό σχετίζεται με τη διατήρηση της ιδιωτικότητας και τη μη παρεμπόδιση της σωστή λειτουργίας των οικιακών υπηρεσιών. Αυτό μπορεί να επιτευχθεί με τη διατήρηση των έξι στοιχείων, ήτοι της εμπιστευτικότητας, ακεραιότητας, αυθεντικοποίησης, εξουσιοδότησης, διαθεσιμότητ

ας και μη άρνησης υπηρεσίας, με την αυθεντικοποίηση να αποτελεί το πρώτο βήμα ασφαλείας του οικιακού συστήματος (Georgios Mantas, et al., 2010).



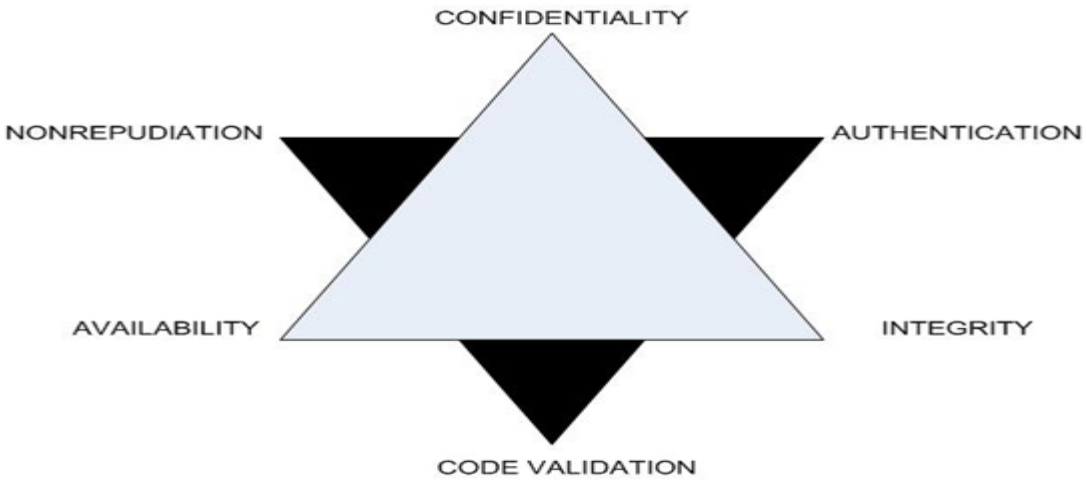
Εικόνα 27: Επίθεση Άρνησης Υπηρεσίας (DoS) στο Έξυπνο Δίκτυο [21]

10. ΕΠΙΤΕΥΞΗ ΑΣΦΑΛΕΙΑΣ

10.1. ΤΡΙΑΔΑ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΕΞΥΠΝΩΝ ΣΥΣΚΕΥΩΝ (CIA & CIA+)

Η ασφάλεια των έξυπνων συσκευών και πόλεων σχετίζεται με την τριάδα ασφαλείας (CIA), ήτοι την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα (Pal & Purushothaman, 2017).

[21] https://www.networkworld.com/article/3128372/ddos-attacks-using-iot-devices-follow-the-manchurian-candidate-model.html, (πρόσβαση 18/04/2021)



Εικόνα 28:Η Τριάδα Ασφαλείας (cia & cia+) [22]

α. Εμπιστευτικότητα είναι η προστασία των πληροφοριών από την δυνατότητα πρόσβασης από τρίτα μη εξουσιοδοτημένα πρόσωπα. Δεδομένης της επικοινωνίας και ανταλλαγής ευαίσθητων πληροφοριών μεταξύ εκατοντάδων συσκευών στο έξυπνο δίκτυο, είναι αναγκαία η επίτευξή της, καθώς αυτή η αλληλεπίδραση και αλληλεξάρτηση όλων των μερών, καθιστά το έξυπνο δίκτυο ευάλωτο σε επιθέσεις. Στον ψηφιακό κόσμο η εμπιστευτικότητα διασφαλίζεται είτε με τον έλεγχο πρόσβασης είτε με την κρυπτογράφηση.

β. Η ακεραιότητα σχετίζεται με την προστασία των πληροφοριών από επιθέσεις που οδηγούν στην αλλοίωση των δεδομένων. Στον ψηφιακό κόσμο η ακεραιότητα εξασφαλίζεται με τις ψηφιακές υπογραφές που αποτελούνται από έναν μοναδικό αριθμό (hash) ο οποίος στηρίζεται στο περιεχόμενο ενός εγγράφου και εντοπίζει κάθε παρέμβαση και αλλαγή. Έτσι,ακόμα και η οποιαδήποτε μικρή αλλαγή του εγγράφου θα οδηγήσει σε τελείως διαφορετικό αριθμό (hash). Στη συνέχεια, ο αριθμός (hash) υπογράφεται από τον δημιουργό του εγγράφου, διασφαλίζοντας έτσι ότι μόνο αυτός τον δημιούργησε. Οι ψηφιακές υπογραφές στηρίζονται στην ίδια τεχνολογία με την κρυπτογράφηση.

γ. Η διαθεσιμότητα σχετίζεται με την αδιάκοπη λειτουργία του έξυπνου συστήματος και τη διαρκή διαθεσιμότητα των δεδομένων προς τους εξουσιοδοτημένους χρήστες. Το νέφος και οι συσκευές αποθήκευσης θα πρέπει να εμφανίζουν τα δεδομένα και τις υπηρεσίες υλικολογισμικού όποτε ζητείται. Αυτό είναι πολύ σημαντικό καθώς οι επιτιθέμενοι χρησιμοποιούν δύο τρόπους για να πλήξουν τη

[22] https://informationsecuritybuzz.com/isbuzz-expert-panel/cia-triad-and-new-emerging-technologies-big-data-and-iot/, (πρόσβαση 16/01/2021)

διαθεσιμότητα. Είτε εισέρχονται στο σύστημα καταστρέφοντάς το ολοσχερώς, είτε το βομβαρδίζουν τόσο πολύ ώστε είναι υπερφορτωμένο για να μην ανταποκρίνεται (DoS, DDoS).

Εκτός των ανωτέρω, υπάρχουν και άλλες πλευρές ασφάλειας που πρέπει να διασφαλιστούν στο έξυπνο δίκτυο (CIA+) (Boris & Thomas, 2017), (Pal & Purushothaman, 2017):

ε. Η αυθεντικοποίηση είναι ουσιώδες ζητούμενο όλων των επιπέδων του έξυπνου συστήματος και είναι αναγκαία για την απόδειξη της γνησιότητας των διασυνδεδεμένων συσκευών και λοιπών μερών και την διασφάλιση οτι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στο έξυπνο σύστημα. Αυτή υλοποιείται είτε με τη χρησιμοποίηση ψηφιακού πιστοποιητικού είτε με τη χρήση ονομάτων χρήστη (usernames) και κωδικών πρόσβασης (passwords).

Στ. Ο έλεγχος πρόσβασης είναι άλλος ένας αναγκαίος όρος ασφαλείας. Σε ένα έξυπνο περιβάλλον ο κύριος έλεγχος πρόσβασης διενεργείται στους αισθητήρες και τους ενεργοποιητές και άρα σχετίζεται με την ασφάλεια των δεδομένων και των εντολών. Η πραγματοποίηση του ελέγχου πρόσβασης γίνεται σταδιακά,με έλεγχο συγκεκριμένων δεδομένων και λειτουργιών κάθε φορά, αφού γίνει συγκεκριμενοποίηση των δεδομένων και κωδικοποίηση των κανόνων (γλώσσα XML ή XACML). Επίσης, ένας άλλος τρόπος ελέγχου είναι και η χρήση της συναίνεσης, από τους ίδιους τους χρήστες.

ζ. Τέλος, η μη απόρριψη (non-repudiation) σχετίζεται με την ικανότητα ενός συστήματος να παρέχει ικανούς ελέγχους και αποδείξεις οτι ένα συγκεκριμένο πρόσωπο ή σύστημα προέβη σε μία συγκεκριμένη ενέργεια, όπως για παράδειγμα η αναφορά επιβεβαίωσης παραλαβής ενός ηλεκτρονικού μηνύματος.

10.2. ΛΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΑ ΔΙΑΦΟΡΑ ΕΠΙΠΕΔΑ ΤΟΥ ΕΞΥΠΝΟΥ ΔΙΚΤΥΟΥ

Η ασφάλεια θα πρέπει να επιτευχθεί σε όλα τα επίπεδα του έξυπνου δικτύου (Abdul Fuad Abdul Rahman, et al., 2016).

α. Στο πρώτο επίπεδο που βρίσκονται οι συσκευές θα πρέπει η τοποθεσία των αισθητήρων και των κόμβων να είναι διαμορφωμένη, έτσι ώστε αυτοί να είναι ασφαλισμένοι και να εμποδιστεί ο μη εξουσιοδοτημένος εντοπισμός τους. Επίσης θα

πρέπει να υπάρχει έλεγχος για την πρόσβαση μόνο του χρήστη και του διαχειριστή του έξυπνου δικτύου, ισχυρή αυθεντικοποίηση και εξουσιοδότηση. Τέλος, η ασφάλεια του λειτουργικού συστήματος και της πλατφόρμας είναι αναγκαία για την αποτροπή εφαρμογής κακόβουλου λογισμικού και κώδικα.

β. Στο δεύτερο επίπεδο επικοινωνίας, η ασφάλεια του δικτύου είναι αναγκαία για την απομόνωση τυχόν επίθεσης λαθρακοής (eavesdropping). Επίσης, η επίτευξη ασφαλών θυρών κατά την επικοινωνία συσκευής προς συσκευή (M2M), επιβάλλεται για την ασφαλή επικοινωνία των κόμβων αισθητήρων με το νέφος. Τέλος, η ασφαλής σήραγγα/ενθυλάκωση των δεδομένων, η κρυπτογράφηση της επικοινωνίας και τα ασύρματα πρωτόκολλα επίσης προσφέρουν προστασία από την επίθεση της λαθρακοής.

γ. Στο τρίτο επίπεδο υποδομής, απαιτείται η ασφάλεια των εφαρμογών του ιστού και του νέφους καθώς εκεί διενεργούνται η αποθήκευση, η υποδομή και οι υπηρεσίες νέφους του έξυπνου δικτύου, του ενδιάμεσου λογισμικού (Middlware), της πλατφόρμας και της αποθήκευσης. Επίσης, απαιτούνται η εφαρμογή ενός κύκλου ζωής ανάπτυξης λογισμικού (SDLC) και περιοδικές αξιολογήσεις ασφαλείας, με στόχο την αποτροπή των απειλών, την αποτροπή κακόβουλου λογισμικού και κώδικα, τη διαρροή δεδομένων και τη μη εξουσιοδοτημένη πρόσβαση.

δ. Τέλος, στο επίπεδο της Αναλυτικής των Δεδομένων απαιτείται η διαχείριση των μεγάλων δεδομένων για την οργάνωση των τεράστιων σε όγκο δεδομένων, ανάλυση των μεγάλων δεδομένων για την ακριβή ανάλυση και την αποκάλυψη κρυφών μοτίβων και συσχετισμών και τέλος ανάλυση προβλέψεων για την πρόβλεψη μελλοντικών απειλών (Kaustav Ghosh & Asoke Nath, 2016).

10.3. ΠΡΑΚΤΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΩΝ ΕΥΠΑΘΕΙΩΝ ΤΩΝ ΕΞΥΠΝΩΝ ΔΙΚΤΥΩΝ

Είναι πολύ σημαντική η τήρηση διάφορων πρακτικών από τους χρήστες και τις κατασκευάστριες εταιρίες. Συγκεκριμένα:

α. Ως προς τους χρήστες: Πρακτικές που πρέπει να εφαρμόζουν οι χρήστες για την επίτευξη της ασφάλειας των έξυπνων δικτύων είναι να αποκτήσουν πλήρη ορατότητα του ακριβούς αριθμού των διασυνδεδεμένων συσκευών και να κάνουν συνεχή επικαιροποίηση αυτού του καταλόγου. Επιπλέον, η λεπτομερής γνώση του τύπου/ταυτότητας κάθε συσκευής και κάθε πληροφορίας γι αυτή (υλικό, λογισμικό, λειτουργικό σύστημα κλπ) και η δημιουργία ενός προφιλ ρίσκου που προκύπτει από

την παρατήρηση της συμπεριφοράς κάθε συσκευής κατά τη διασύνδεσή της με τις άλλες, μπορεί να προλάβει πολλούς κινδύνους.

Μία άλλη σημαντική πρακτική ασφαλείας είναι η κατάτμηση του δικτύου σε τμήματα, η οποία επιτρέπει τον ευκολότερο έλεγχο των κινήσεων δεδομένων μεταξύ των μερών του έξυπνου δικτύου και άρα την ευχερέστερη διαπίστωση τυχών επιθέσεων. Η δημιουργία ισχυρών κωδικών και η συνεχής ενημέρωση με αναβαθμισμ ένο λογισμικό επιδιόρθωσης των συσκευών για τυχόν γνωστές αδυναμίες είναι σημαντική. Τέλος, η παρακολούθηση σε πραγματικό χρόνο των συσκευών επιτρέπει τη διαρκή ανάλυση της συμπεριφοράς τους και την πρόβλεψη για αντιμετώπιση τυχόν μελλοντικών ζητημάτων ασφαλείας**.** [23]

β. Ως προς τις κατασκευάστριες εταιρίες: Οι κατασκευαστές θα πρέπει να αντιμετωπίζουν τις γνωστές αδυναμίες συσκευών σε επόμενα μοντέλα, να εφαρμόζουν λογισμικά επιδιόρθωσης σε υπάρχουσες συσκευές και να σταματήσουν την υποστήριξη απαρχαιωμένων συσκευών. Επίσης, θα πρέπει να εστιάσουν στην ασφάλεια από τη φάση του σχεδιασμού και να διεξάγουν συνεχείς ελέγχους ώστε να διαπιστώνεται ότι δεν έχουν παραβλέψει αδυναμίες συστημάτων ή συσκευών. Θα μπορούσαν επίσης να αναπτύξουν ένα σύστημα για να δέχονται αναφορές ασφαλείας των ήδη χρησιμοποιούμενων συσκευών, από εξωτερικές οντότητες**.**[24]

Εκτός των ανωτέρω, άλλες ενέργειες ασφαλείας είναι η χρήση κλειδώματος της υπηρεσίας μετά από κάποιο χρόνο αδράνειας (account timeout), το κλείδωμα του χρήστη μετά από έναν συγκεκριμένο αριθμό λανθασμένων Κωδικών (Account logout), η χρήση διπλής αυθεντικοποίησης (κωδικός και όνομα χρήστη παράλληλα), περιορισ μοί ως προς το επιτρεπόμενο περιεχόμενο ενός κωδικού πρόσβασης, επιλογή των αναγκαίων θυρών και κλείσιμο των μη χρησιμοποιούμενων, εφαρμογή αναβαθμίσεων και επιδιορθώσεων, κρυπτογράφηση των δεδομένων, ανακάλυψη και αποτροπή των επιθέσεων, αναφορά συμβάντων (event reporting), εκτός σύνδεσης δημιουργία αντιγράφων ασφαλείας των δεδομένων, αντιική προστασία, έλεγχοι διεισδύσεων στο σύστημα, εφαρμογή μεθόδων ελέγχου των εισερχόμενων δεδομένων,ψηφιακή υπογρα φή κώδικα (Syed Rizvi, et al., 2020).

[23] https://www.paloaltonetworks.com/cyberpedia/how-to-secure-iot-devices-in-the-enterprise, (πρόβαση 16/03/2021)

[24] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained, (πρόσβαση 11/02/2021)

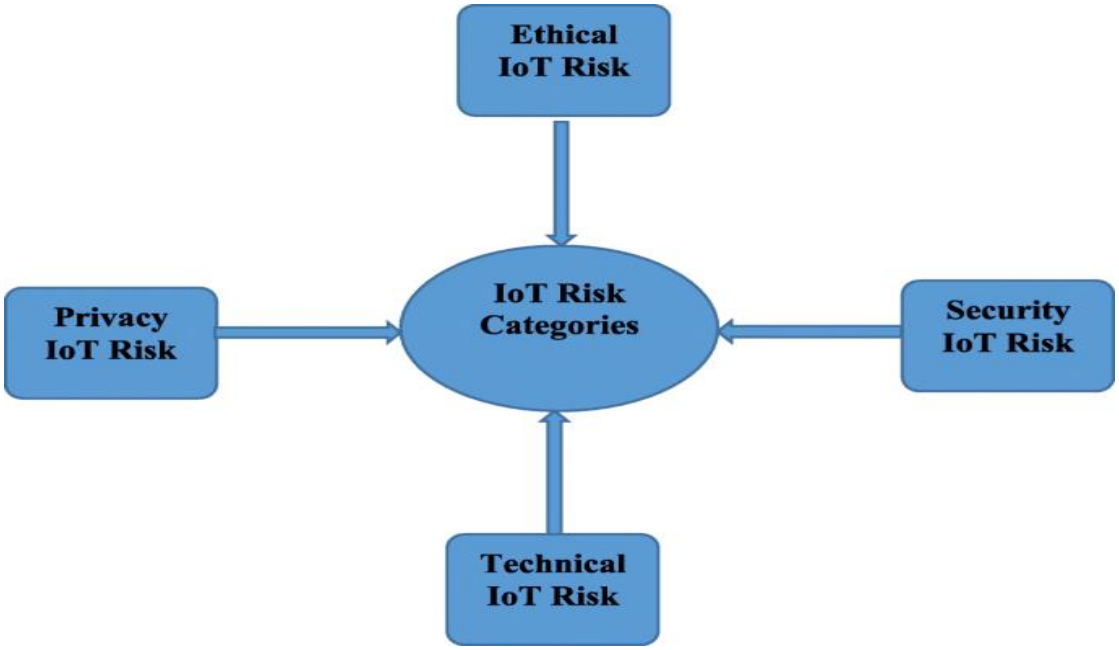
10.3.1. ΟΙ ΜΕΘΟΔΟΛΟΓΙΕΣ ΜΕΤΡΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ ΓΙΑ ΤΗΝ ΑΠΟΤΡΟΠΗ ΤΩΝ ΚΙΝΔΥΝΩΝ

Η μέτρηση του ρίσκου στο έξυπνο δίκτυο είναι πολύ σημαντικός παράγοντας για την αποτροπή των κινδύνων ασφαλείας. Υπάρχει ένας μεγάλος αριθμός μεθοδολογιών αξιολόγησης της ασφάλειας των πληροφοριών, που στηρίζονται σε ποικιλία παραμέτρων. Συνεπώς, δεν υπάρχει μία μόνο συγκεκριμένη μεθοδολογία που να ανταποκρίνεται σε μία τόσο μεγάλη ποικιλία έξυπνων συσκευών και να παράγει αξιόπιστα αποτελέσματα.

Ορισμένες τέτοιες γνωστές μέθοδοι είναι (Pal & Purushothaman, 2017), (Stylianos Kavalarisa, 2015) σύμφωνα με την Κοινότητα Ασφάλειας Εφαρμογών Ανοιχτού Ιστού (OWASP):

- Η μέτρηση ρίσκου η οποία μετρά το ρίσκο συσχετίζοντας την πιθανότητα με το αποτέλεσμα και χρησιμοποιείται σε σύνθετα επιχειρηματικά μοντέλα.
- Η μέθοδος μέτρησης κοινών αδυναμιών (CVSS), η οποία καταμετρά τις αδυναμίες που στηρίζονται στις τρείς κατηγορίες, ήτοι βάσης, χρόνου και περιβάλλοντος και
- Η ανάλυση του μονοπατιού επίθεσης (TMAP), η οποία αξιολογεί τις απειλές που σχετίζονται με τέσσερις παράγοντες, ήτοι την πρόσβαση, την ευπάθεια, τον στόχο και την επηρεαζόμενη τιμή.

Θα πρέπει όμως να επισημανθεί ότι το μειονέκτημα όλων αυτών των μεθόδων, είναι οτι απευθύνονται κυρίως σε επαγγελματίες ασφαλείας υπολογιστών και δεν είναι εύχρηστες από τον απλό χρήστη.



Εικόνα 29: Μέτρηση Ρίσκου στο Έξυπνο Δίκτυο [25]

10.4. ΜΗΧΑΝΙΣΜΟΙ & ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΕΞΥΠΝΩΝ ΔΙΚΤΥΩΝ

Για την προστασία των πολύ ευάλωτων και ετερογενών έξυπνων συστημάτων είναι αναγκαία η εφαρμογή ισχυρών μηχανισμών αυθεντικοποίησης και ιδιωτικότητας των δεδομένων, μηχανισμοί που θα μπορούν να αντέχουν τις συνεχώς αυξανόμενες επιθέσεις και μέθοδοι έγκαιρης πρόβλεψης ακόμα και ασήμαντων επιθέσεων, καθώς η εκ των υστέρων αντιμετώπιση τους έχει αποδειχθεί ότι αποβαίνει άκαρπη. Όλα τα ανωτέρω είναι αναγκαία καθώς οι ιδιαιτερότητες των έξυπνων δικτύων εξαιτίας της μικρής υπολογιστικής ισχύος των περισσότερων έξυπνων συσκευών, έχουν ως αποτέλεσμα να μην είναι επαρκή τα τείχη και πρωτόκολλα ασφαλείας .

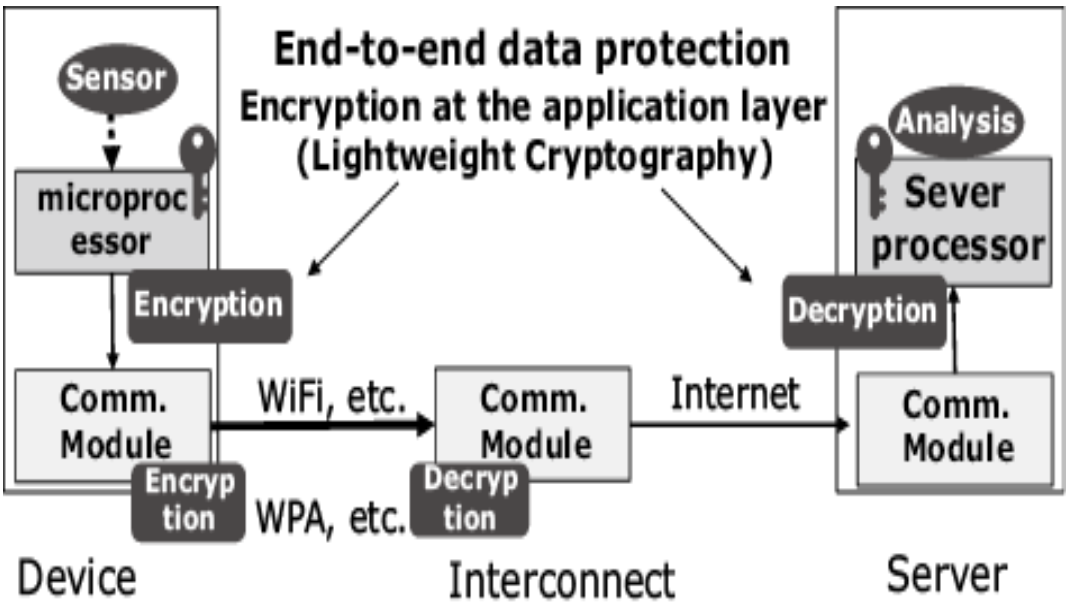
Υπάρχουν δύο κατηγορίες μέτρων ασφάλειας που πρέπει να ληφθούν στα έξυπνα δίκτυα: **α. Η ασφάλεια λειτουργίας**, για την προστασία όλου του δικτύου και της τεχνολογίας από κυβερνοεπιθέσεις και **β. η ασφάλεια των συλλεχθέντων δεδομένων**. Όμως έχει αποδειχθεί ότι είναι ζωτικής σημασίας η επίτευξη της ασφάλειας και ιδιωτικότητας από τον σχεδιασμό, δηλαδή θα πρέπει τα ανωτέρω δύο βασικά μέτρα ασφαλείας να ενσωματωθούν στον πυρήνα των έξυπνων δικτύων και όχι να προστίθενται αναποτελεσματικά εκ των υστέρων .

[25] https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-020-00111-0 ,(πρόσβαση, 18/01/2021

Λόγω της ιδιαιτερότητας, ετερογένειας και ευπάθειας των έξυπνων δικτύων και συσκευών, δεν είναι κατάλληλα όλα τα παραδοσιακά εργαλεία ασφάλειας που χρησιμοποιούνται για τη θωράκιση των παραδοσιακών δικτύων. Τα εργαλεία που μπορούν να χρησιμοποιηθούν στα έξυπνα δίκτυα είναι (Youyang Qu, 2017) :

10.4.1. ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Η χρήση της κρυπτογράφησης διαδραματίζει σημαντικό ρόλο στην ασφάλεια του έξυπνου περιβάλλοντος. Η καθολική και περιοδική ανανέωση των κλειδιών κρυπτογράφησης ή των πιστοποιητικών απαιτούνται όταν ξεκινάει μία καινούργια επικοινωνία. Όμως, η περιορισμένη υπολογιστική ισχύς των αισθητήρων και συσκευών ειδικά στις έξυπνες πόλεις τις καθιστά ακατάλληλες για υψηλού επιπέδου υπολογισμούς που πραγματοποιεί η κρυπτογραφία. Επίσης, η περιορισμένη μνήμη των συσκευών τις καθιστά ακατάλληλες για μεγάλου μεγέθους κλειδιών κρυπτογράφησης/αποκρυπτογράφησης. Συνεπώς, η κρυπτογράφηση Δημοσίου Κλειδι ού (PKI), παρότι δημιουργεί μεγάλα εχέγγυα ασφάλειας, καθώς έχει την απαραίτητη ευελιξία για να λειτουργήσει σε ένα τόσο διάχυτο σύστημα όπως είναι το έξυπνο δίκτυο δεν μπορεί να χρησιμοποιηθεί.



Εικόνα 30: Κρυπτογράφηση στο Έξυπνο Δίικτυο [26]

[26] https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html, (πρόσβαση 21/02/2021)

Βάσει των ανωτέρω συνεπώς, απαιτείται ένα ελαφρύ μοντέλο κρυπτογράφησης δημοσίου κλειδιού που θα απαιτεί μικρή υπολογιστική δύναμη και μικρή κατανάλωση ενέργειας. Επίσης, απαιτούνται περισσότερα εχέγγυα ασφαλείας κατά τη μεταφορά δεδομένων από τους αισθητήρες στο νέφος, με τη χρήση αλγορίθμων κλειδιών και ενός συστήματος αποτελεσματικών τυχαίων αριθμών.

10.4.2. ΤΕΧΝΟΛΟΓΙΑ ΚΑΤΑΝΕΜΗΜΕΝΗΣ ΕΓΓΡΑΦΗΣ (BLOCKCHAIN)

Η τεχνολογία κατανεμημένης εγγραφής (Blockchain), είναι μια νέα τεχνολογία η οποία παρουσιάζεται ως μία δημόσια, μη δυνάμενη να τροποποιηθεί ως προς το ιστορικό της, διανεμημένη σειρά δεδομένων, ομαδοποιημένων σε χρονικά αριθμημένα «τμήματα», «συστοιχίες» (*blocks*).[27]Σε αυτή την τεχνολογία, κάθε τμήμα συνδέεται κρυπτογραφικά και υπογράφεται ψηφιακά από κάθε κόμβο με τον προηγούμενο του. Γι αυτό και μια οποιαδήποτε προσπάθεια αλλαγής των δεδομένων ενός τμήματος θα ήταν αδύνατη καθώς δεν θα μπορούσε να επιβεβαιωθεί κρυπτογραφικά από κανέναν κόμβο στο σύνολο τους.

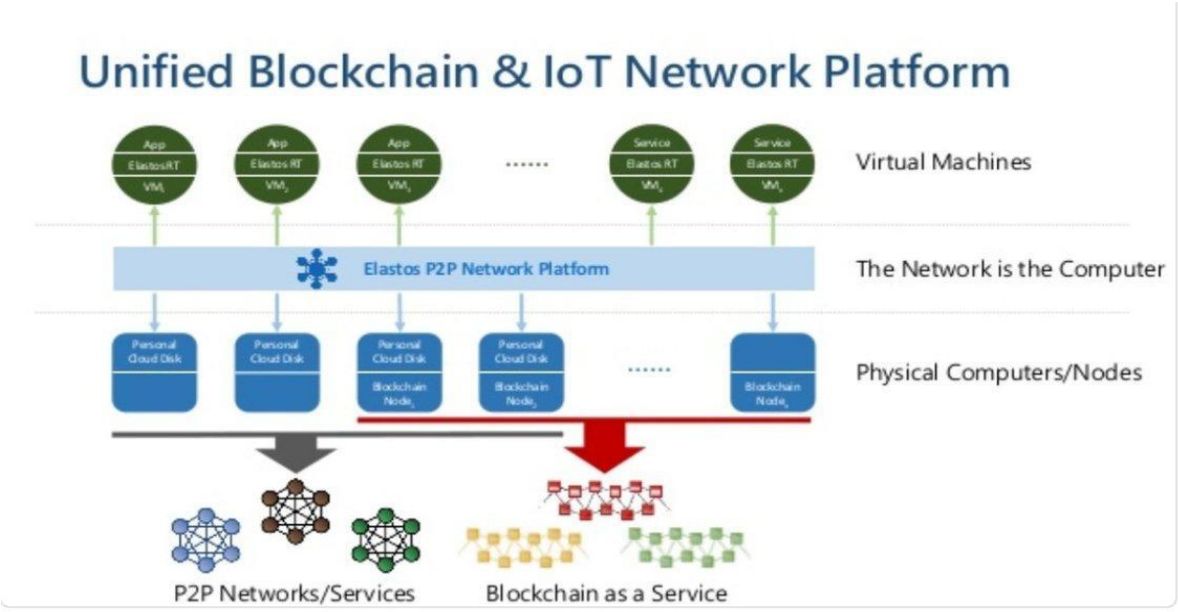
Η τεχνολογία αυτή είναι πολύ αποτελεσματική σε ένα έξυπνο δίκτυο καθώς είναι ιδιαίτερα αποτελεσματική σε περιβάλλοντα όπου αλληλεπιδρά μεγάλος αριθμός συσκευών. Με αυτή την τεχνολογία, αντικαθίσταται η ιδέα του κεντρικού διακομιστή των έξυπνων δικτύων, με αυτή της βάσης δεδομένων κατανεμημένου καθολικού (distributed ledger) σε κάθε μεταφορά δεδομένων με έγκυρη αυθεντικοποίηση (Sunil Kumar Singh & Sumit Kumar, 2021). Εδώ, δεν είναι πλέον αναγκαία η αποθήκευση των λεπτομερειών των μεταφορών, καθώς αρχεία των μεταφορών είναι διαθέσιμα σε πολλούς υπολογιστές της αλυσίδας. Ωστόσο, είναι αναγκαία η χρήση πολλαπλών υπογραφών, για να εξουσιοδοτηθεί μία μεταφορά. Εάν ένας εισβολέας προσπαθήσει να διεισδύσει στο σύστημα, πολλαπλά αντίγραφα είναι διαθέσιμα σε πολλούς υπολογιστές σε όλο τον κόσμο. Έτσι, για να παραβιαστεί το δίκτυο κατανεμημένης εγγραφής απαιτείται η συναίνεση περισσότερο από το 50% των συστημάτων του δικτύου.

Τα πλεονεκτήματά της τεχνολογίας αυτής που επιτρέπει τη χρήση της σε ένα έξυπνο δίκτυο (Nallapaneni Manoj Kumara, 2018) είναι η διασφάλιση του απαραβίαστου των δεδομένων με χρήση κρυπτογραφίας που τα καθιστά αναλλοίωτα, ο ισχυρότερος έλεγχος ταυτότητας και εξουσιοδότηση για έξυπνες συσκευές, η

[27] https://el.wikipedia.org/wiki/Blockchain , (πρόσβαση 21/02/2021)

δυνατότητα κοινής χρήσης μηνυμάτων (peer-to-peer), η αξιοπιστία του συστήματος, η καταγραφή του ιστορικού των ενεργειών, ο διαμοιρασμός αρχείων και η βελτιωμένη επεκτασιμότητα του συστήματος, με αποτέλεσμα τη διανομή του φόρτου εργασίας σε πολλούς υπολογιστές, η άμεση λειτουργία, η μείωση του κόστους ανάπτυξης μίας μεγάλης διαδικτυακής δομής, οι ασφαλείς ενημερώσεις λογισμικού.

Επιπλέον,[28]η τεχνολογία αυτή παρέχει βελτιωμένη προστασία της ιδιωτικής ζωής και ασφαλείας διασφαλίζοντας την επικοινωνία μεταξύ έξυπνων συσκευών και την ιχνηλασιμότητα και υπευθυνότητα των δεδομένων των αισθητήρων. Ακόμη, εξαλείφει τον κίνδυνο παραβίασης δεδομένων καθώς μπορεί να βελτιστοποιήσει τα τρέχοντα πρωτόκολλα παρέχοντας κρυπτογράφηση δεδομένων και επικοινωνιών. Τέλος, η αποκέντρωση των δεδομένων είναι ένα σημαντικό πλεονέκτημα αυτής της τεχνολογίας, καθώς δεδομένης της έλλειψης κεντρικού σημείου ελέγχου, εξαλείφει μεμονωμένα σημεία επίθεσης ή αποτυχίας.



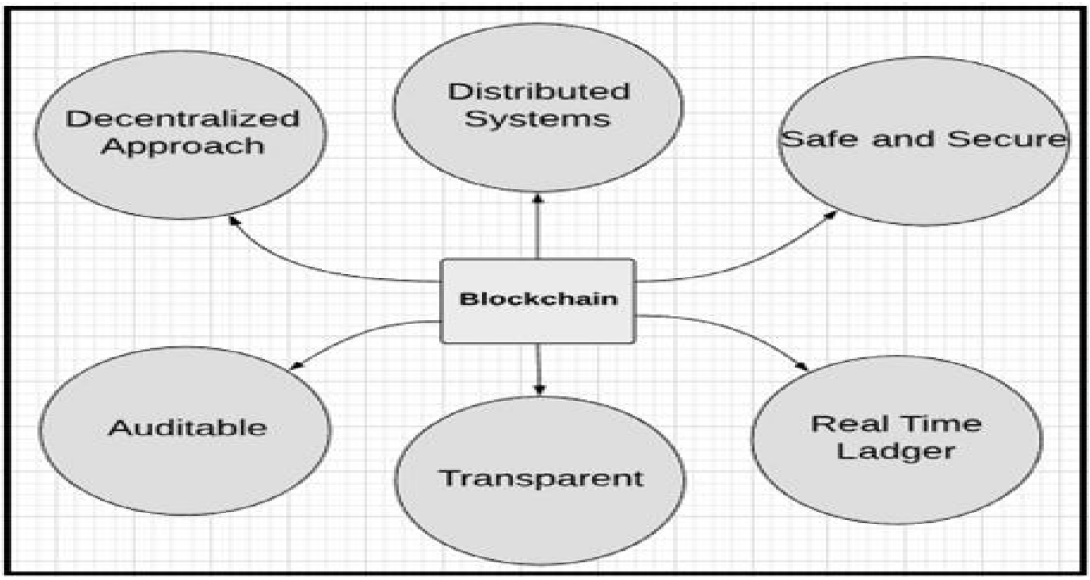
Εικόνα 31: Λειτουργία της τεχνολογίας blockchain στο εξυπνο δικτυο [29]

Η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί ως ενδιάμεσος για βελτιωμένη κλιμάκωση, προστασία των δεδομένων, αξιοπιστία και ιδιωτικότητα. Αυτό μπορεί να

[28] https://www.apriorit.com/dev-blog/638-blockchain-how-can-blockchain-secure-iot-networks, (πρόσβαση, 01/03/2021)
[29] https://twitter.com/ronald_vanloon/status/999282072207446021 , (πρόσβαση, 14/03/2021)

υλοποιηθεί με τη χρήση της σε όλες τις διασυνδεδεμένες συσκευές και κατά τον συγχρονισμό όλων των διαδικασιών μεταφοράς δεδομένων.

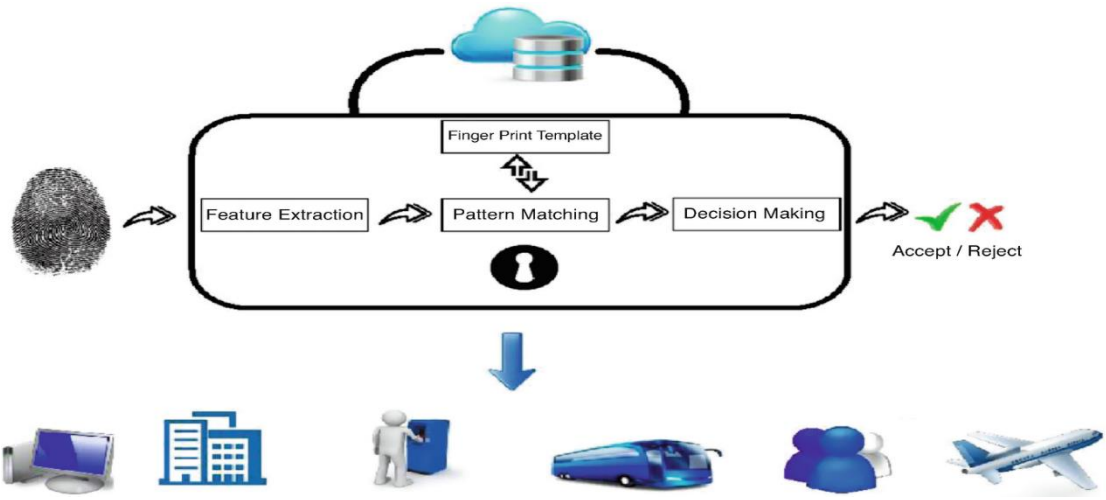
Πέραν των άλλων πλεονεκτημάτων ασφαλείας τα έξυπνα συμβόλαια, μπορούν να προσφέρουν μία αποκεντρωμένη πολιτική επαλήθευσης και ελέγχου αξιοπιστίας μίας έξυπνης συσκευής. Τέλος, τα ζητήματα ασφαλείας των πρωτοκόλλων επικοινωνίας στο έξυπνο δίκτυο, μπορούν να λυθούν με την ενσωμάτωση αυτής της τεχνολογίας. (Hyunsik Yang & Younghan Kim, 2019) (Bruhadeshwar Bezawada, et al., 2018) (FLAUZAC Olivier, et al., 2015) (Gayatri Kapil, et al., 2020)



Εικόνα 32: Χαρακτηριστικά της Τεχνολογίας Κατανεμημένης Εγγραφής (Blockchain) (Tanweer Alam & Mohamed Benaida, 2020)

10.4.3. ΒΙΟΜΕΤΡΙΑ

Στα έξυπνα συστήματα, η Βιομετρία μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση, καθώς αναγνωρίζει ένα πρόσωπο βάσει βιολογικών ή συμπεριφορικών χαρακτηριστικών. Έτσι, επιτρέπει να εξάγονται δεδομένα από δακτυλικά αποτυπώματα, πρόσωπα, φωνές, χειρόγραφες υπογραφές κλπ.



Εικόνα 33: Χρήση Βιομετρικών Δεδομένων στο Έξυπνο Δίκτυο [30]

10.4.4. ΜΗΧΑΝΕΣ ΕΚΜΑΘΗΣΗΣ ΚΑΙ ΕΞΟΡΥΞΗ ΔΕΔΟΜΕΝΩΝ (DATA MINING)

Οι μηχανές εκμάθησης χρησιμοποιούνται συχνά για την βελτίωση των συστημάτων ανίχνευσης εισβολών. Κατά την εξόρυξη δεδομένων δημιουργούνται πολλά ζητήματα ασφάλειας και ιδιωτικότητας ευαίσθητων δεδομένων, όπως εντοπισμός τοποθεσίας και μοτίβα συμπεριφορών. Γι αυτό τον λόγο έχουν αναπτυχθεί διάφορες τεχνολογίες προστασίας ασφάλειας (PPDM, DPPDM, IDS κ.λ.π.) (Niranjan & Nitish, 2016).

10.4.5.ΘΕΩΡΙΑ ΠΑΙΓΝΙΩΝ (GAME THEORY)

Πρόκειται για ένα ισχυρό μαθηματικό εργαλείο, το οποίο κατέστη ένα από τα πιο ισχυρά εργαλεία στην επιστήμη των οικονομικών, όμως έχει αποδειχθεί ότι μπορεί να χρησιμοποιηθεί στην κυβερνοασφάλεια και έχει κεντρίσει το ενδιαφέρον τα τελευταία χρόνια και σε άλλους τομείς. Με απλά λόγια, είναι η μελέτη των διαδικασιών λήψης στρατηγικών αποφάσεων[31]. Πρόκειται δηλαδή για ένα θεωρητικό πλαίσιο, με στόχο τη μοντελοποίηση καταστάσεων σύγκρουσης και συνεργασίας μεταξύ οντοτήτων, που καλούνται παίκτες (Players), καθώς και ανάλυσης της συμπεριφοράς τους. Οι οντότητες/παίκτες θεωρούνται ότι λειτουργούν ορθολογιστικά, δηλαδή με στόχο να επιτύχουν το μέγιστο όφελος ή τη βέλτιστη μέτρηση ρίσκου για τον εαυτό τους. Ένα παιχνίδι αποτελείται από τρία στοιχεία, ήτοι τους παίκτες/οντότητες οι οποίοι μπορούν

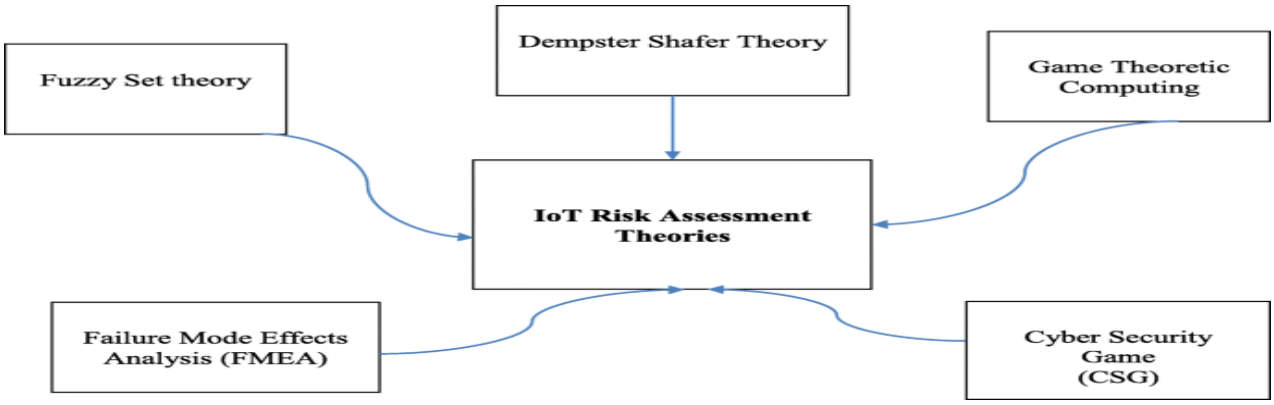
[30] https://link.springer.com/chapter/10.1007/978-3-319-98734-7_19, (πρόσβαση, 25/03/2021)
[31] https://el.wikipedia.org/wiki/%CE%98%CE%B5%CF%89%CF%81%CE%AF%CE%B1_%CF%80%CE%B1%CE%B9%CE%B3%CE%BD%CE%AF%CF%89%CE%BD , (πρόσβαση 15/01/2021).

να λαμβάνουν αποφάσεις στο παιχνίδι, δεύτερον τις στρατηγικές που μπορούν να ακολουθήσουν οι παίκτες και τρίτον το αποτέλεσμα, δηλαδή τα κέρδη ή τις απώλειες που προκαλούνται από την υιοθέτηση των επιμέρους στρατηγικών (Habtamu Abie & Ilangko Balasingham, 2012).

Στο Διαδίκτυο των Πραγμάτων η θεωρία των παιγνίων έχει εφαρμοστεί πολύ σε σχέση με την ιδιωτικότητα των δεδομένων, με στόχο την ανάλυση τόσο της ιδιωτικότητας όσο και της ακρίβειας των δεδομένων. Ενδεικτικά, έχουν προταθεί διάφορα μοντέλα για την ανάλυση της αλληλεπίδρασης μεταξύ του παρόχου και του χρήστη μέσα σε ένα μοντέλο συνεργατικής βαθιάς μάθησης (Collaborative Deep Learning/CDL), μοντέλα για την ορθολογιστική συνεργασία μεταξύ των έξυπνων συσκευών άκρου κ.λ.π. (Deepti Gupta, et al., 2021). Επίσης, πολύ σπουδαία στον τομέα της ασφάλειας είναι η μοντελοποίηση των συγκρούσεων επίθεσης-άμυνας και λοιπών ρίσκων στα έξυπνα συστήματα, δηλαδή η μοντελοποίηση των αποφάσεων των εισβολέων σε σχέση με διάφορες μεταβλητές ή αβέβαια χαρακτηριστικά γνωρίσματα των στόχων, που αποσκοπούν στην απόσπαση δεδομένων από τους αμυνόμενους. Αυτή η μοντελοποίηση μπορεί να οδηγήσει σε αποτελεσματικές λύσεις διαχείρισης απειλών, καθώς η αποτελεσματικότητα ενός μηχανισμού άμυνας στο διαδίκτυο των πραγμάτων εξαρτάται από την αλληλεπίδραση των ενεργειών των δύο παικτών, δηλαδή του εισβολέα και του επιτιθέμενου. Έτσι, η στρατηγική του εισβολέα εξαρτάται από τις ενέργειες του αμυνόμενου και το αντίστροφο.

Οι προτεινόμενες λύσεις που βασίζονται στη θεωρία παιγνίων χρησιμοποιούν παραδοσιακές λύσεις, προχωρώντας ένα βήμα παραπέρα. Ειδικότερα, η θεωρία των παιγνίων χρησιμοποιεί τη μαθηματική απόδειξη για να διερευνήσει μεθόδους ασφαλείας με πιο μεθοδικό τρόπο. Επίσης, χρησιμοποιώντας το αποτέλεσμα που προέκυψε από την ανάλυση του παιχνιδιού μπορεί να συνεισφέρει στη δημιουργία πιο αξιόπιστης άμυνας του συστήματος, ενώ με τη χρήση του κατάλληλου μοντέλου μπορούν να ενσωματωθούν λύσεις ασφαλείας διαμοιρασμένες σε όλο το σύστημα, σε αντίθεση με τις παραδοσιακές μεθόδους ασφαλείας που λαμβάνουν αποφάσεις με πιο κεντρικό τρόπο. Ορισμένα παραδείγματα μοντέλων θεωρίας των παιγνίων είναι το δίλημμα του φυλακισμένου(Static Prisoner’s Dilemma Game), το παιχνίδι μηδενικού αθροίσματος(Static zero-sumgame), το μοντέλο ηγεσίας του Στακελμπεργκ (Stackelberg game) κ.λ.π. (Do Cuong, et al., 2017).

Βάσει των ανωτέρω και συνοψίζοντας, η θεωρία των παιγνίων χρησιμοποιούμενη μαζί με τη μέτρηση ρίσκου μπορούν να αποτελέσουν ένα πολύ αποτελεσματικό εργαλείο άμυνας.



Εικόνα 34: Θεωρίες Εκτίμησης Κινδύνου στο Διαδίκτυο των Πραγμάτων (Kamalanathan Kandasamy, et al., 2020)

10.4.6.ΟΝΤΟΛΟΓΙΑ

Η οντολογία, δηλαδή η ανάλυση του συσχετισμού των οντοτήτων και εννοιών στο έξυπνο δίκτυο, έχει χρησιμοποιηθεί περιορισμένα για την επίλυση προβλημάτων ασφαλείας, όπως εντοπισμός κυβερνοεπιθέσεων και διαχείριση ρίσκων ασφαλείας.Έ νας περιορισμός που υπάρχει σε αυτή,είναι οτι οι μελέτες για τη χρήση της οντολογίας επικεντρώνονται σε συγκεκριμένες εφαρμογές και όχι σε ένα ενιαίο μοντέλο.

10.4.7.ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ

Η αυθεντικοποίηση στοχεύει στην προστασία των δεδομένων και τον έλεγχο πρόσβασης σε ένα έξυπνο σύστημα, μέσα από τον έλεγχο της ταυτότητας των έξυπνων συσκευών. Έτσι, μέσα σε ένα έξυπνο σύστημα, κάθε συσκευή θα πρέπει να είναι σε θέση να αναγνωρίσει και να αυθεντικοποιήσει όλες τις υπόλοιπες. Η ισχυρή αυθεντικοποίηση βοηθά στην αποτροπή εντολών στο σύστημα από μη εξουσιοδοτημένους χρήστες ή συσκευές, καθώς και στον εντοπισμό εισβολέων οι οποίοι παριστάνουν ότι αποτελούν μέρος του έξυπνου συστήματος με στόχο την απόκτηση πρόσβασης στα δεδομένα.

Κάθε έξυπνη συσκευή χρειάζεται μια μοναδική ψηφιακή ταυτότητα, η οποία μπορεί να αυθεντικοποιηθεί κάθε φορά που επιχειρεί να συνδεθεί σε μια πύλη ή έναν κεντρικό διακομιστή, μέσω της σύνδεσής της σε ένα κρυπτογραφικό κλειδί, μοναδικό

ανά συσκευή. Με αυτή την μοναδική ψηφιακή ταυτότητα αφενός οι διαχειριστές του έξυπνου συστήματος μπορούν να εντοπίσουν ανά πάσα στιγμή κάθε έξυπνη συσκευή μέσα στο σύστημα και αφετέρου οι συσκευές επικοινωνούν με ασφάλεια, αποτρέποντας τον έλεγχο του συστήματος από κακόβουλους παράγοντες.

Υπάρχουν διάφορες μέθοδοι αυθεντικοποίησης κατά την επικοινωνία των οντοτήτων στο έξυπνο σύστημα όπως είναι: η μονή αυθεντικοποίηση, με την οποία μόνο η μία οντότητα από τις δύο μπορεί να αυθεντικοποιήσει τον εαυτό της, η αμφίδρομη αυθεντικοποίηση, με την οποία και οι δύο οντότητες μπορούν να αυθεντικοποιηθούν, η τριπλή αυθεντικοποίηση με την οποία μία κεντρική οντότητα αυθεντικοποιεί τις δύο οντότητες και τις βοηθά να αυθεντικοποιήσουν η μία την άλλη, η κατανεμημένη αυθεντικοποίηση, η οποία χρησιμοποιεί μια κατανεμημένη μέθοδο ελέγχου ταυτότητας μεταξύ των μερών της επικοινωνίας και τέλος η κεντρική αυθεντικοποίηση, η οποία χρησιμοποιεί έναν κεντρικό διακομιστή ή ένα αξιόπιστο τρίτο μέρος για τη διανομή και διαχείριση των πιστοποιητικών ελέγχου ταυτότητας που χρησιμοποιούνται.

Δεδομένου ότι το έξυπνο δίκτυο, είναι ένα σύνολο διαφορετικών μηχανισμών και τεχνολογιών, είναι πολύ σημαντική η πολυεπίπεδη αυθεντικοποίηση (MFA), δηλαδή η παροχή εξουσιοδότησης για την επικύρωση της ταυτότητας κάθε τελικού σημείου στο έξυπνο σύστημα. Αυτή πραγματοποιείται με παροχή στοιχείων σε πραγματικό χρόνο σε συνδυασμό με την απαίτηση πιστοποιήσεων. Για την υλοποίηση μίας ισχυρής αυθεντικοποίησης πρέπει να χρησιμοποιούνται ισχυρές αλλά αποτελεσματικές λύσεις κρυπτογραφίας για την τυποποίηση της ασφαλούς επικοινωνίας μεταξύ των μερών ενός έξυπνου συστήματος.[32] Ειδικά στο επίπεδο συλλογής (perception layer), επειδή απαιτείται η απορρητότητα των δεδομένων κατά τη μετάδοσή τους μεταξύ των κόμβων, είναι αναγκαία η αυθεντικοποίηση των κόμβων σε συνδυασμό με την κρυπτογράφηση των δεδομένων. Επιπλέον, λόγω των περιορισμών των κόμβων (ενέργειας,χώρου αποθήκευσης κ.λ.π.) θα πρέπει να εφαρμοστεί ένας συνδυασμός ελαφρών ρυθμίσεων ασφαλείας, που περιλαμβάνουν τη χρήση ελαφρών αλγορίθμων κρυπτογράφησης και πρωτοκόλλων ασφαλείας. Αυθεντικοποίηση σε κάθε τελικό σημείο απαιτείται, παράλληλα και με άλλα εργαλεία

[32] https://securityboulevard.com/2020/09/the-top-internet-of-things-iot-authentication-methods-and-options/ , (πρόσβαση 04/05/2021)

ασφαλείας, και στο επίπεδο δικτύου και το επίπεδο εφαρμογών με στόχο τη διασφάλιση της ιδιωτικότητας των χρηστών (Mohammed El-hajj, et al., 2019).

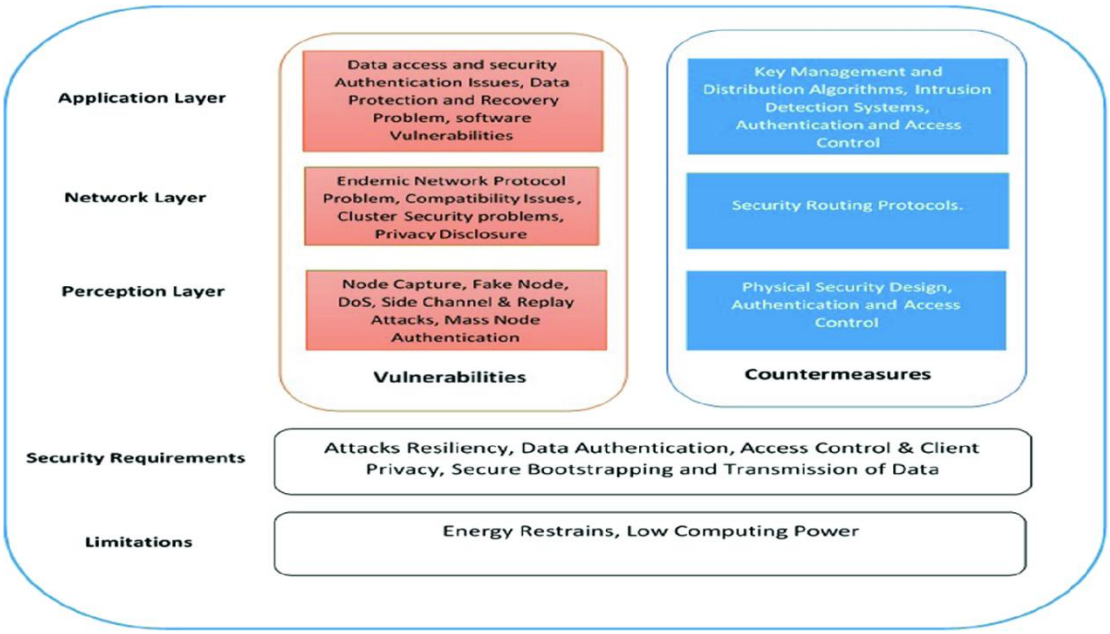
Συνοψίζοντας, η αυθεντικοποίηση κάθε επιπέδου του έξυπνου δικτύου είναι ουσιώδης για την επίτευξη της ασφάλειάς του. Για να είναι όμως η αυθεντικοποίηση αποτελεσματική, θα πρέπει να λαμβάνεται υπόψη η ετερογένεια και οι περιορισμοί των μερών του έξυπνου συστήματος και άρα η αναγκαιότητα αντικατάστασης των παραδοσιακών μεθόδων ασφαλείας με νέες προσαρμοσμένες στις ιδιαιτερότητες του έξυπνου δικτύου.

10.5. ΠΩΣ ΝΑ ΕΠΙΤΕΥΧΘΕΙ Η ΑΣΦΑΛΕΙΑ ΤΟΥ ΕΞΥΠΝΟΥ ΔΙΚΤΥΟΥ ΑΠΟ ΤΗΝ ΒΑΣΗ ΜΕΧΡΙ ΤΟ ΝΕΦΟΣ

Στο έξυπνο δίκτυο, είναι πολύ σημαντική η διατήρηση της ασφάλειας σε όλα τα επίπεδα, καθώς αυτά αλληλεπιδρούν. Συγκεκριμένα αυτό μπορεί να επιτυχθεί με τους εξής τρόπους:

α. Διατήρηση της ακεραιότητας της αλυσίδας τροφοδοσίας των δεδομένων: Για τη διατήρηση αυτής, οι κατασκευαστές των έξυπνων δικτύων και συσκευών, θα πρέπει να υποβάλουν σε ελέγχους όλες τις επιμέρους συσκευές του έξυπνου δικτύου, θα πρέπει να γνωστοποιούν στους χρήστες κάθε αλλαγή του συστήματος, κάθε τεχνική αδυναμία των συσκευών, τυχόν αναβαθμίσεις του συστήματος και να παρέχουν εύκολα προσβάσιμες οδηγίες και λεπτομέρειες τη λειτουργία των έξυπνων συσκευών.

β. Ασφάλεια επικοινωνίας και δικτύου: Πολύ σημαντική για την ασφάλεια, είναι η επικοινωνία των θυρών και των συσκευών τόσο μεταξύ τους όσο και με το νέφος. Η δημιουργία υποκαναλιών επικοινωνίας, η ανάλυση προγενέστερων απειλών του συστήματος, η κατηγοριοποίηση των συσκευών, η ανάλυση των μη εξουσιοδοτημένων κινήσεων και η χρήση τεχνολογίας παρεμπόδισης παρεμβολών ή παρακώλυσης επικοινωνιών, μπορούν να προστατεύσουν το έξυπνο δίκτυο από επιθέσεις.



Εικόνα 35: Λύσεις Για την αντιμετώπιση των κινδύνων στο Έξυπνο Δίκτυο (Anon., 2019)

γ. Ασφάλεια δεδομένων: Για την ασφάλεια των δεδομένων απαιτείται η ασφάλεια των σημείων εξόδου και η ασφάλεια επικοινωνίας (με χρήση της κρυπτογράφησης κλπ.). Επίσης, η ανωνυμοποίηση των χρηστών και η λίστα ελέγχου πρόσβασης θα πρέπει να διασφαλίζεται.

δ. Αποτροπή διαδικτυακών κλοπών: Απαιτείται η δημιουργία έξυπνων δικτύων που θα έχουν την ικανότητα να αναγνωρίζουν και να περιορίζουν τις απειλές, αναλύοντας συνεχώς δεδομένα και διαμοιράζοντας τις πληροφορίες για γνωστές απειλές σε όλες τις συσκευές και μέρη του ετερογενούς δικτύου.

ε. Δημιουργία Προτύπων Ασφαλείας: Έχει επιχειρηθεί να δημιουργηθούν κάποια πρότυπα, τα οποία όμως δεν καλύπτουν τις ανάγκες ασφαλείας που δημιουργεί η συνεχώς αναπτυσσόμενη έξυπνη τεχνολογία (Morta Vitunskaite, 2019). Σύμφωνα με έρευνα του Ινστιτούτου Βρεττανικών Προτύπων (2015), τα πρότυπα ασφαλείας που υπάρχουν σήμερα δεν είναι πολύ κατανοητά, για τη δημιουργία ασφαλείας κατά τον σχεδιασμό του έξυπνου δικτύου και επικεντρώνονται σε πολύ συγκεκριμένα τεχνικά χαρακτηριστικά. Ακόμα, τα πρότυπα αυτά δεν έχουν υιοθετηθεί ακόμα από τη βιομηχανία και δεν έχουν καταστεί υποχρεωτικά. Ενδεικτικά, κάποια από τα υπάρχοντα πρότυπα είναι το IEEE, που είναι ένας οργανισμός που παίζει σπουδαίο ρόλο στη δημιουργία τεχνολογικών προτύπων και προτύπων ασφαλείας για το διαδίκτυο των πραγμάτων, εξαιτίας του οποίου ενσωματώθηκαν ορισμένα πρότυπα του παρελθόντος. Εκτός αυτού, ηγείται του έργου IEEE P2413, με επικέντρωση στην

διασφάλιση της προστασίας, ασφάλειας και ιδιωτικότητας της έξυπνης τεχνολογίας (Cherry, 2017) και έκανε βήματα στο να δημιουργήσει κάποια πρότυπα με στόχο την ασφάλεια σε όλα τα επίπεδα. Άλλα πρότυπα είναι τα DIN, NEN, CEN, CENELEC, ETSI, ISO και IEC, ANSI, GOST R.

ε. Διαχείριση Εμπιστοσύνης (Trust Management): Διαδραματίζει ουσιώδη ρόλο κατά την επικοινωνία των συσκευών μεταξύ τους, διεξάγοντας με τη βοήθεια μίας κεντρικής οντότητας υπολογισμούς φήμης, προκειμένουνα αποφασιστεί εάν μία συσκευή μπορεί να θεωρηθεί έμπιστη.

στ. Διαχείριση Ταυτότητας: Είναι πολύ σημαντική καθώς προσφέρει μοναδική αναγνώριση, αυθεντικοποίηση και εξουσιοδότηση για κάθε μία από τις συσκευές, διασφαλίζοντας έτσι τόσο την αξιοπιστία των ροών δεδομένων όσο και τον ασφαλή έλεγχο πρόσβασης.

Εκτός των ανωτέρω, κάθε σχεδιασμός και μέτρο ασφαλείας, θα πρέπει να λαμβάνουν υπόψη την διαρκή κλιμάκωση που χαρακτηρίζει τη λειτουργία των έξυπνων δικτύων, καθώς ακόμα και μία απλή επιπλέον εντολή μέσα στο έξυπνο δίκτυο, μπορεί να προκαλέσει άρνηση υπηρεσίας. Επίσης, θα πρέπει να ληφθεί υπόψη ότι τα δεδομένα δεν προστατεύονται σε όλα τα στάδια, καθώς η κρυπτογράφηση δεν είναι συνολική. Έτσι, τα μεταδεδομένα ευαίσθητων δεδομένων μπορούν να παρέχουν πολύτιμες πληροφορίες σε εισβολείς.

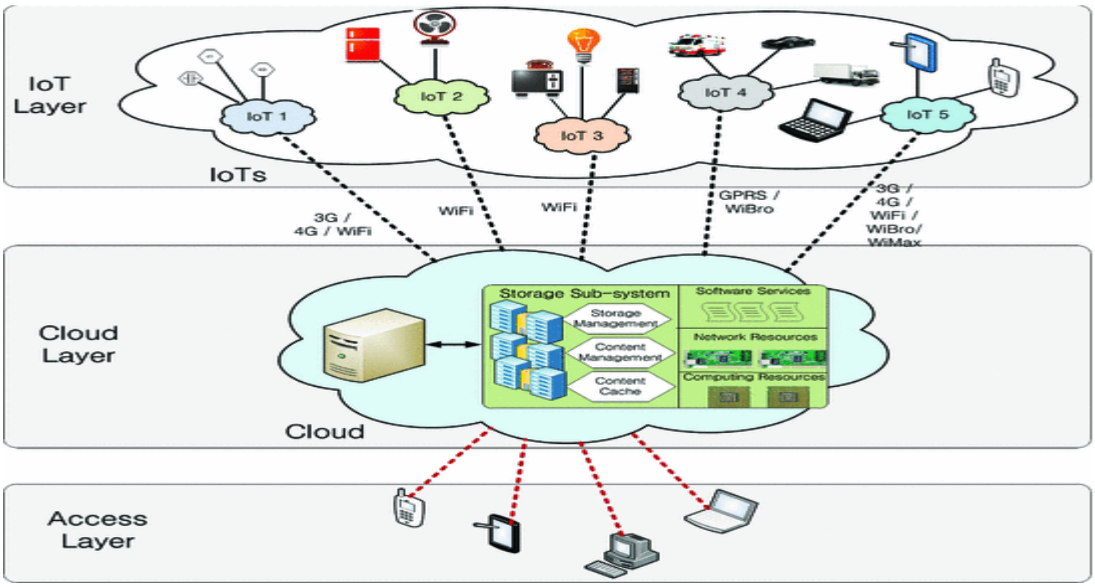
11. ΝΕΦΟΣ (Cloud)

Το νέφος είναι μία συλλογή διακομιστών στους οποίους οι χρήστες έχουν πρόσβαση μέσω σύνδεσης στο διαδίκτυο. Συνήθως, κάθε νέφος διαχειρίζεται ένας πάροχος νέφους-μία εταιρία που προσφέρει τις σχετικές υπηρεσίες, όπως είναι η σύνδεση των συσκευών με το νέφος, αποθήκευση, επεξεργασία και οπτικοποίηση των δεδομένων. Η υπολογιστική νέφους (Cloud Computing) είναι ένα καινούργιο επιχειρηματικό μοντέλο το οποίο επιτρέπει στις επιχειρήσεις την υιοθέτηση υπηρεσιών πληροφορικής χωρίς μεγάλο κόστος και επιπλέον την παροχή υπολογιστικών υπηρεσιών. Υπάρχουν πολλά μοντέλα υπολογιστικής νέφους, το δημόσιο, το ιδιωτικό και το υβριδικό.

Η χρήση του νέφους είναι αναγκαία, καθώς οι έξυπνες συσκευές έχουν συνήθως περιορισμένη ισχύ, αποθήκευση και υπολογιστικές ικανότητες. Γι αυτό, συνήθως στηρίζονται στα μεγάλα κέντρα δεδομένων του νέφους προκειμένου να διεξάγουν τη συλλογή ανάλογου τεράστιου αριθμού δεδομένων με μεγάλη ταχύτητα

και ακόμα να παρέχουν στον τελικό χρήστη πολλές υπηρεσίες και χαρακτηριστικά,όπως πρόσβαση, κλιμάκωση, φορητότητα, αποθήκευση και υπολογιστική με χαμηλό κόστος. Τα κέντρα δεδομένων (Datacenters) αποτελούν το βασικό σύστημα για τη διεξαγωγή των υπηρεσιών υπολογιστικής νέφους και αποτελούν εγκαταστάσεις οι οποίες φιλοξενούν έναν μεγάλο αριθμό διακομιστών που συνδέονται χρησιμοποιώντας δύο ή τρία επίπεδα διακοπτών. Τα κέντρα δεδομένων κατασκευάζονται και διαχειρίζονται από μεγάλες εταιρίες (Amazon, Microsoft κ.λ.π.). Ένα από τα βασικά χαρακτηριστικά των κέντρων δεδομένων, είναι η εικονικοποίηση διακομιστή με τη χρήση ενός επιπέδου εικονικοποίησης, που στοχεύει στον αποτελεσματικό διαμοιρασμό και απομόνωση των υπολογιστικών πόρων, έτσι ώστε να μπορούν να τρέχουν σε μία μόνο φυσική συσκευή πολλαπλά λειτουργικά συστήματα (Papadimitriou, χ.χ.).

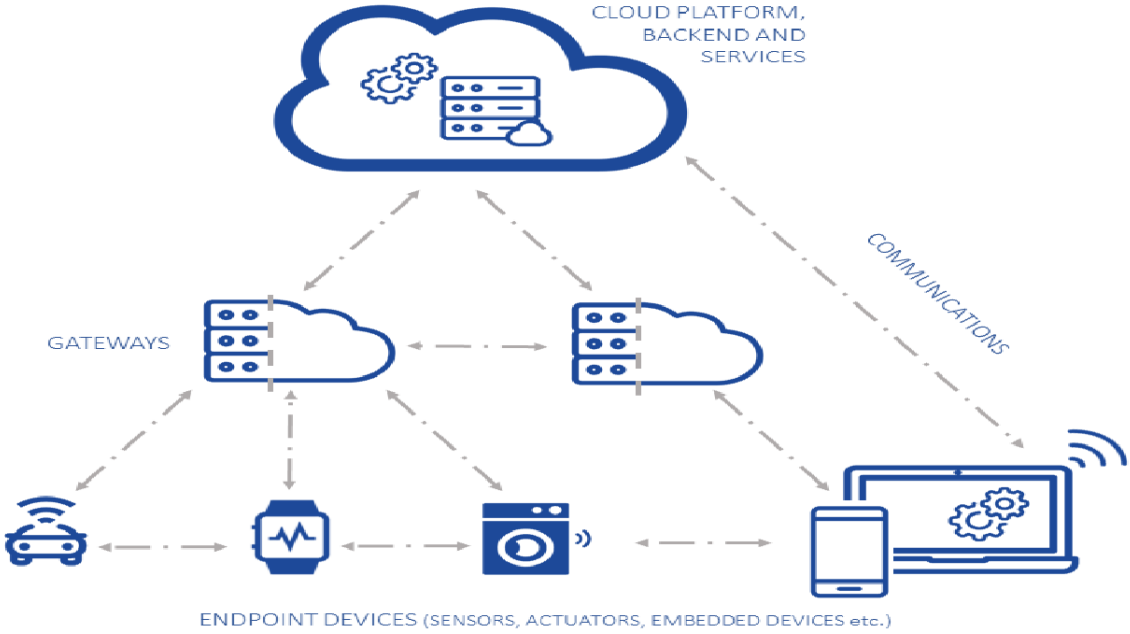
Η υπολογιστική νέφους έχει πολλά πλεονεκτήματα όπως καλή διαχείριση πόρων, δυνατότητα κλιμάκωσης (scalability), διαχείρισης δεδομένων μεγάλης κλίμακας και σύνδεσης από παντού. Επιπλέον χαρακτηριστικά της υπολογιστικής νέφους είναι η δυνατότητα χρήσης του νέφους ταυτόχρονα από πολλούς χρήστες και η ελαστικότητα. Η υπολογιστική νέφους παρέχει τέσσερεις κύριες κατηγορίες υπηρεσιών όπως Λογισμικό ως υπηρεσία (SaaS) που αφορά τις εφαρμογές του παρόχου που χρησιμοποιούνται από πολλούς χρήστες σε ένα σύστημα νέφους, Σύστημα ως υπηρεσία (PaaS) που αναφέρεται σε πλατφόρμα που χρησιμοποιείται για τη δημιουργία εφαρμογών με τη χρήση γλώσσας προγραμματισμού και βιβλιοθηκών, Δίκτυο ως υπηρεσία (NaaS) που παρέχει στους χρήστες το εικονικό (virtual) δίκτυο που ζητούν και Σύστημα ως υπηρεσία (IaaS) που παρέχει υπηρεσίες υπολογισμού, επεξεργασίας και αποθήκευσης στους χρήστες. Ωστόσο, όλες αυτές οι υπηρεσίες παρέχονται αφού τα ανεπεξέργαστα μεγάλα δεδομένα (raw data) φτάσουν στο νέφος, γεγονός που έχει επίπτωση στην ικανότητα σύνδεσης, στο ρυθμό μεταφοράς δεδομένων, στην επεξεργασία κλπ.



Εικόνα 36: Ενσωμάτωση νέφους με το Διαδίκτυο των Πραγμάτων (Mohammad Aazam, et al., 2015)

11.1. ΝΕΦΟΣ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (CoT)

Το νέφος των πραγμάτων (Cloud of Things) είναι ο συγκερασμός των δύο τεχνολογιών, του νέφους και του διαδικτύου των πραγμάτων, που παρέχει στους χρήστες απεριόριστες δυνατότητες σε ζωντανό χρόνο, όπως υπολογιστική και αποθήκευση των δεδομένων που παράγονται από τις έξυπνες συσκευές. Έτσι τα τελευταία χρόνια έχουν δημιουργηθεί διάφορες εφαρμογές όπως Βιντεοπαρακολούθηση ως υπηρεσία, Δεδομένα ως υπηρεσία, Ανίχνευση ως υπηρεσία κλπ (Syrine Sahmim & Hamza Gharsellaoui, 2017). Η αρχιτεκτονική του νέφους των πραγμάτων έχει απασχολήσει πολύ, λόγω της ετερογένειας τόσο του νέφους όσο και του διαδικτύου των πραγμάτων. Για την αντιμετώπιση αυτής συνήθως εισάγονται ενδιάμεσα επίπεδα πόρων τόσο από την πλευρά το νέφους όσο και από την πλευρά των πραγμάτων έτσι ώστε να διευκολυνθεί η αλληλεπίδραση των εφαρμογών (Ado Adamou Abba Ari, et al., 2019).



Εικόνα 37: Αρχιτεκτονική του Νέφους των Πραγμάτων (Skouloudi & Gema Fernández, 2018)

11.2. ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΝΕΦΟΥΣ

Σύμφωνα με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) (Skouloudi & Gema Fernández, 2018), τα ζητήματα ασφαλείας που προκύπτουν από την συγχώνευση του διαδικτύου των πραγμάτων με το νέφος κατατάσσονται σε τρείς κατηγορίες:

α. Ζητήματα διασύνδεσης, δηλαδή αλληλεπίδρασης και επικοινωνίας μεταξύ των τελικών σημείων, των θυρών και του νέφους.

β. Ζητήματα ανάλυσης, δηλαδή επεξεργασίας, φιλτραρίσματος και συγκέντρ ωσης των δεδομένων που προέρχονται από έξυπνες συσκευές διαφορετικών επιπέδων του συστήματος και

γ. Ζητήματα ενσωμάτωσης, δηλαδή συγκερασμού των χαρακτηριστικών εκείνων που επιτρέπουν την σε ζωντανό χρόνο αμφίδρομη ροή των δεδομένων (API s κ.λ.π).

Σε σχέση με τη διασύνδεση, τα ζητήματα ασφαλείας που ανακύπτουν σχετίζονται με τη μεγάλη ετερογένεια των συσκευών, των πρωτοκόλλων επικοινωνίας, των μηχανισμών και την έλλειψη κοινώς αποδεκτών προτύπων, με αποτέλεσμα τη μεγάλη διαφοροποίηση των αναγκών ασφαλείας σε κάθε επίπεδο και συσκευή. Επίσης, όταν η επεξεργασία των πληροφοριών γίνεται στην παρυφή (edge) και όχι στο

νέφος, δημιουργούνται ζητήματα διατήρησης της ιδιωτικότητας και απορρητότητας των δεδομένων κατά τη ροή τους στο νέφος, λόγω των περιορισμένων δυνατοτήτων επεξεργασίας και αποθήκευσης ορισμένων τελικών σημείων, που επηρρεάζουν τις ρυθμίσεις αυθεντικοποίησης, κρυπτογράφησης και ελέγχου πρόσβασης.

Σε σχέση με την ανάλυση, επειδή η επεξεργασία των δεδομένων πολλές φορές διενεργείται στην παρυφή (edge) σε πραγματικό χρόνο, επισκιάζεται η ασφάλεια, καθώς η παρυφή (edge) είναι πιο ευάλωτη σε επιθέσεις επειδή είναι υλικά προσβάσιμη, δεν μπορούν να εφαρμοστούν σε αυτή παραδοσιακές μέθοδοι ασφάλισης του νέφους και λόγω της αποκεντροποίησης των υπηρεσιών καθίσταται πιο περίπλοκη διαδικασία η εφαρμογή μηχανισμών ασφαλείας.

Σε σχέση με την ενσωμάτωση, τα ζητήματα ασφαλείας σχετίζονται με την έλλειψη εφαρμογής εκ κατασκευής από τους προγραμματιστές χαρακτηριστικών ασφαλείας, όπως αυθεντικοποίηση, κρυπτογράφηση κ.λ.π. Επίσης, δεν υπάρχουν συγκεκριμένες οδηγίες ανάπτυξης ασφαλούς έξυπνου υλικο-λογισμικού λόγω της ετερογένειας του συστήματος ενώ η χρήση απαρχαιωμένων συσκευών και η έλλειψη ενημερώσεων αποτελεί άλλο έναν σημαντικό παράγοντα ασφάλειας.

Τέλος, θα πρέπει να σημειωθεί ότι η μη ασφαλής επιφάνεια διεπαφής του νέφους το καθιστά ευάλωτο (Syed Rizvi, et al., 2020). Αυτό συσχετίζεται με την εφαρμογή μη ασφαλών πρωτοκόλλων που δεν επιτρέπουν τη σωστή κρυπτογράφηση (SSL), τη χρήση εφαρμογών με ασφάλεια, την εφαρμογή απαρίθμησης ταυτοποίησης λογαριασμού (Account enumeration) κ.λ.π. . (Ado Adamou Abba Ari, et al., 2019).

11.2.1. ΠΡΑΚΤΙΚΕΣ ΠΟΥ ΔΗΜΙΟΥΡΓΟΥΝ ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΝΕΦΩΝ.

Εκτός των προαναφερόμενων, πρακτικές που συμβάλλουν στη διακινδύνευση της ασφαλείας των νεφών [33]είναι :

α. Η αποτυχία εφαρμογής όλων των ρυθμίσεων ασφαλείας του νέφους (misconfiguration) η οποία παίζει κυρίαρχο ρόλο στην παραβίαση των δεδομένων νέφους. Αυτό σχετίζεται με το γεγονός ότι το νέφος είναι έτσι σχεδιασμένο ώστε να είναι εύχρηστο και να επιτρέπει τον εύκολο διαμοιρασμό δεδομένων, γεγονός που

[33] https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/# , (πρόσβαση ,15/03/2021)

καθιστά δύσκολο να διασφαλιστεί, ειδικά από τις επιχειρήσεις, ότι τα δεδομένα τους είναι προσβάσιμα μόνο από εξουσιοδοτημένα μέρη.

β. Οι οργανισμοί που χρησιμοποιούν υποδομή νέφους, δεν έχουν πλήρη έλεγχο της υποδομής τους αφού, δεν είναι εξοικειωμένοι με την δημιουργία ασφαλείας της υποδομής νέφους τους και για την ασφάλεια της υποδομής τους βασίζονται στους ελέγχους ασφαλείας του παρόχου νέφους (CSP).

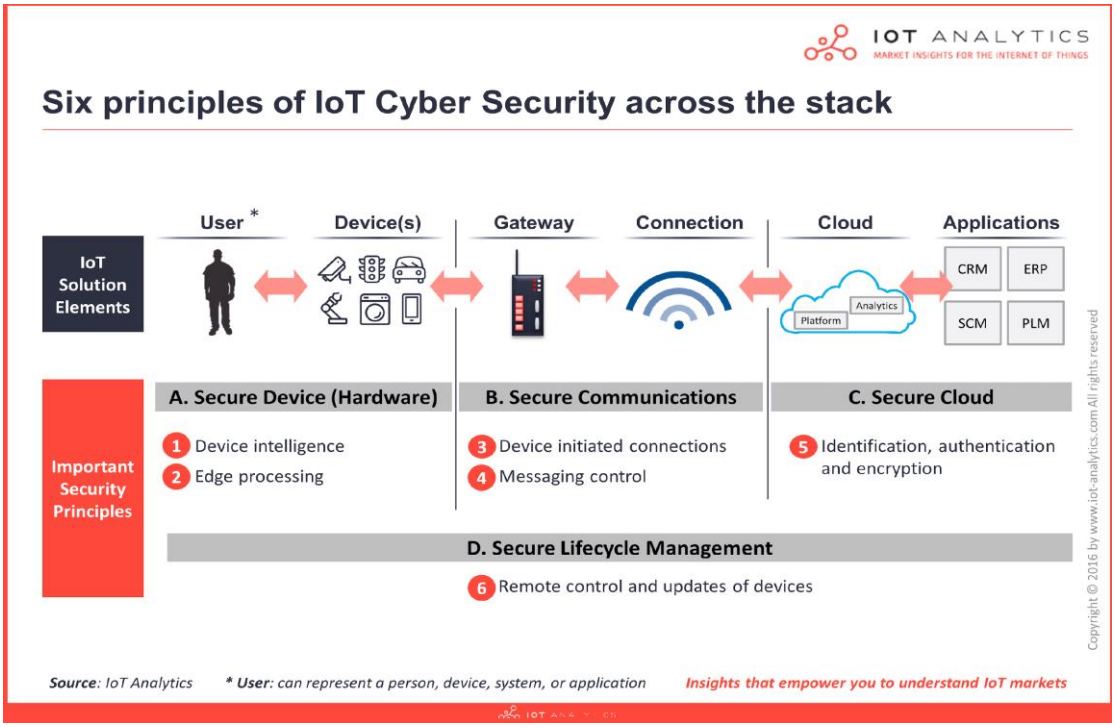
γ. Η μη εξουσιοδοτημένη πρόσβαση, που διευκολύνεται από το γεγονός ότι το μοντέλο ανάπτυξης νέφους, δηλαδή η διαμόρφωση παραμέτρων περιβάλλοντος (όπως η προσβασιμότητα και η ιδιοκτησία της υποδομής ανάπτυξης και του μεγέθους αποθήκευσης), είναι προσβάσιμο από το Δημόσιο Διαδίκτυο, γεγονός που το καθιστά μεν προσπελάσιμο από τους χρήστες, αλλά παράλληλα το καθιστά και εύκολο στόχο.

δ. Οι Διασυνδέσεις Προγραμματισμού Εφαρμογών (APIs) που παρέχονται από τους παρόχους υπηρεσιών νέφους, με σκοπό να διευκολύνουν την εφαρμογή από τους χρήστες, δημιουργούν ζητήματα ασφαλείας σε περίπτωση που οι χρήστες δεν έχουν ασφαλίσει αποτελεσματικά τις διασυνδέσεις τους και που οι οδηγίες που προορίζονται για τους πελάτες χρησιμοποιηθούν από επιτιθέμενους με σκοπό να αναγνωρίσουν και να έχουν πρόσβαση σε ευαίσθητα δεδομένα.

ε. Η οικειοποίηση συνδεδεμένων λογαριασμών, λόγω της χρήσης αδύναμων κωδικών είναι επίσης από τα πιο σοβαρά προβλήματα ασφαλείας των νεφών, καθώς αφενός οι οργανισμοί βασίζονται όλο και περισσότερο στη χρήση τους για τη διεκπεραίωση των βασικών εργασιών τους και αφετέρου αδυνατούν συνήθως να αναγνωρίσουν έγκαιρα και αποτελεσματικά αυτές τις απειλές.

Στ. Η αδυναμία από τους οργανισμούς να παρακολουθούν και να προστατεύουν τους πόρους τους που βρίσκονται στο νέφος, καθώς βρίσκονται εκτός του εργασιακού δικτύου, σε υποδομές που η επιχείρηση δεν κατέχει, με αποτέλεσμα τα παραδοσιακά εργαλεία ασφαλείας να μην έχουν καμία αποτελεσματικότητα.

ζ. Η δυνατότητα διαμοιρασμού δεδομένων που παρέχουν τα περισσότερα νέφη μέσω της πρόσκλησης για συνεργασία δια ηλεκτρονικού μηνύματος ή με διαμοιρασμό σύνδεσης που επιτρέπει κάθε έναν που διαθέτει τη διεύθυνση (URL) να έχει πρόσβαση σε αυτά, δημιουργεί μεγάλους κινδύνους καθώς είναι δύσκολο να γίνει έλεγχος των προσώπων που έχουν πρόσβαση. Αυτό συμβαίνει γιατί ο σύνδεσμος για παράδειγμα μπορεί να προωθηθεί περαιτέρω σε άλλους, να υποκλαπεί κλπ.



Εικόνα 38: Ασφάλεια Νέφους [34]

η. Σε ένα νέφος είναι πολύ πιο δύσκολος ο εντοπισμός των κακόβουλων χρηστών οι οποίοι ήδη έχουν εξουσιοδοτημένη πρόσβαση στο δίκτυο και σε ευαίσθητα δεδομένα και οι οποίοι στην προσπάθειά τους να αποκτήσουν μεγαλύτερη πρόσβαση αφήνουν έκθετο έναν οργανισμό σε περισσότερους επιτιθέμενους, καθώς τα νέφη είναι προσβάσιμα και από δημόσια και ανοιχτή σύνδεση.

Συνοψίζοντας, από όλα τα ανωτέρω προκύπτει, ότι οι μεγαλύτεροι κίνδυνοι από τη χρήση του νέφους είναι η απώλεια ή διαρροή πληροφοριών που σχετίζεται κυρίως με την πρόσβαση σε αυτά μέσω ανοιχτού/δημόσιου διαδικτύου και με την έλλειψη γνώσης σωστού διαχειρισμού τους με εχέγγυα ασφαλείας. Τέλος, λόγω του γεγονότος ότι οι οργανισμοί έχουν έλεγχο και ορατότητα των νεφών σε ορισμένα μόνο επίπεδα αυτών είναι δύσκολη τόσο η διεξαγωγή ελέγχων ασφαλείας όσο και η προστασία της επεξεργασίας και αποθήκευσης των δεδομένων με τους υπάρχοντες κανονισμούς και νόμους.

[34] https://iot-analytics.com/understanding-iot-cyber-security-part-2/, (πρόσβαση, 29/03/2021)

Εικόνα 39: Προκλήσεις Ασφαλείτας του Νέφους των Πραγμάτων (Ado Adamou Abba Ari, et al., 2019)

11.2.2. ΚΥΡΙΟΤΗΤΑ,ΑΠΟΘΗΚΕΥΣΗ ΚΑΙ ΕΛΕΓΧΟΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΝΕΦΟΣ

Οι οργανισμοί που αποθηκεύουν τα δεδομένα τους σε νέφη, συνήθως δεν γνωρίζουν που ακριβώς αυτά είναι αποθηκευμένα. Και αυτό γιατί οι πάροχοι νεφών συνήθως διαθέτουν διάφορα γεωγραφικώς διαμοιρασμένα κέντρα δεδομένων. Αυτό έχει ως στόχο να διευκολύνει την προσβασιμότητα και εκτέλεση των εργασιών και επιτρέπει στους παρόχους τη διασφάλιση της ακώλυτης χρήσης των υπηρεσιών. Όμως, αυτή η πρακτική δημιουργεί εκτός των άλλων σύγχυση σε σχέση με τη δικαιοδοσία και τους νόμους για την προστασία των δεδομένων, έχοντας επίπτωση με τη σειρά της στην ιδιωτικότητα και ασφάλεια των δεδομένων [35].

11.3. ΕΠΙΘΕΣΕΙΣ ΚΑΤΑ ΤΟΥ ΝΕΦΟΥΣ

Οι επιθέσεις που σχετίζονται με το νέφος, γίνονται είτε κατά τη μεταφορά των δεδομένων είτε εντός του νέφους.

α. Οι επιθέσεις που γίνονται κατά τη μεταφορά των μηνυμάτων είναι οι γνωστές επιθέσεις της λαθρακοής (eavesdropping), της χειραγώγησης μηνυμάτων, της εισόδου μηνυμάτων και των επιθέσεων επανάληψης.

[35] https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/#, (πρόσβαση,15/02/2021)

β. Οι επιθέσεις εντός του νέφους, μπορεί να προέρχονται είτε από πρακτικές που χρησιμοποιούν μη έμπιστοι πάροχοι νέφους, είτε από επιθέσεις από ανταγωνιστές (Papadimitriou, χ.χ.).

β.1. Οι πρακτικές που ακολουθούν οι μη έμπιστοι πάροχοι νέφους και οι οποίες μπορούν να οδηγήσουν σε παραβιάσεις, είναι αρχικά η δημιουργία πολλών αντιγράφων δεδομένων τα οποία παραμένουν στο σύστημα ακόμα και μετά τον τερματισμό μίας υπηρεσίας νέφους. Δεύτερον, ορισμένοι πάροχοι εκμεταλλεύονται την αναλυτική και της εξόρυξη δεδομένων με στόχο την αύξηση του εμπορικού τους κέρδους είτε μέσω της αξιοποίησης από τους ίδιους των δεδομένων είτε μέσω της πώλησής τους σε μη εξουσιοδοτημένα μέρη. Τέλος, οι πάροχοι μπορούν να προβαίνουν σε καταγραφή της δραστηριότητας των χρηστών εντός του νέφους χωρίς τη συναίνεσή τους.

β.2. Οι πιο γνωστές επιθέσεις των ανταγωνιστών-εισβολέων είναι:

- Οι επιθέσεις υπευθύνου (Hypervisor Attacks), οι οποίες επιτρέπουν την απόκτηση ελέγχου σε όλες τις εικονικές μηχανές και δεδομένα που υπάρχουν σε έναν συγκεκριμένο διακομιστή νέφους, με την εκμετάλλευση όλων των ευπαθειών του υπευθύνου.
- Η επίθεση αλλαγής τοποθεσίας (Placement locality) είναι η τοποθέτηση μεγάλου αριθμού εικονικών μηχανών στον ίδιο κεντρικό διακομιστή με την εικονική μηχανή-στόχο.

Τέλος, η εσφαλμένη διαμόρφωση δικτύου (network misconfiguration) η οποία στο νέφος σχετίζεται με την εσφαλμένη διαμόρφωση των εικονικών διακοπτών από τον κεντρικό χειριστή δικτύου, μπορεί να προσφέρει το περιθώριο σε ανταγωνιστές να επιτρέψουν την επικοινωνία μεταξύ εικονικών μηχανών διαφορετικών κεντρικών διακομιστών.

11.3.1. ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΖΗΤΗΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΝΕΦΟΥΣ

Λύσεις (Skouloudi & Gema Fernández, 2018) για την αντιμετώπιση των κινδύνων που δημιουργούνται κατά τη διασύνδεση μπορεί αρχικά να προσφέρει η εικονικοποίηση (virtualization) των πόρων, δηλαδή η χρήση ενός μηχανισμού αφαίρεσης,στοχευμένου στην απόκρυψη των λεπτομερειών της υλοποίησης και της κατάστασης των πόρων από τους χρήστες προκειμένου να επιτευχθεί ομογενοποίηση, δηλαδή όλοι οι πόροι να συμπεριφέρονται ως ένας.

Δεύτερον, η ασφάλεια των επικοινωνιών, των ροών της ανάλυσης δεδομένων και των αποθηκευμένων δεδομένων μπορεί να επιτευχθεί με την κατηγοριοποίηση των μεταφερόμενων δεδομένων και τη χρήση της κρυπτογράφησης τόσο κατά τη μεταφορά όσο και κατά την αποθήκευση. Επίσης, με τη χρήση τεχνικών φιλτραρίσματος και διαχείρισης των δεδομένων στην παρυφή (edge) μπορεί να γίνεται έλεγχος ασφαλείας των δεδομένων σε πρώιμο στάδιο και έτσι να διασφαλίζεται εκ των προτέρων η ροή προς το νέφος.

Τρίτον στο επίπεδο της ανάλυσης, η σκλήρυνση (hardening) των τελικών σημείων, με ανανέωση των κωδικών, την αποστολή αναφορών αποτυχίας στο νέφος ή την κατηγοριοποίηση, διασφαλίζει το σύστημα από επιθέσεις.

Τέταρτον, στο επίπεδο της ενσωμάτωσης, η ασφάλεια θα μπορούσε να επιτευχθεί με την εισαγωγή νέων ενδιάμεσων επιπέδων, όπως ασφαλών συσκευών, δρομολογητών και θυρών με σκοπό την επίτευξη περισσότερου ελέγχου και άρα ασφάλεια στο επίπεδο παρυφών (edge) αλλά και στο επίπεδο νέφους (θύρα API).

Τέλος, η δημιουργία ενιαίων προτύπων ασφαλείας, οι διαρκείς ενημερώσεις και η ασφάλεια από άκρο σε άκρο του συστήματος κρίνεται αναγκαία σε όλα τα επίπεδα του νέφους.

12. ΔΕΔΟΜΕΝΑ ΜΕΓΑΛΗΣ ΚΛΙΜΑΚΑΣ (BIG DATA)

Τα δεδομένα μεγάλης κλίμακας στο διαδίκτυο των πραγμάτων σχετίζονται με την επεξεργασία μεγάλου αριθμού δεδομένων σε πραγματικό χρόνο καθώς και με την αποθήκευσή τους χρησιμοποιώντας έναν μεγάλο αριθμό τεχνολογιών. Τα χαρακτηριστικά των δεδομένων μεγάλης κλίμακας είναι ο μεγάλος όγκος τους λόγω της διαρκούς συλλογής στα έξυπνα δίκτυα, η ποικιλία τους (βάσεις δεδομένων, κείμενα, βίντεο, φωτογραφίες κλπ), η ταχύτητα παραγωγής και επεξεργασίας τους, η ποικιλομορφία τους, δηλαδή ακόμα και η αντιφατικότητά τους σε περιόδους αιχμής και τέλος η πολυπλοκότητά τους λόγω της προέλευσής τους από διαφορετικές πηγές.

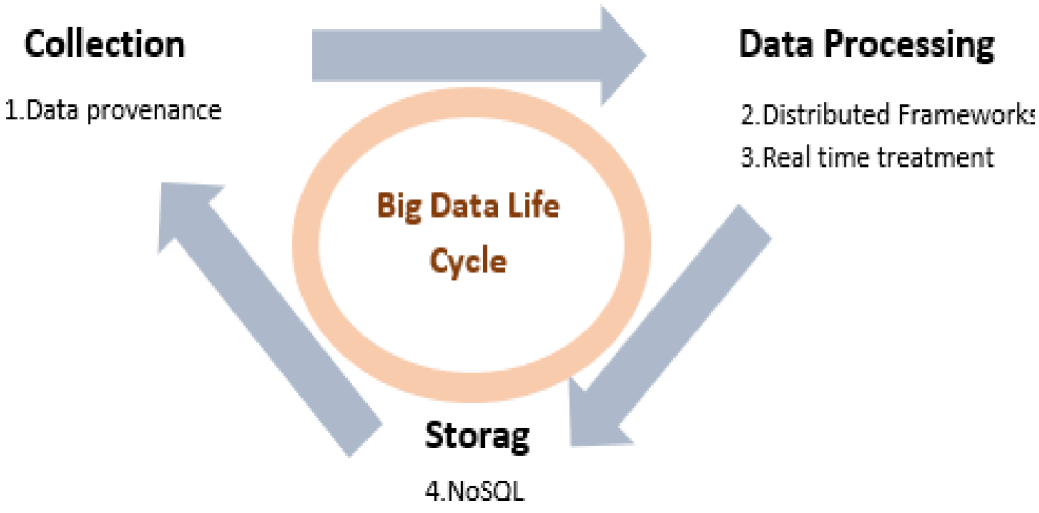
12.1. ΕΠΕΞΕΡΓΑΣΙΑ ΚΑΙ ΑΝΑΛΥΣΗ

Τα δεδομένα πρέπει να συνδεθούν, συνδυαστούν, καθαριστούν και μεταμορφωθούν σε κατάλληλη μορφή προτού υποστούν επεξεργασία (Hammood, 2016). Η αναλυτική των δεδομένων μεγάλης κλίμακας παίζει ουσιώδη ρόλο καθώς πρόκειται για τη διαδικασία ανάλυσης μεγάλου αριθμού δεδομένων με στόχο την αναγνώριση κρυμμένων μοτίβων,

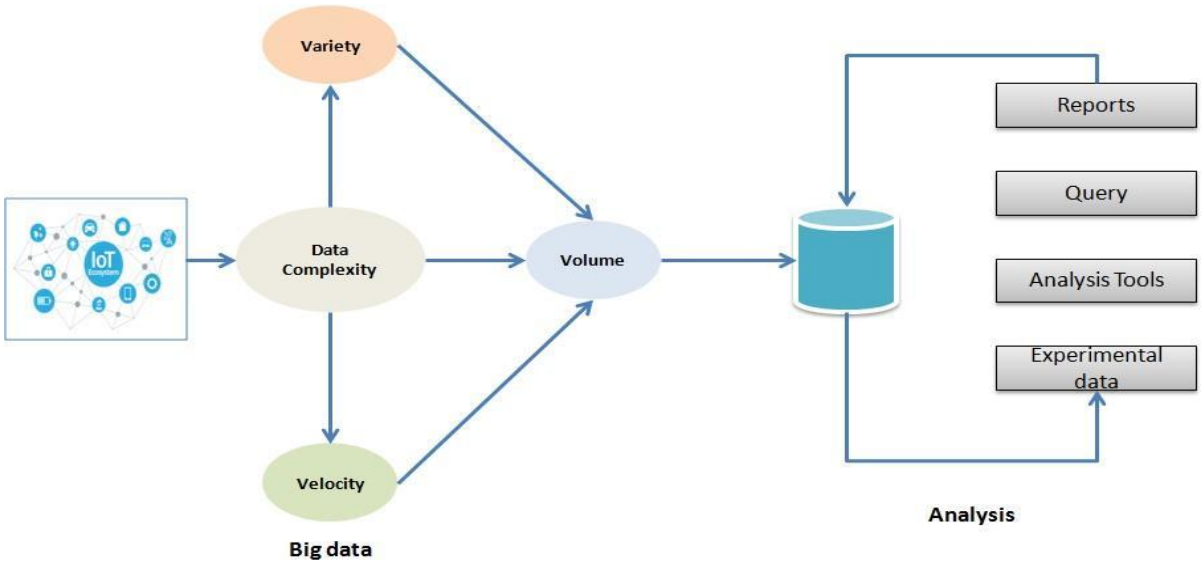
άγνωστων συσχετίσεων, τάσεων της αγοράς, προτιμήσεις καταναλωτών και άλλων χρήσιμων πληροφοριών.

Η διαδικασία επεξεργασίας των δεδομένων μεγάλης κλίμακας στο διαδίκτυο των πραγμάτων ξεκινά με τη συλλογή μη δομημένων δεδομένων από τις διασυνδεδεμένες έξυπνες συσκευές. Τα δεδομένα μεγάλης κλίμακας που συλλέγονται εξαρτώνται από τρείς παράγοντες, τον όγκο, την ταχύτητα και την ποικιλία. Στη συνέ χεια, αφού αποθηκευτούν σε μεγάλους φακέλους δεδομένων, αναλύονται με τη χρήση διάφορων εργαλείων και παράγουν αναφορές των επεγεργασμένων δεδομένων.

Οι συσκευές στέλνουν τα δεδομένα σε πύλες που τα φιλτράρουν μειώνοντας τον όγκο των μεταφερόμενων δεδομένων στο επόμενο στάδιο. Με τη χρήση της αναλυτικής γίνεται μία γρήγορη αναγνώριση χρήσιμων μοτίβων που ευρέθησαν νωρίτερα στο νέφος. Η πύλη του νέφους είναι αναγκαία για να γίνει μετάφραση πρωτοκόλλου και επικοινωνία μεταξύ των πρωτοκόλλων δεδομένων, ενώ ασφαλίζει και τη μεταφορά δεδομένων μεταξύ πύλης και κεντρικού διακομιστή του έξυπνου δικτύου.



Εικόνα 40: Κύκλος των Δεδομένων Μεγάλης Κλίμακας (Ibtissame KANDROUCH, et al., October 29 – November 1, 2018)



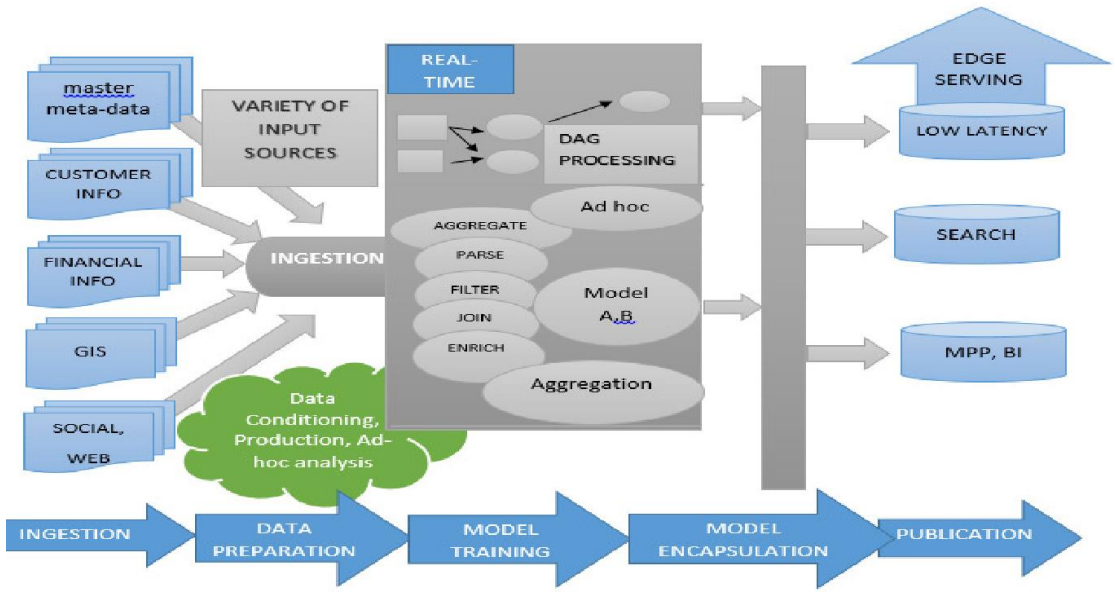
Εικόνα 41: Διαδικασία Επεξεργασίας των Δεδομένων Μεγάλης Κλίμακας στο Έξυπνο Δίκτυο[36]

12.2. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕΓΑΛΗΣ ΚΛΙΜΑΚΑΣ

Στην αρχιτεκτονική των δεδομένων μεγάλης κλίμακας, τα δεδομένα τμηματοποιούνται, αντιγράφονται και διανέμονται ανάμεσα σε χιλιάδες κόμβους. Πολύ σημαντικό χαρακτηριστικό της αρχιτεκτονικής των δεδομένων μεγάλης κλίμακας είναι η αυτοματοποιημένη κλιμακωτή αποθήκευση (auto-tiering storage), δηλαδή ένα λογισμικό διαχείρισης της αποθήκευσης με τη χρήση πίνακα δίσκων που εμπεριέχει έναν τεράστιο αριθμό δεδομένων και τα διαχειρίζεται εξασφαλίζοντας χώρο, αποτελεσματική εκτέλεση και μείωση κόστους. Για λόγους εκτέλεσης, τα δεδομένα τμηματοποιούνται σε ζεστά, δηλαδή σε αυτά που χρησιμοποιούνται συχνά για ανάλυση και στα υπόλοιπα που θεωρούνται κρύα.

Εκτός των ανωτέρω, η μοντέρνα αρχιτεκτονική υποστηρίζει την υπολογιστική σε ζωντανό χρόνο (real time analytics), δηλαδή την συλλογή μεγάλων ποσοτήτων δεδομένων από διάφορες πηγές, τα οποία στη συνέχεια φιλτράρονται, αναλύονται μέσω εξόρυξης δεδομένων, ταξινόμησης και αλγορίθμων πρόβλεψης και διατηρούνται ως αναφορές με σκοπό να αξιοποιηθούν για τη λήψη αποφάσεων από τις επιχειρήσεις. Τέλος, άλλα πολύ σημαντικά χαρακτηριστικά των δεδομένων μεγάλης κλίμακας είναι η υποστήριξη εντολών/ερωτημάτων των οποίων το αποτέλεσμα εξαρτάται από κάποια μεταβλητή (ad-hoc queries) και ο δυναμικός και μαζικός από πολλούς επεξεργαστές προγραμματισμό (Vaibhav Hans & Neelu J.Ahuja, 2016).

[36] https://www.whizlabs.com/blog/iot-and-big-data/, (πρόσβαση, 02/03/2021)



Εικόνα 42: Συνεχής Υπολογιστική των Δεδομένων Μεγάλης Κλίμακας (Vaibhav Hans & Neelu J.Ahuja, 2016)

12.3.ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ ΜΕΓΑΛΗΣ ΚΛΙΜΑΚΑΣ

Η ασφάλεια των δεδομένων μεγάλης κλίμακας αφορά όλα τα μέτρα και εργαλεία που χρησιμοποιούνται για την προστασία των δεδομένων και των διαδικασιών ανάλυσης από επιθέσεις, κλοπές ή άλλες κακόβουλες ενέργειες. Οι μηχανισμοί ασφαλείας στην τεχνολογία των δεδομένων μεγάλης κλίμακας είναι γενικά αδύναμοι, καθώς τα ίδια τα χαρακτηριστικά αυτής της τεχνολογίας δημιουργούν μεγάλα ρίσκα ασφαλείας (Vaibhav Hans & Neelu J.Ahuja, 2016).

Συγκεκριμένα, η μη ασφαλής υπολογιστική με τη χρήση μη έμπιστων υπολογιστικών προγραμμάτων μπορεί να οδηγήσει σε δημοσιοποίηση ευαίσθητων δεδομένων ή σε αλλοίωσή τους που με τη σειρά της οδηγεί σε εξαγωγή λανθασμένων προβλέψεων ή αναλύσεων καθώς και σε άρνηση υπηρεσίας (DoS). Η αδυναμία αξιολόγησης και φιλτραρίσματος των δεδομένων λόγω του τεράστιου αριθμού που συλλέγονται από πολλές πηγές και η συνεχής ροή τους είναι άλλη μία αδυναμία αυτής της τεχνολογίας. Επίσης, υπάρχει αδυναμία ελέγχου πρόσβασης σε επίπεδο μεγάλων δεδομένων ενώ με τη χρήση εντολών/ερωτημάτων των οποίων το αποτέλεσμα εξαρτάται από κάποια μεταβλητή (ad-hoc queries) είναι δυνατή η απόκτηση πρόσβασης σε ευαίσθητες πληροφορίες.

Υπάρχει ζήτημα και με την αποθήκευση των δεδομένων σε αυτή την τεχνολογία η οποία είναι μη ασφαλής, καθώς η κρυπτογράφηση δεδομένων σε ζωντανό

χρόνο μπορεί να επηρεάσει την εκτέλεση των εργασιών αποθήκευσης, τα κρύα δεδομένα μεταφέρονται σε μη ασφαλή επίπεδα του πίνακα δίσκων και η ασφαλής επικοινωνία μεταξύ κόμβων, ενδιάμεσων επιπέδων και τελικών χρηστών είναι απενεργοποιημένη εκ κατασκευής. Τέλος, η ίδια η εξόρυξη δεδομένων και αναλυτική προϋποθέτουν παραβίαση της ιδιωτικότητας και μη συνειδητή αποθήκευση δεδομένων.

Σύμφωνα με (Gayatri Kapil, et al., 2020) τα ζητήματα ασφαλείας των δεδομένων μεγάλης κλίμακας οφείλονται στο ότι :

α. Τα περισσότερα παράλληλα και κατανεμημένα υπολογιστικά συστήματα, έχουν μόνο ένα επίπεδο προστασίας.

β. Είναι διαρκώς αυξανόμενη η χρήση μη σχεσιακών βάσεων δεδομένων (NOSQL) .

γ. Η αυτόματη μεταφορά δεδομένων απαιτεί πρόσθετα μέτρα ασφαλείας, τα οποία όμως δεν είναι διαθέσιμα.

δ. Τα συστήματα συνήθως δεν μπορούν να είναι αξιόπιστα και ακριβή όταν λαμβάνουν τεράστιες ποσότητες δεδομένων.

ε. Η χρήση τεχνικών εξόρυξης δεδομένων από ειδικούς πληροφορικής, μπορεί να οδηγήσει στη συλλογή ευαίσθητων προσωπικών δεδομένων των χρηστών, χωρίς την ενημέρωση ή συγκατάθεσή τους.

στ. Η διενέργεια ενδεικνυόμενων λεπτομερών ελέγχων δεν πραγματοποιούνται στα δεδομένα μεγάλης κλίμακας, λόγω του τεράστιου όγκου πληροφοριών.

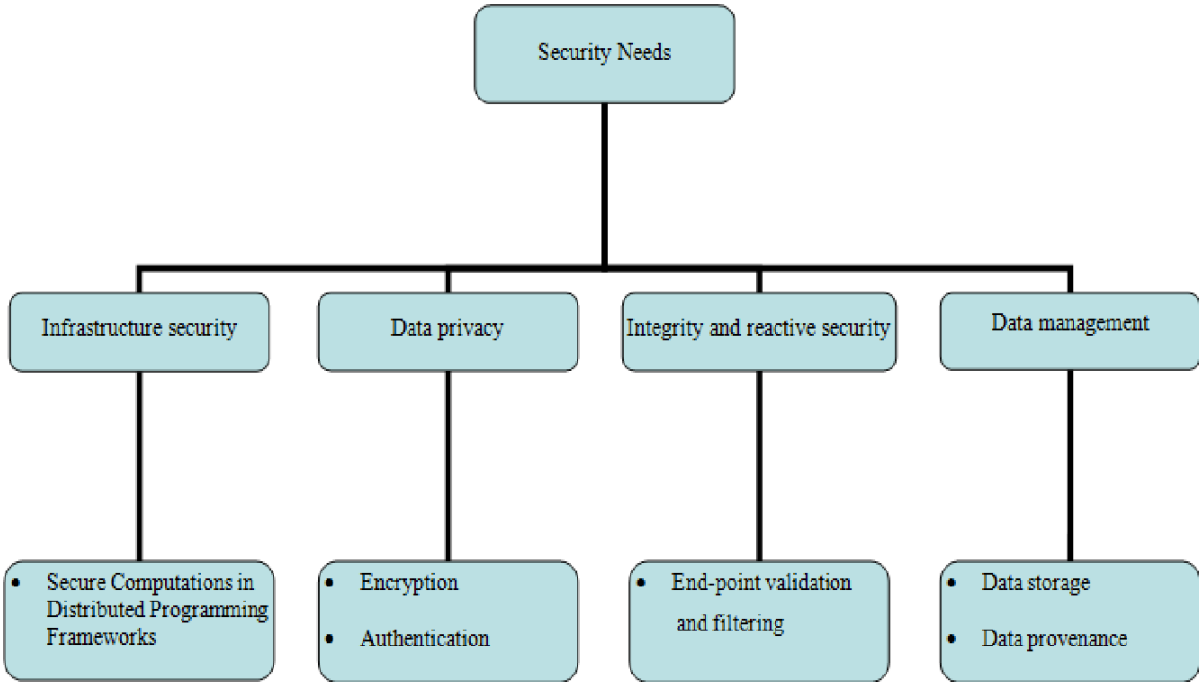
ζ. Λόγω του μεγάλου μεγέθους των δεδομένων, η προέλευσή τους δεν εντοπίζεται.

η. Τα δεδομένα μεγάλης κλίμακας αποθηκεύονται σε διάφορους κόμβους που ανήκουν σε πολλά συμπλέγματα υπολογιστών (clusters) και είναι διασκορπισμένα σε όλο τον κόσμο. Η επικοινωνία μεταξύ κόμβων και συμπλεγμάτων ασφαλίζεται μέσα από τα συνηθισμένα δημόσια και ιδιωτικά δίκτυα. Όμως, εάν αλλοιωθεί η ενδοεπικοινωνία μεταξύ κόμβων και συμπλεγμάτων από κάποιον εισβολέα είναι εύκολο να ανακτηθούν πολύτιμες πληροφορίες. Γι αυτό τον λόγο θα πρέπει να υιοθετηθούν νέα ασφαλή πρωτόκολλα δικτύου με στόχο την προστασία των διασυνδέσεων μεταξύ των μερών. Επίσης, πολύ σημαντική είναι η ανάπτυξη αξιόπιστων αλγορίθμων κρυπτογράφησης.

12.3.1. ΠΡΑΚΤΙΚΕΣ ΠΟΥ ΔΗΜΙΟΥΡΓΟΥΝ ΚΙΝΔΥΝΟΥΣ

Εκτός όλων των ανωτέρω, οι κίνδυνοι ασφαλείας στα δεδομένα μεγάλης κλίμακας οφείλονται σε πολύ μεγάλο βαθμό και στο γεγονός ότι τα δεδομένα δεν αποθηκεύονται πλέον σε φυσικές τοποθεσίες αλλά σε αποθήκες-νέφη, τα οποία είναι εύκολα προσβάσιμα από εισβολείς, επειδή συνήθως προσφέρουν προστασία σε ένα μόνο επίπεδο. Επιπλέον, δεδομένου ότι οι χρήστες δεν έχουν την γνώση να ελέγχουν τον μεγάλο όγκο των δεδομένων, αποτελούν εύκολο στόχο για παραβίαση. [37]

Άλλοι κίνδυνοι που δημιουργούνται, είναι όταν πριν την ανάλυση των δεδομένων δεν διασφαλίζεται η σωστή λειτουργία του έξυπνου δικτύου, όπως ενδεικτικά όταν τα συλλεχθέντα δεδομένα είναι αναξιόπιστα και δεν γίνεται σωστή επεξεργασία τους με αποτέλεσμα να μην επιλέγονται τα σωστά προς αποθήκευση. Τέλος, κίνδυνοι δημιουργούνται και από την απόκτηση πρόσβασης από εισβολείς στα κέντρα δεδομένων των παρόχων, στις συσκευές, σε κλοπή δεδομένων από διαχειριστές τηλεπικοινωνιών κλπ.



Εικόνα 43: Ανάγκες Ασφαλείας των Δεδομένων Μεγάλης Κλίμακας (Ibtissame KANDROUCH, et al., October 29 – November 1, 2018)

[37] https://datafloq.com/read/why-your-big-data-iot-security-are-vulnerable/2169, (πρόσβαση, 05/03/2021)

Συνεπώς, βάσει των ανωτέρω η ανάγκη ασφαλούς χρήσης της τεχνολογίας των δεδομένων μεγάλης κλίμακας, απαιτεί τη διασφάλιση ασφαλούς υπολογιστικής στα κατανεμημένα συστήματα προγραμματισμού, το φιλτράρισμα και τον έλεγχο εγκυρότητας των τελικών σημείων, την ασφάλεια του ίδιου του νέφους, την παρακολούθηση της κίνησης του δικτύου με στόχο την έγκαιρη ανίχνευση εισβολών και τον λεπτομερή έλεγχο της εφαρμογής των πολιτικών προστασίας. Επίσης, η ανωνυμοποίηση, η διαχείριση κλειδιού, η κρυπτογράφηση, αυθεντικοποίηση και η προστασία της επεξεργασίας δεδομένων σε ζωντανό χρόνο είναι αναγκαία.

13. ΕΞΟΡΥΞΗ ΔΕΔΟΜΕΝΩΝ (DATA MINING) ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

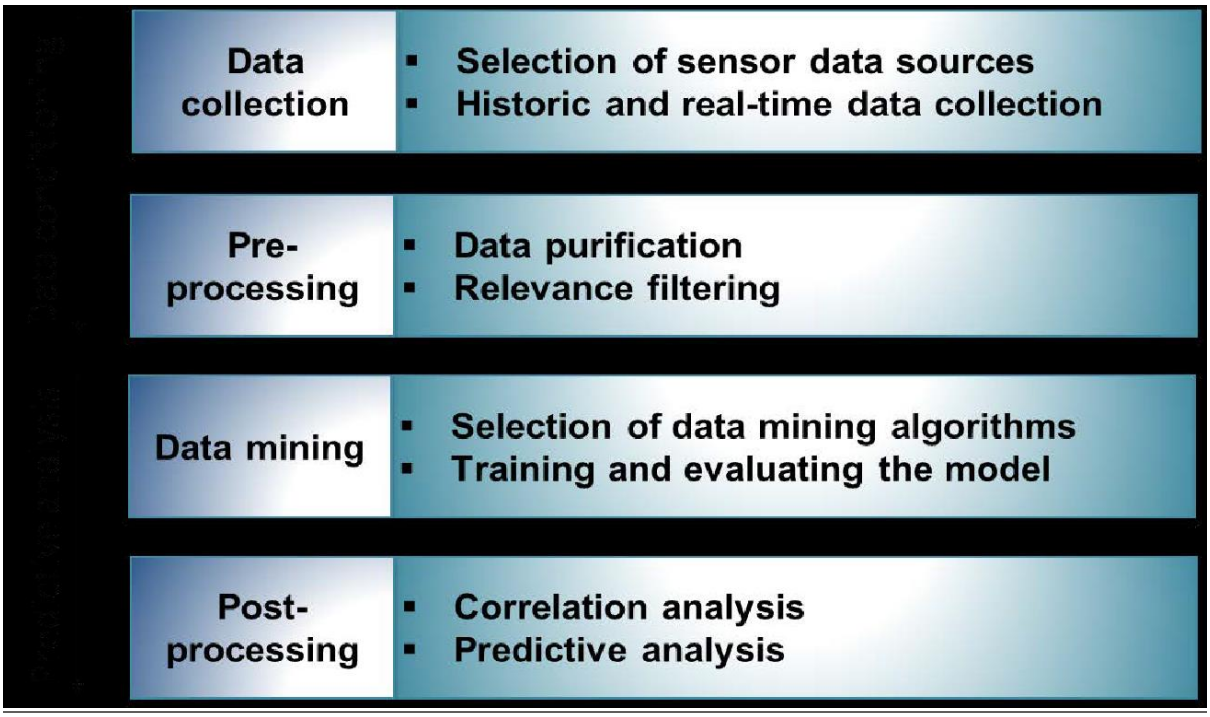
Η εξόρυξη δεδομένων είναι ένας διεπιστημονικός τομέας της επιστήμης των υπολογιστών και των στατιστικών με συνολικό στόχο την εξαγωγή πληροφοριών (με έξυπνες μεθόδους) από ένα σύνολο δεδομένων και τη μετατροπή των πληροφοριών σε κατανοητή δομή για περαιτέρω χρήση. Η διαφορά μεταξύ ανάλυσης δεδομένων και εξόρυξης δεδομένων είναι ότι η ανάλυση δεδομένων χρησιμοποιείται για τη δοκιμή μοντέλων και υποθέσεων στο σύνολο δεδομένων, όπως ανάλυση της αποτελεσματικότητας μιας καμπάνιας μάρκετινγκ, ανεξάρτητα από την ποσότητα των δεδομένων. Αντίθετα, η εξόρυξη δεδομένων χρησιμοποιεί μηχανική εκμάθηση (Machine learning) και στατιστικά μοντέλα για να αποκαλύψει κρυφά ή κρυμμένα μοτίβα σε μεγάλο όγκο δεδομένων.[38]

13.1. ΔΙΑΔΙΚΑΣΙΑ

Για την εξόρυξη δεδομένων ακολουθείται η εξής διαδικασία: Αρχικά γίνεται μία προεπεξεργασία των δεδομένων με τη συλλογή, επιλογή και ενσωμάτωση των δεδομένων, τα οποία αποστέλλονται είτε σε μία πλατφόρμα νέφους είτε σε μία ομίχλη για ανάλυση και αποθήκευση. Εν συνεχεία, αυτά τα δεδομένα διαμορφώνονται σε μορφή κατάλληλη για εξόρυξη μέσω καθαρισμού, φιλτραρίσματος, αντιγραφής, ανίχνευσης ανωμαλιών, ανάλυσης οντοτήτων και επιλογής χαρακτηριστικών. Τέλος, ακολουθεί η εξόρυξη δεδομένων η οποία ακολουθεί και σχετίζεται με την εφαρμογή έξυπνων μεθόδων για την εξαγωγή μοτίβων δεδομένων. Τέλος, γίνεται αξιολόγηση των

[38] https://en.wikipedia.org/wiki/Data_mining (πρόσβαση 18/03/2021).

σημαντικότερων μοτίβων και η παρουσίασή τους με τρόπο κατανοητό (LEI XU, et al., 2014).



Εικόνα 44: Βήματα Εξόρυξης Δεδομένων στο Έξυπνο Δίκτυο (Peter Wlodarczak, et al., 2017)

13.2. ΚΑΤΑΛΛΗΛΕΣ ΤΕΧΝΙΚΕΣ ΕΞΟΡΥΞΗΣ ΔΕΔΟΜΕΝΩΝ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Δεδομένης της ετερογένειας και της συνεχούς προσαρμοστικότητας του έξυπνου δικτύου κατά την εξόρυξη δεδομένων, πρέπει να εφαρμόζονται οι κατάλληλες τεχνικές, καθώς συνεχώς είτε μπορεί να προστίθενται νέες συσκευές, είτε ορισμένες από αυτές μπορει να διακόψουν την αποστολή δεδομένων λόγω προβλημάτων μπαταρίας, λόγω διακοπής σύνδεσης κλπ.

Μία από αυτές τις τεχνικές είναι η μηχανική μάθηση (machine learning), η οποία σύμφωνα με τον Άρθουρ Σάμουελ ορίζεται ως «*Πεδίο μελέτης που δίνει στους υπολογιστές την ικανότητα να μαθαίνουν,χωρίς να έχουν ρητά προγραμματιστεί».* Η μηχανική μάθηση διερευνά τη μελέτη και την κατασκευή αλγορίθμων που μπορούν να μαθαίνουν από τα δεδομένα και να κάνουν προβλέψεις σχετικά με αυτά. Παραδείγματα εφαρμογών αποτελούν τα φίλτρα ενοχλητικής αλληλογραφίας (spam

filtering), η οπτική αναγνώριση χαρακτήρων (OCR), οι μηχανές αναζήτησης και η υπολογιστική όραση [39] (Peter Wlodarczak, et al., 2017).

Αυτή η τεχνική χρησιμοποιείται προκειμένου η εξόρυξη δεδομένων να προσαρμόζεται στις συνεχείς αλλαγές στο έξυπνο περιβάλλον και να διαχειρίζεται τα ασαφή δεδομένα. Εφαρμόζεται ειδικά όταν οι κανόνες γίνονται περίπλοκοι ή πρέπει να δημιουργηθούν από τον προγραμματιστή πολλοί κανόνες. Αποτελεί παρακλάδι της Τεχνητής Νοημοσύνης και στοχεύει στο να εφαρμόσει την ανθρώπινη μάθηση στον υπολογισμό χωρίς να υπάρχει ανάγκη διεξοδικού προγραμματισμού.

Βασικά χαρακτηριστικά αυτής της τεχνικής που την καθιστούν κατάλληλη στην εξόρυξη δεδομένων είναι η ικανότητα να μαθαίνει τους κανόνες της εξόρυξης από το ιστορικό των δεδομένων μέχρι εκείνη τη στιγμή, η ικανότητα εκμάθησης και νέων κανόνων (πχ. με την είσοδο νέας συσκευής) και η ικανότητα να υπολογίζει πιθανότητες για μελλοντικά γεγονότα μέσα από ιστορικά δεδομένα χωρίς να επηρεάζεται από μικρές αλλαγές στη ροή πληροφοριών.

13.3. ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΕΞΟΡΥΞΗΣ ΔΕΔΟΜΕΝΩΝ

Μία από τις σπουδαιότερες προκλήσεις που σχετίζεται με τα δεδομένα μεγάλης κλίμακας και το διαδίκτυο των πραγμάτων, είναι η εξαγωγή των χρήσιμων πληροφοριών από έναν τεράστιο όγκο δεδομένων με ταυτόχρονη επίτευξη της ασφάλειας και ιδιωτικότητας αυτών. Η ιδιαιτερότητα όμως του έξυπνου δικτύου απαιτεί γρήγορες και αποτελεσματικές τεχνικές εξόρυξης δεδομένων λόγω της συνεχούς παραγωγής τεράστιου όγκου πληροφοριών ακόμα και μέσα από δεδομένα ιστοσελίδων, τον συγκερασμό ετερογενών, αβέβαιων, ασαφών,ανοκλήρωτων, δομημένων και μη πηγών και τύπων δεδομένων, την επικοινωνία διαφορετικών τύπων συσκευών και συστημάτων, την υποχρέωση εξαγωγής πολύπλοκων πληροφοριών και συμπερασμάτων μετά από συσχετισμό μεταξύ τους. Επιπλέον, υπάρχει ανάγκη ανάπτυξης αποτελεσματικών δομών εξόρυξης δεδομένων που να υπηρετούν την ασφάλεια και ιδιωτικότητα των δεδομένων μεγάλης κλίμακας καθώς και τον διαμοιρασμό τους. (Deepti & Nasib Singh , 2018), (Peter Wlodarczak, et al., 2017).

Ζητήματα ιδιωτικότητας μπορεί να προκύψουν σε όλα τα στάδια της εξόρυξης δεδομένων. Έτσι στο επίπεδο παροχής δεδομένων, ο πάροχος θα πρέπει να είναι σε

[39] https://el.wikipedia.org/wiki/%CE%9C%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 , (πρόσβαση,15/02/2021)

θέση να διαφυλάξει την ιδιωτικότητα των ευαίσθητων προσωπικών δεδομένων. Στο επίπεδο συλλογής δεδομένων θα πρέπει να διασφαλισθεί από τη μία πλευρά ότι τα επεξεργασθέντα δεδομένα δεν περιλαμβάνουν ευαίσθητα δεδομένα και από την άλλη πλευρά ότι αυτά διατηρούν την χρησιμότητά τους. Στο επίπεδο της εξόρυξης δεδομένων θα πρέπει να χρησιμοποιηθούν οι κατάλληλοι αλγόριθμοι έτσι ώστε να εξαχθούν πολύτιμα δεδομένα αλλά με τον πιο ασφαλή δυνατό τρόπο.

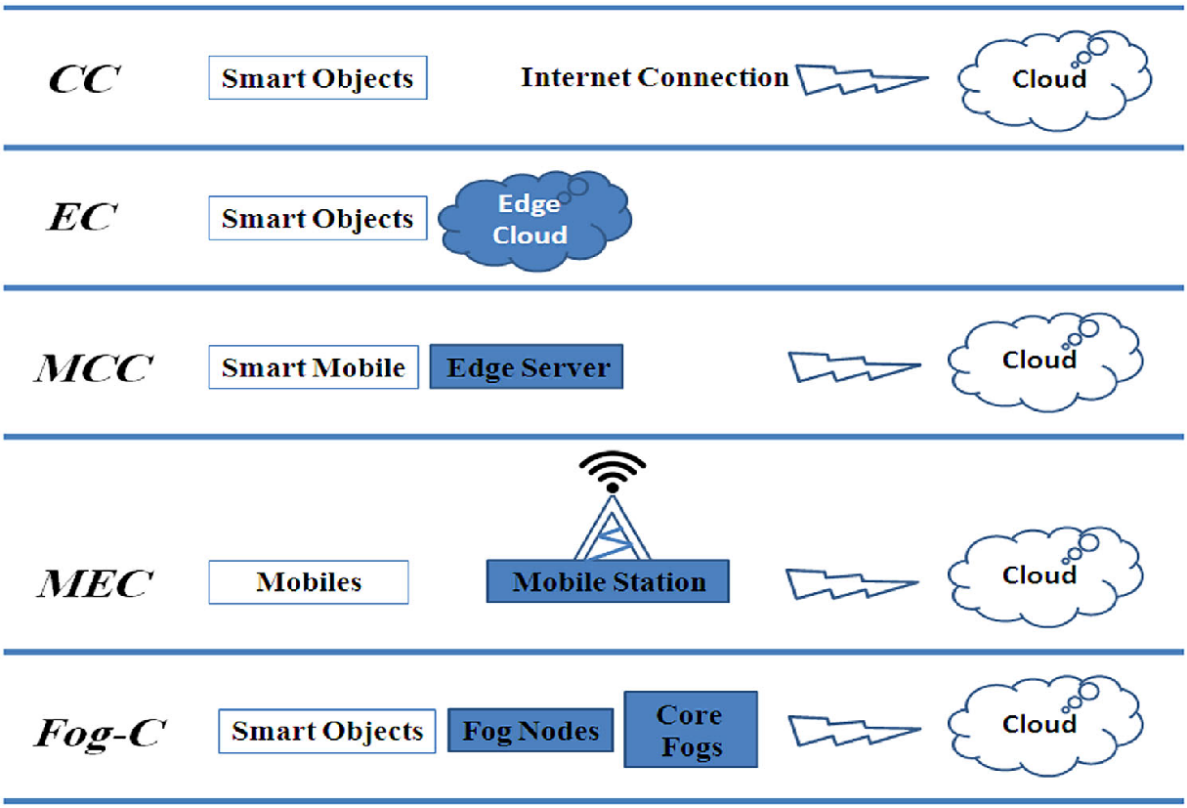
Για τη διαφύλαξη των ζητημάτων ιδιωτικότητας που ανακύπτουν από την εξόρυξη δεδομένων, όπως η μη εξουσιοδοτημένη πρόσβαση στα προσωπικά δεδομένα, η χρήση αυτών για σκοπούς διαφορετικούς από αυτούς για τους οποίους συλλέχθηκαν εξαρχής κ.λ.π., έχει αναπτυχθεί ένα πεδίο που ονομάζεται διαφύλαξη της ιδιωτικότητας της εξόρυξης δεδομένων (PPDM) και έχει ως στόχο αφενός τη μη εξόρυξη δεδομένων που οδηγούν απευθείας σε αναγνώριση της ταυτότητας των χρηστών (όπως ταυτότητα και κινητό τηλέφωνο) και αφετέρου τον αποκλεισμό παραβιάσεων της ιδιωτικότητας των εξορυχθέντων δεδομένων. Τέλος, κατά το στάδιο της απόφασης μετάδοσης δεδομένων, θα πρέπει να διασφαλίζεται η αξιοπιστία των αποφάσεων (LEI XU, et al., 2014).

14. ΥΠΟΛΟΓΙΣΤΙΚΗ ΠΑΡΥΦΩΝ

Η υπολογιστική παρυφών (Edge Computing) είναι μία επέκταση της υπολογιστικής νέφους που χρησιμοποιείται για αποκεντρωμένη υπολογιστική, παρέχοντας νέες υπηρεσίες και χαρακτηριστικά. Η ομίχλη ή αλλιώς άκρο, είναι ουσιαστικά μία μορφή της υπολογιστικής άκρου. Ειδικώτερα, η υπολογιστική παρυφών διαθέτει διάφορα μοντέλα τα σημαντικότερα από τα οποία είναι το τοπικό άκρο (Local Edge), η κινητή υπολογιστική άκρου (MEC), η κινητή υπολογιστική νέφους (MCC) και η υπολογιστική ομίχλης. Η υπολογιστική ομίχλης, στηρίζεται στην πυκνή κατανομή διαφορετικών κόμβων ομίχλης που βρίσκονται κοντά στον τελικό χρήστη, προκειμένου να διενεργήσει διάφορες υπολογιστικές και αποθηκευτικές εργασίες και λειτουργεί ως μεσάζοντας μεταξύ των έξυπνων συσκευών και του νέφους (Adnan Abi Sen & Mohammad Yamin, 2020).

Με την υπολογιστική ομίχλης γίνεται το πάντρεμα των τεχνολογιών του έξυπνου δικτύου και του νέφους, με στόχο από τη μία πλευρά να αντιμετωπιστούν οι περιορισμοί του έξυπνου δικτύου και από την άλλη πλευρά να δοθεί στο νέφος μία πιο δυναμική και αποκεντρωμένη παροχή υπηρεσιών στον τελικό χρήστη. Έτσι, το νέφος

αποκεντροποιείται, καθώς οι υπηρεσίες μεταφέρονται πιο κοντά στο τελευταίο άκρο του συστήματος και στον τελικό χρήστη, συστήνοντας έτσι το διαδίκτυο των πάντων(IoE). Στο έξυπνο δίκτυο, το κατώτερο επίπεδο αποτελείται από τις φυσικές συσκευές και μέρη. Αυτές διασυνδέονται απευθείας μεταξύ τους και με το διαδίκτυο για να σχηματίσουν το επίπεδο δικτύου αισθητήρων. Όμως, συνήθως υπάρχει ένα ενδιάμεσο επίπεδο,το οποίο καλείται ομίχλη ή παρυφή (fog ή edge).



Εικόνα 45: Μοντέλα Υπολογιστικής Ομίχλης (Adnan Abi Sen & Mohammad Yamin, 2020)

14.1. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΟΜΙΧΛΗΣ

Η υπολογιστική ομίχλης/παρυφών στις εφαρμογές κατασκευής και αυτοματισμού είναι αρχιτεκτονική δικτύου και συστήματος που προσπαθεί να συλλέξει, να αναλύσει και να επεξεργαστεί δεδομένα από αυτά τα στοιχεία, όμως πιο αποτελεσματικά από την παραδοσιακή αρχιτεκτονική νέφους. Η υπολογιστική παρυφών είναι εγκατεστημένη στο τέλος του δικτύου αισθητήρων και οπτικοποιεί τη δομή του νέφους, επεξεργαζόμενη τα δεδομένα κοντά στην πηγή-αισθητήρες. Εν συνεχεία,τα δεδομένα υπόκεινται σε εκ νέου επεξεργασία και φιλτράρισμα με σκοπό να περιοριστεί ο ρυθμός

μεταφοράς και η κατανάλωση ενέργειας. Τότε μόνο τα σχετικά δεδομένα μεταφέρονται στο νέφος, όπου αποθηκεύονται, αναλύονται και οπτικοποιούνται.

Ο στόχος αυτής της αρχιτεκτονικής είναι η μείωση της ποσότητας των δεδομένων που αποστέλλονται στο νέφος, η μείωση των καθυστερήσεων δικτύου και διαδικτύου, η βελτίωση του χρόνου απόκρισης του συστήματος σε απομακρυσμένες κρίσιμες εφαρμογές. Η βασική όμως διαφορά από άλλες αρχιτεκτονικές είναι ότι παρόλο που και άλλες ωθούν την νοημοσύνη και την επεξεργασία πιο κοντά στο σημείο προέλευσης των δεδομένων, δηλαδή στο άκρο του δικτύου, εντούτοις η υπολογιστική ομίχλης ωθεί τη νοημοσύνη στο επίπεδο αρχιτεκτονικής δικτύου τοπικού δικτύου (LAN), επεξεργαζόμενο τα δεδομένα σε κόμβο ομίχλης ή πύλη έξυπνου δικτύου.[40]

14.1.1. ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

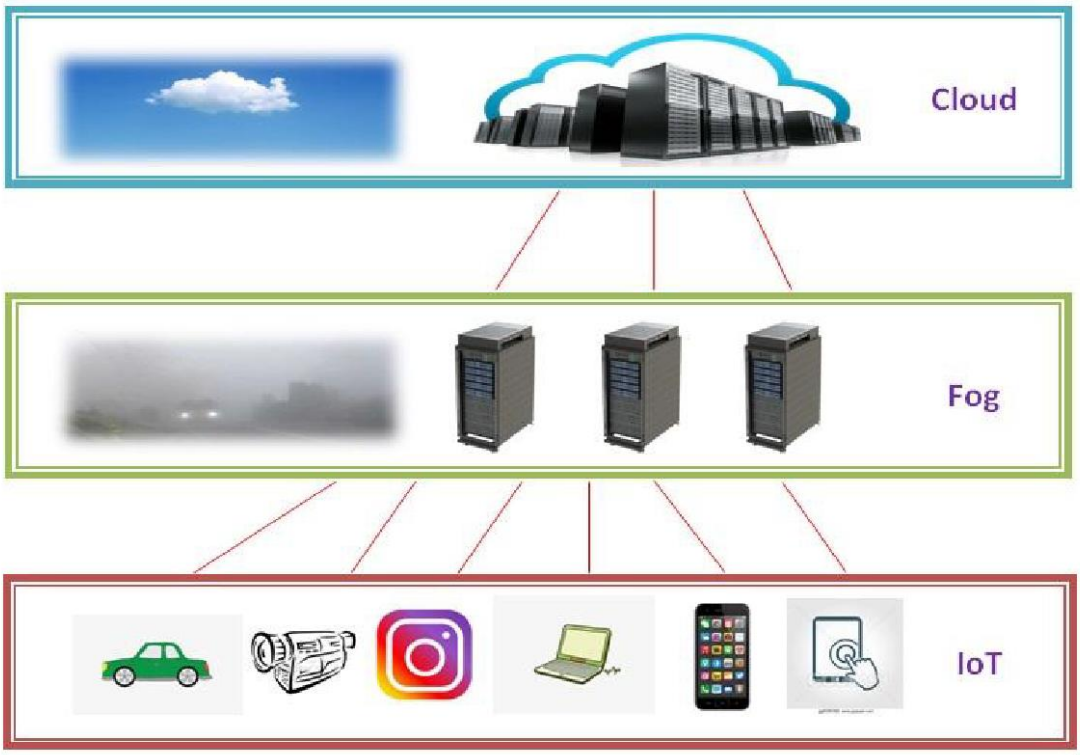
Το βασικό χαρακτηριστικό της υπολογιστικής ομίχλης είναι η τοποθεσία της, γι αυτό και μπορεί να υποστηρίξει πολλές εφαρμογές με μικρό χρόνο αναμονής. Ένα άλλο σημαντικό χαρακτηριστικό είναι η γνώση των τοποθεσιών όλων των κόμβων, προκειμένου να επιτευχθεί η κινητικότητα των δεδομένων (Verma & Shalini Chandra, 2019).

Άλλο βασικό χαρακτηριστικό της ομίχλης ή παρυφής είναι η ελαστικότητα και η μειωμένη κατανάλωση ενέργειας. Η ομίχλη, έρχεται να αντιμετωπίσει τα προβλήματα του νέφους σε σχέση με το διαδίκτυο των πραγμάτων, όπως την ασφάλεια, τις μεγάλες αποστάσεις και τα δεδομένα μεγάλης κλίμακας που οδηγούν σε μείωση της ποιότητας των υπηρεσιών (Rute C. Sofia & DANIEL MANIGLIA AMANCIO DA SILVA, 2020). Σε αυτή την αρχιτεκτονική ενσωματώνονται μηχανισμοί που οδηγούν στον καλύτερο διαμοιρασμό της υπολογιστικής και αποθήκευσης δεδομένων μέσα σε ένα συγκεκριμένο σύστημα

Εκτός των άλλων, (Adnan Abi Sen & Mohammad Yamin, 2020) η ομίχλη έχει την ικανότητα μέσω των εφαρμογών προεπεξεργασίας να μετατρέπει τα ωμά δεδομένα σε έξυπνα, μειώνοντας το μέγεθός τους και την ταχύτητα σύνδεσης, αποφορτίζοντας έτσι το νέφος. Επίσης, η ομίχλη έχει την ικανότητα να λαμβάνει αποφάσεις σε επείγουσες περιπτώσεις προτού τα δεδομένα μεταφερθούν στο νέφος και χωρίς καθυστέρηση. Οι κόμβοι ομίχλης συμβάλουν στο να παρέχεται μεγαλύτερη φορητότητα και διαθεσιμότητα των υπηρεσιών ακόμα και όταν δεν υπάρχει σύνδεση

[40] https://info.opto22.com/fog-vs-edge-computing , (πρόσβαση, 16/02/2021)

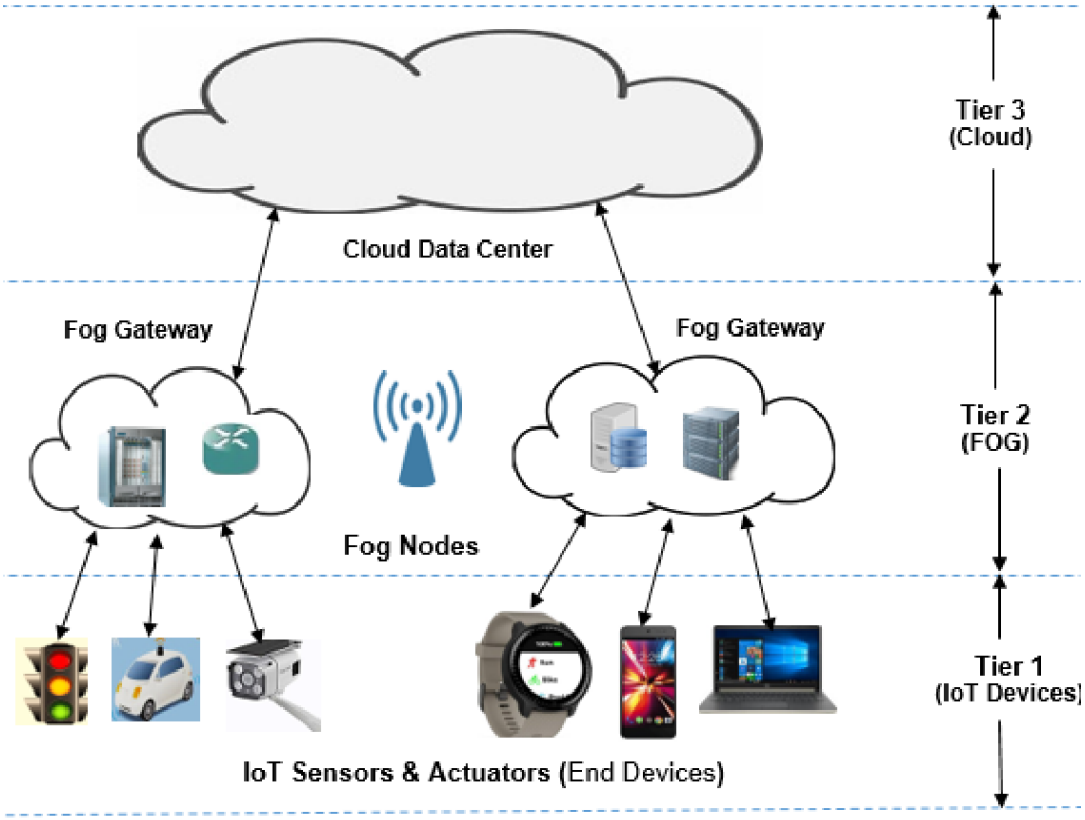
στο διαδίκτυο. Η ομίχλη αυξάνει την ασφάλεια των δεδομένων, καθώς μπορεί να εφαρμόσει πολιτική ή κρυπτογράφηση των δεδομένων προτού μεταφερθούν στο νέφος.



Εικόνα 46: Θέση της Ομίχλης μεταξύ του Νέφους και των Έξυπνων Συσκευών (Verma & Shalini Chandra, 2019)

Τέλος, εδώ είναι πολύ σημαντική η χρήση της υπολογιστικής της επίγνωσης των συνθηκών (context awareness), η οποία σχετίζεται με την επίγνωση τοποθεσίας, της ώρας, των γειτονικών συσκευών, χρηστών και λοιπών συνθηκών και ορίζεται ως κάθε πληροφορία που μπορεί να χρησιμοποιηθεί για να περιγράψει την κατάσταση μίας οντότητας. Οντότητα μπορεί να είναι ένα άτομο, αντικείμενο ή τοποθεσία που σχετίζεται με την αλληλεπίδραση μεταξύ του χρήστη και μίας εφαρμογής (Rute C. Sofia & DANIEL MANIGLIA AMANCIO DA SILVA, 2020). Οι πληροφορίες δεδομένων είναι αυτές που προκύπτουν μετά από επεξεργασία των ανεπεξέργαστων πληροφοριών που συλλέγονται από τις έξυπνες συσκευές. Στο έξυπνο δίκτυο η υπολογιστική της επίγνωσης συνθηκών διαδραματίζει ουσιώδη ρόλο στη βελτίωση των υπολογιστικών ενεργειών του συστήματος όπως ως προς το που πότε και γιατί πρέπει να επεξεργαστούν κάποια δεδομένα, για την βελτιωμένη αυθεντικοποίηση και έλεγχο πρόσβασης, για τη βελτίωση της δρομολόγησης-ροής των δεδομένων, για τη λήψη

καλύτερων αποφάσεων ως προς τον τόπο επεξεργασίας και αποθήκευσης δεδομένων καθώς και για τον διαμοιρασμό αυτών, για την καλυτέρευση της επικοινωνίας και αλληλεπίδραση των συσκευών.



Εικόνα 47: Αρχιτεκτονική Υπολογιστικής Ομίχλης/Νέφους (Rute C. Sofia & DANIEL MANIGLIA AMANCIO DA SILVA, 2020)

14.2. ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Ένα πολύ σημαντικό ζήτημα που σχετίζεται με την ασφάλεια της υπολογιστικής ομίχλης είναι η αυθεντικοποίηση μεταξύ των κόμβων αλλά και με το νέφος, η οποία γίνεται προβληματική λόγω της ύπαρξης πολλών διαφορετικών παρόχων υπηρεσιών ομίχλης (σε αντίθεση με την ύπαρξη ενός παρόχου για το νέφος). Επίσης, λόγω των περιορισμών των έξυπνων συσκευών, οι υπολογιστικές εργασίες συνήθως διενεργούνται έξω από τους κόμβους ομίχλης, με αποτέλεσμα λόγω της ανταλλαγής των υπηρεσιών να απαιτείται αυθεντικοποίηση και σε επίπεδο επικοινωνίας. Εκτός των άλλων, ο έλεγχος πρόσβασης στην υπολογιστική ομίχλης, θα πρέπει να καλύπτει την έλλειψη παρακολούθησης όλων των κενών μεταξύ έξυπνου δικτύου-ομίχλης-νέφους

καθώς και τους περιορισμούς των πόρων. Επιπλέον, ο κίνδυνος ύπαρξης κακόβουλου κόμβου (rogue node) που πείθει τον χρήστη να τον χρησιμοποιήσει, χειραγωγώντας τα δεδομένα, είναι διπλάσιος καθώς στην υπολογιστική ομίχλης υπάρχει δυναμική δημιουργία και απάλειψη ηλεκτρονικών φακέλων και άρα είναι δύσκολος ο μετέπειτα αποκλεισμός οποιουδήποτε κόμβου. Τέλος, η τοποθεσία των κόμβων και όλου του δικτύου, αποκαλύπτεται πολύ εύκολα μέσω της υπολογιστικής ομίχλης, καθώς για τη μεταφορά δεδομένων από κόμβο σε κόμβο ομίχλης αποκαλύπτεται η τοποθεσία τους (Verma & Shalini Chandra, 2019).

15. ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΤΟΥ ΕΞΥΠΝΟΥ ΔΙΚΤΥΟΥ ΑΠΟ ΝΟΜΙΚΗ ΣΚΟΠΙΑ (ΚΑΝΟΝΙΣΜΟΣ 2016/679)

Η προστασία και διαχείριση όλων των ευαίσθητων προσωπικών δεδομένων που συγκεντρώνονται από τις διασυνδεδεμένες συσκευές, δεν είναι μόνο τεχνικό ζήτημα αλλά αποτελεί το μεγάλο στοίχημα που καλείται να αντιμετωπιστεί και νομικά τα επόμενα χρόνια. Η προστασία των προσωπικών δεδομένων, μπορεί να διασφαλιστεί με διαφανή και ανοιχτή διαχείριση των ευαίσθητων πληροφοριών, με ανωνυμοποίηση και ψευδωνυμοποίηση και με συλλογή μόνο κατόπιν συναίνεσης των δοθέντων πληροφορίων και με σωστή διαχείριση των υπολοίπων.

Σήμερα, για την προστασία των δεδομένων αυτών έχει ψηφιστεί ο Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών που ενσωματώθηκε στην ελληνική νομοθεσία με τον νόμο **4624/2019.** Με αυτά τα νομοθετήματα έχουν καθιερωθεί αρχές που πρέπει να διέπουν την επεξεργασία προσωπικών δεδομένων όπως: νομιμότητα, αντικειμενικότητα και διαφάνεια κατά την επεξεργασία, να συλλέγονται και υπόκεινται σε επεξεργάζονται για καθορισμένους σκοπούς, να υπάρχει ελαχιστοποίηση και ακρίβεια των δεδομένων, περιορισμός του σκοπού εργασίας και περιόδου αποθήκευσης, λογοδοσία του υπευθύνου επεξεργασίας και ακεραιότητα και εμπιστευτικότητα των συλλεχθέντων δεδομένων[41]. Ταυτόχρονα, οι χρήστες αποκτούν δικαιώματα από την επεξεργασία των δεδομένων τους όπως

[41] https://www.cyberinsurancegreece.com/nomothesia/iot/, (πρόσβαση 15/01/2021).

δικαίωμα ενημέρωσης, πρόσβασης, διόρθωσης, διαγραφής/δικαίωμα στη λήθη, περιορισμού της επεξεργασίας, εναντίωσης και φορητότητας[42].

Με την υιοθέτηση μίας κεντρικής στρατηγικής μέσω της υιοθέτησης του ανωτέρω Κανονισμού δημιουργούνται ελπίδες για καλύτερη αντιμετώπιση των τεράστιων προκλήσεων και νομικών ζητημάτων που δημιουργεί το συνεχώς εξελισσόμενο έξυπνο δίκτυο, δεδομένου ότι οι μέχρι της ψήφισης του Κανονισμού μεμονωμένες νομοθετικές πρωτοβουλίες και νομικά πλαίσια αποδείχτηκαν αναποτελεσματικές[43].

15.1. Η ΣΥΝΑΙΝΕΣΗ (CONSENT) ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Ο νέος Κανονισμός Προστασίας Δεδομένων (GDPR) δίνει τον εξής ορισμό για τη συναίνεση*: «Πρόκειται για μία θετική ενέργεια, η οποία κατοχυρώνει μία ελεύθερη, συγκεκριμένη, πλήρως ενημερωμένη και ξεκάθαρη συμφωνία του υποκειμένου για την επεξεργασία των προσωπικών του δεδομένων, όπως με γραπτή δήλωση, ηλεκτρονικά ή προφορικά.*

Στο διαδίκτυο των πραγμάτων, λόγω της ύπαρξης μεγάλου αριθμού έξυπνων συσκευών που συνεχώς συλλέγουν και επεξεργάζονται έναν τεράστιο αριθμό δεδομένων των χρηστών, οι οποίοι πολλές φορές ούτε καν το υποψιάζονται (δεδομένα-cookies, ιστορικό περιήγησης, μέσα κοινωνικής δικτύωσης κ.λ.π.), είναι πολύ σημαντική η με πλήρη συνείδηση παροχή συναίνεσης των χρηστών για τη συλλογή, επεξεργασία και διατήρηση αυτών των δεδομένων. Προκειμένου να υπάρξει τέτοιου είδους συναίνεση, θα πρέπει να βρεθούν τρόποι (Susan Y.L. Wakenshaw1*, 2018) να γίνει εμφανής και κατανοητή η συλλογή και κίνηση δεδομένων, να καταλάβει ο χρήστης -υποκείμενο τα ρίσκα και τις επιπτώσεις της κίνησης των δεδομένων καθώς και τι ακριβώς σημαίνει η συναίνεση, να γίνουν οι όροι συλλογής επεξεργασίας και διατήρησης των δεδομένων πιο κατανοητοί, ευανάγνωστοι, προτυποποιημένοι και προσβάσιμοι στους χρήστες και να δοθεί η δυνατότητα στους χρήστες αληθινής επιλογής και δυνατότητας διαπραγμάτευσης των όρων, με τη χρήση των κατάλληλων αυτοματισμών στη συναίνεση.

Συνεπώς, η συναίνεση θα πρέπει να συσχετίζεται με μία δυναμική διαλεκτική διαδικασία που βρίσκεται υπό συνεχή διαπραγμάτευση και κατοχυρώνει την

[42] https://www.lawspot.gr/gdpr/faq?lspt_context=gdpr , (πρόσβαση 15/01/2021).
[43] https://www.lawspot.gr/nomika-blogs/vasilis_karkatzoynis/internet-things-big-data-watch-monitor-or-control (πρόσβαση 15/01/2021).

ιδιωτικότητα, ως προς την ποσότητα των δεδομένων, την ταυτότητα του προσώπου και τους λοιπούς παράγοντες, όπως τον χρόνο διατήρησης αυτών των στοιχείων. Ως εργαλεία για την επίτευξη του άνω στόχου, χρησιμοποιούνται εκτός των άλλων οι πολιτικές προστασίας, οι ενημερώσεις για δημιουργία αρχείων πληροφοριών(cookies) και η δημιουργία όρων και προϋποθέσεων για όλες αυτές τις ενέργειες.

Ειδικά σε ένα έξυπνο σύστημα, η συναίνεση θα πρέπει να συσχετίζεται με την επίγνωση από τον χρήστη της διασύνδεσης των αντικειμένων και της συλλογής των δεδομένων του, της αλληλεπίδρασης των αντικειμένων με τον χρήστη και τον πάροχο της υπηρεσίας και της ακριβούς γνώσης του πώς θα χρησιμοποιηθούν αυτά τα δεδομένα. Για την αποτελεσματική λειτουργία της συναίνεσης, θα πρέπει επίσης να δημιουργούνται ειδοποιήσεις για όλα τα ανωτέρω αλλά και για τον εντοπισμό τυχόν κακόβουλων ενεργειών στο σύστημα. Όλα αυτά γίνονται ακόμα πιο επιτακτικά σε ένα περιβάλλον έξυπνου σπιτιού, καθώς η εν αγνοία συλλογή δεδομένων γίνεται ιδιαίτερα επικίνδυνη, καθώς αυτό χρησιμοποιεί προηγμένη-αυτοματοποιημένη τεχνολογία σε διάφορα συστήματα για να ελέγχει και παρακολουθεί κάθε λειτουργία μέσα στο σπίτι (ενέργεια, θερμοκρασία, κλιματισμός κ.λ.π.).

16. ΕΠΙΛΟΓΟΣ/ΣΥΜΠΕΡΑΣΜΑΤΑ

Παρά τη δυναμική και τα πλεονεκτήματα του Διαδικτύου των Πραγμάτων, η έλλειψη ασφάλειας εξακολουθεί να αποτελεί μία από τις μεγαλύτερες αδυναμίες του, για την επίλυση της οποίας πρέπει να γίνουν ακόμα πολλά βήματα. Για την επίτευξη της ασφάλειας έχει αποδειχθεί ότι θα πρέπει να διασφαλιστεί η ακεραιότητα του έξυπνου συστήματος από άκρο σε άκρο. Όμως αυτό δεν είναι εύκολη υπόθεση, αρχικά επειδή η ίδια η φύση και τα χαρακτηριστικά των έξυπνων δικτύων, ειδικά στα πλαίσια της έξυπνης πόλης και του έξυπνου σπιτιού, οδηγούν στη δημιουργία μεγάλων κινδύνων ασφαλείας και ιδιωτικότητας

Έτσι, σ αυτή την εργασία, αφού μελετήθηκαν η δομή, η αρχιτεκτονική και οι ευπάθειες των έξυπνων συσκευών, τεχνολογιών και λοιπών συστατικών του έξυπνου δικτύου και πιο συγκεκριμένα των έξυπνων πόλεων και των έξυπνων σπιτιών, αλλά και το είδος των επιθέσεων που μπορούν αυτά να δεχτούν, δημιουργήθηκαν συμπεράσματα για τα βασικά ζητήματα ασφαλείας στα διάφορα επίπεδα του Διαδικτύου των Πραγμάτων. Εν συνεχεία, μελετήθηκαν και προτάθηκαν διάφορες τεχνολογίες και πρακτικές αντιμετώπισης των κινδύνων και επιθέσεων. Έτσι, βάσει της

παρούσας εργασίας, διαπιστώθηκε ότι τα κυριότερα ζητήματα ασφαλείας του έξυπνου δικτύου σχετίζονται με τα κάτωθι:

Τα έξυπνα δίκτυα έχουν πολλές ιδιαιτερότητες που καθιστούν την προστασία τους με παραδοσιακά μέσα αναποτελεσματική. Αυτό οφείλεται πρωτίστως στη μεγάλη ανομοιογένεια των συστατικών (συσκευών, πρωτοκόλλων και τεχνολογιών) του δικτύου, καθένα από τα οποία απαιτεί και διαφορετικές ρυθμίσεις ασφαλείας. Εκτός αυτού, τα ίδια τα βασικά στοιχεία που χαρακτηρίζουν τη λειτουργία των έξυπνων συσκευών, δηλαδή η αυτονομία,η συνδεσιμότητα, η επίγνωση του περιβάλλοντος και η αλληλεπίδραση των έξυπνων συσκευών με τον χρήστη, δηλαδή η μοναδική ικανότητα τους να εκτελούν αυτόνομους υπολογισμούς, είναι ακριβώς αυτά που τις καθιστούν και πιο ευάλωτες. Σημαντικό ρόλο για την ασφάλεια του έξυπνου δικτύου διαδραματίζουν επίσης τα έξυπνα πρωτόκολλα, τα οποία όμως είναι ιδιαίτερα ευάλωτα επειδή έχουν να αντιμετωπίσουν από τη μία πλευρά παραβιάσεις ασφαλείας των πλατφορμών των παρόχων νέφους και από την άλλη πλευρά ζητήματα ιδιωτικότητας δεδομένων, αυθεντικοποίησης, εξουσιοδότησης και σωστής διαχείρισης σε ένα διάχυτο ετερογενές περιβάλλον.

Η διενέργεια ασφαλούς δρομολόγησης στο έξυπνο δίκτυο είναι άλλο ένα στοίχημα για την επίτευξη ασφαλείας όλου του συστήματος, η οποία δυσχεραίνεται πολύ λόγω των εγγενών προβλημάτων εκ της φύσεως του έξυπνου δικτύου, ήτοι των περιορισμένων πόρων (περιορισμοί ενέργειας, αποθηκευτικού χώρου κλπ), της δυναμικής τοπολογίας δρομολόγησης, της κλιμάκωσης και των αποσυνδέσεων και των κενών του δικτύου.

Άλλο σημαντικό ζήτημα ασφαλείας εγείρει η ραχοκοκκαλιά του έξυπνου δικτύου, δηλαδή το νέφος, το οποίο στο Διαδίκτυο των Πραγμάτων ναι μεν προσφέρει τα κατάλληλα εργαλεία για τη συλλογή, επεξεργασία, διαχείριση και αποθήκευση τεράστιου όγκου δεδομένων σε πραγματικό χρόνο, όμως υπάρχει μεγάλος κίνδυνος απώλειας ή διαρροής πληροφοριών που σχετίζεται κυρίως με την πρόσβαση σε αυτά μέσω ανοιχτού/δημόσιου διαδικτύου και με την έλλειψη γνώσης σωστού διαχειρισμού τους με εχέγγυα ασφαλείας. Ειδικά όμως, η είσοδος τρίτων μερών για την αποθήκευση δεδομένων στο νέφος, επιτρέπει την απομακρυσμένη πρόσβαση και παρακολούθηση και άρα την πρόσβαση στα δεδομένα από παντού. Επιπρόσθετα, η υιοθέτηση της υπολογιστική παρυφών καθιστά ακόμα πιο ευάλωτο το έξυπνο δίκτυο καθώς η παρυφή (edge) είναι πιο ευάλωτη σε επιθέσεις επειδή είναι υλικά προσβάσιμη,δεν μπορούν να εφαρμοστούν σε αυτή παραδοσιακές μέθοδοι ασφάλισης του νέφους και λόγω της

αποκεντροποίησης των υπηρεσιών καθίσταται πιο περίπλοκη διαδικασία η εφαρμογή μηχανισμών ασφαλείας.

Εκτός των ανωτέρω, η χρήση της τεχνολογίας των δεδομένων μεγάλης κλίμακας η οποία είναι αναγκαία στο Διαδίκτυο των Πραγμάτων λόγω της παραγωγής τεράστιου όγκου δεδομένων, δημιουργεί μεγάλο ρίσκο, καθώς οι μηχανισμοί ασφαλείας αυτής της τεχνολογίας είναι γενικά αδύναμοι εξαιτίας των ίδιων των χαρακτηριστικών της, ενώ και η ίδια η εξόρυξη δεδομένων και αναλυτική προϋποθέτουν παραβίαση της ιδιωτικότητας και μη συνειδητή αποθήκευση δεδομένων. Όλα τα ανωτέρω προκαλούνται επειδή η εξαγωγή, ανάλυση, μεταφορά, αποθήκευση και επεξεργασία μεγάλων ποσοτήτων δεδομένων μπορούν να οδηγήσουν σε παρακολούθηση, ανάλυση συμπεριφοράς και δημιουργίας προφιλ και φωτογράφισης των προσώπων που αφορούν.

Επίσης, καταδείχθηκε ότι οι κίνδυνοι ασφαλείας και ιδιωτικότητας επιτείνονται περαιτέρω και από διάφορες κακές πρακτικές των ίδιων των χρηστών, λόγω άγνοιας των κινδύνων και των ρυθμίσεων ασφαλείας αλλά και των κατασκευαστών. Ειδικά οι κατασκευάστριες εταιρίες δεν ενσωματώνουν από τον σχεδιασμό διάφορες εφαρμογές και ρυθμίσεις ασφαλείας στις έξυπνες συσκευές, ενώ πολλές από αυτές δεν μπορούν εκ κατασκευής να αναβαθμιστούν ή έχουν περιορισμούς. Επιπλέον, οι επιταγές της αγοράς οδηγούν τις εταιρίες να μην επενδύουν στην ασφάλεια αλλά στην ευχρηστότητα των συσκευών με στόχο το εμπορικό κέρδος.

Τέλος, δεν υπάρχουν ενιαίες αρχές ασφαλείας και έχουν δημιουργηθεί ελάχιστα πρότυπα ασφαλείας για την κατασκευή των έξυπνων δικτύων και συσκευών, τα οποία μάλιστα δεν έχουν καταστεί υποχρεωτικά. Ούτε όμως έχει δοθεί μεγάλη έμφαση και στην πολύ σημαντική ρητή και ξεκάθαρη γνώση και συναίνεση του χρήστη για τη συλλογή, επεξεργασία και αποθήκευση των ευαίσθητων προσωπικών δεδομένων του ή την εφαρμογή πολιτικών προστασίας, νόμων και περιορισμών για την επεξεργασία, το απόρρητο και την ιδιωτικότητα των συλλεχθέντων προσωπικών δεδομένων.

16.1. ΜΕΛΛΟΝΤΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ

Όλες οι μελλοντικές έρευνες θα πρέπει να επικεντρωθούν στη δημιουργία εγγενώς ασφαλών συστημάτων σε όλα τα επίπεδα του έξυπνου δικτύου, καθώς έχει αποδειχθεί πολλάκις ότι η εκ των υστέρων προσπάθεια επίτευξης ασφάλειας αποβαίνει άκαρπη. Γι αυτό τον λόγο εφαρμογές ασφαλείας και ιδιωτικότητας θα πρέπει να ενσωματώνονται κατά τον σχεδιασμό των συσκευών και επιπλέον τα δεδομένα θα

πρέπει μεν να είναι ανοιχτά και διασυνδεδεμένα, όμως η αποθήκευση και χρήση τους θα πρέπει να γίνονται με τήρηση των αρχών ασφάλειας και ιδιωτικότητας. Προς αυτή την κατεύθυνση είναι σημαντική η υιοθέτηση υποχρεωτικών προτύπων ασφαλείας κατά την κατασκευή και η δημιουργία μηχανισμών έγκαιρου εντοπισμού των απειλών και αδυναμιών με στόχο την αποτροπή τους. Ειδικότερα, είναι μεγάλη πρόκληση η αντιμετώπιση των ποικίλων απειλών των εισβολέων στα διάφορα επίπεδα του συστήματος, καθώς μπορεί να εισαχθεί κακόβουλο λογισμικό στους φυσικούς αισθητήρες από τους εισβολείς με σκοπό να παραχθούν ψευδή δεδομένα, ανεπεξέργαστα δεδομένα μπορούν να κλαπούν από το νέφος, παραβιασμένες θύρες μπορούν να προκαλέσουν ζητήματα ασφαλείας στο νέφος των πραγμάτων κλπ. Ουσιώδης είναι και η αντιμετώπιση των καθυστερήσεων που δημιουργούνται κατά τη μεταφορά δεδομένων και οι λοιποί περιορισμοί των πόρων.

Επιπλέον, οι συσκευές χρειάζονται μία ταυτότητα και σωστή διαχείριση αυτής, έτσι ώστε να παρέχεται ταυτόχρονα ευχρηστότητα των ψηφιακών υπηρεσιών, δικαιώματα και άδειες πρόσβασης στο έξυπνο δίκτυο, διασφαλίζοντας έτσι τόσο την αξιοπιστία των ροών δεδομένων όσο και τον ασφαλή έλεγχο πρόσβασης. Η διαχείριση εμπιστοσύνης (Trust Management) είναι εξίσου σοβαρή υπόθεση καθώς θα οδηγήσει σε πιο ασφαλή επικοινωνία των συσκευών μεταξύ τους. Εκτός των ανωτέρω, κάθε σχεδιασμός και μέτρο ασφαλείας, θα πρέπει να λαμβάνουν υπόψη τη διαρκή κλιμάκωση που χαρακτηρίζει τη λειτουργία των έξυπνων δικτύων, καθώς ακόμα και μία απλή επιπλέον εντολή μέσα στο έξυπνο δίκτυο, μπορεί να προκαλέσει άρνηση υπηρεσίας. Επίσης, θα πρέπει να λαμβάνεται υπόψη και ότι τα δεδομένα δεν προστατεύονται σε όλα τα στάδια, καθώς η κρυπτογράφηση δεν είναι συνολική και ότι τα μεταδεδομένα ευαίσθητων δεδομένων μπορούν να παρέχουν πολύτιμες πληροφορίες σε εισβολείς.

Ομοίως, θα πρέπει να δοθεί ιδιαίτερη προσοχή στο ότι η παραγωγή δεδομένων σε αληθινό χρόνο δημιουργεί ζητήματα ασφαλείας που πρέπει να ερευνηθούν περαιτέρω. Επιπλέον, η ενσωμάτωση του νέφους και του διαδικτύου των πραγμάτων δημιουργεί πολλές προκλήσεις, όπως της ενσωμάτωσης των συσκευών, παρακολούθη σης του νέφους και της λειτουργίας των κατανεμημένων έξυπνων εφαρμογών κλπ.

Εκτός των ανωτέρω, η ανάγκη ασφαλούς χρήσης της τεχνολογίας των μεγάλων δεδομένων, απαιτεί τη διασφάλιση ασφαλούς υπολογιστικής στα κατανεμημένα συστήματα προγραμματισμού, το φιλτράρισμα και τον έλεγχο εγκυρότητας των τελικών σημείων, την ασφάλεια του ίδιου του νέφους, την παρακολούθηση της κίνησης

του δικτύου με στόχο την έγκαιρη ανίχνευση εισβολών και τον λεπτομερή έλεγχο της εφαρμογής των πολιτικών προστασίας. Επίσης, η ανωνυμοποίηση, η διαχείριση κλειδιού, η κρυπτογράφηση, αυθεντικοποίηση και η προστασία της επεξεργασίας δεδομένων σε ζωντανό χρόνο είναι αναγκαία.

Για την ιδιωτικότητα, η δημιουργία σωστά σχεδιασμένων ρόλων και πολιτικών εξουσιοδότησης παράλληλα με τη διασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε ευαίσθητα δεδομένα είναι ακόμα πρόκληση, ειδικά όταν απαιτείται η διασφάλιση της ακεραιότητας των δεδομένων εν μέσω συνεχών εξουσιοδοτημένων αλλαγών. Επιπλέον, σε σχέση με την ιδιωτικότητα είναι βασικό οι νέες τεχνολογίες να συμμορφώνονται σε κανονισμούς και πολιτικές ιδιωτικότητας όπως είναι ο νέος Κανονισμός Προστασίας Προσωπικών Δεδομένων και να δοθεί μεγαλύτερη έμφαση στη ρητή και συνειδητή συναίνεση των χρηστών σε ο,τι αφορά τα ευαίσθητα προσωπικά τους δεδομένα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ

[1] Watts, Silvia.; The Internet of Things(IoT): Applications, Technology, and Privacy Issues, 2016.

[2] IOT Technical Challenges and Solutions, Pal Arpan, Puushothaman, Balamuralidshar,Series: Artech House Power Engineering 2017.

[3] The Technical foundation of Iot, Andryan Boris, Konigseder, Thomas, 2017, Artech House

[4] Iot Security Issues, Alasdair Gilchrist, Edition Boston 2017.

ΜΕΛΕΤΕΣ

[1] (ENISA), E. U. A. F. N. A. I. S., 2017,*Baseline Security Recommendations for IoT,* s.l.: ENISA.

[2] Abdul Fuad Abdul Rahman, Maslina Daud & Madihah Zulfa Mohamad, 2016. *Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework.* s.l., s.n.

[3] Abdulrahman Almohaimeed, Srikanth Gampa & Gurtaj Singh, 2019. *Privacy-Preserving IoT Devices.* Farmingdale, NY, USA, s.n.

[4] Abhinandan Banik & Samir Kumar Bandyopadhyay, 2018. Solve Big Data Security Issues. *International Journal of Computer Applications Technology and Research*, p. Samir Kumar Bandyopadhyay.

[5] Abhishek Raghuvanshi a, ⇑. U. K. S., 2020. *Internet of Things for smart cities- security issues and challenges,* s.l.: s.n.

[6] Adnan Abi Sen & Mohammad Yamin, 2020. Advantages of using fog in IoT applications. *International Journal of Information Technology.*

[7] Ado Adamou Abba Ari, και συν., 2019. Enabling privacy and security in Cloud of Things: Architecture,applications, security & privacy challenges. *Applied Computing and Informatics.*

[8] ADRIAN PEKAR, J. M. K. G. S. Z., 2020. *Application Domain-Based Overview of IoT Network,* s.l.: s.n.

[9] Afzaal, M., 2019. Security and Privacy in Smart Cities: Issues and Current Solutions.

[10] Agazzi, A. E., 2020. Smart home, security concerns of IoT.

[11] Alin ZAMFIROIU, και συν., 2020. *IoT Communication Security Issues for Companies: Challenges, Protocols and The Web of Data.* s.l., s.n.

[12] Alper Kaan Sarica & Pelin Angin, 2020. Explainable Security in SDN-Based IoT Networks. *sensors*.

[13] Anna Triantafyllou, 1. P. S. ,. a. T. D. L., 2018. *Network Protocols, Schemes, and Mechanisms for iot,* s.l.: s.n.

[14] Anon., 2017. *Internet of Things Security Guideline V1.0,* s.l.: Workstream 5 Security and Network Resilience of the IoT Alliance Australia (IoTAA).

[15] Anwaar AlDairi, L. T., 2017. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *The International Workshop on Smart Cities Systems Engineering (SCE 2017)*.

[16] Attila Kertész, Szilvia Váradi, Radhika Garg & Burkhard Stiller, 2016. *Legal and Regulative Aspects of IoT Cloud Systems.* Vienna, Austria, IEEE.

[17] Benjamin K. Sovacool, Mari Martiskainen a & Dylan D. Furszyfer Del Rio, 2021. Knowledge, energy sustainability, and vulnerability in the demographics of smart home technology diffusion. *Energy Policy*.

[18] Boris, A. & Thomas, K., 2017. *The Technical Foundations of Iot.* s.l.:Artech House.

[19] Bruhadeshwar Bezawada, και συν., 2018. *Behavioral Fingerprinting of IoT Devices.* s.l., s.n., p. Pages 41–50.

[20] Burkhard Stiller, Eryk Schiller & Corinna Schmitt, 2020. An Overview of Network Communication Technologies for IoT. Στο: *Handbook of Internet-of-Things.* s.l.: Springer.

[21] Dan Dragomir∗, L. G. S. C. a. A. R., χ.χ. *A Survey on Secure Communication Protocols for IoT Systems.* s.l., 2016 International Workshop on Secure Internet of Things.

[22] Dange, S., 2019. *IoT Botnet: The Largest Threat to the IoT Network.* Greater Noida, s.n.

[23] Danny Yuxing Huang, και συν., 2019. IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale. *Computer Science Cryptography and Security*.

[24] Deepti , S. & Nasib Singh , . G., 2018. Data Mining in IoT and its Challenges. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING,* p. 293.

[25] Den ver BraganRAGANza & B. Tulasi, 2017. RFID Security Issues in IoT: A Comparative Study. *ORIENTAL JOURNAL OF COMPUTER SCIENCE & TECHNOLOGY*.

[26] Dipra Mitra, Sohan Goswami, Debasish Hati & Soumali Roy, 2020. COMPARATIVE STUDY OF IOT PROTOCOLS. *PJAEE (Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(7)*.

[27] ENISA, 2018. *Good Practices for Security of Internet of Things,* s.l.: ENISA.

[28] Erol Gelenbe, και συν., 2020. *IoT Network Attack Detection and Mitigation.* s.l., IEEE.

[29] Faraz Idris Khan & Sufian Hameed, 2019. Understanding Security Requirements and Challenges in Internet of Things (IoTs): A Review. *Journal of Computer Networks and Communications*.

[30] Filho, M. F., 2020. *Vulnerabilities and security issues of IoT devices Technical Report,* s.l.: White Paper #01022020.

[31] FLAUZAC Olivier, GONZALEZ Carlos & NOLOT Florent, 2015. Architecture for iot network. *Procedia Computer Science International Workshop on Big Data and Data Mining Challenges on IoT and Pervasive Systems*.

[32] Florian Metzger, και συν., 2019. Modeling of Aggregated IoT Traffic and Its Application to an IoT Cloud. *Proceedings of the IEEE*.

[33] Foram Chovatiya, Purvi Prajapati, Jalpesh Vasa & Jay Patel, 2017. *A Research Direction on Data Mining with IOT.* s.l., s.n.

[34] G. Saibabu, Anuj Jain & V. K. Sharma, 2020. Security Issues and Challenges in IoT Routing over Wireless Communication. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*.

[35] Gayatri Kapil, Alka Agrawal & Prof. Raees Ahmad Khan, 2020. Big Data Security challenges: Hadoop Perspective. *International Journal of Pure and Applied Mathematics*.

[36] Gayatri Kapil, Alka Agrawal & R. A. Khan, 2020. Big Data Security and Privacy Issues. *Asian Journal of Computer Science and Technology*, pp. pp. 128-133.

[37] Georgios Mantas, Dimitris Lymperopoulos & Nikos Komninos, 2010. Security in Smart Home Environment. Στο: *Wireless Technologies for Ambient Assisted Living and Health Care: Systems and Applications.* s.l.:Medican Information Science.

[38] Gilchrist, A., 2017. *Iot Security Issues.* Boston επιμ. s.l.:s.n.

[39] Giuseppe Nebbione & Maria Carla Calzarossa, 2020. Security of IoT Application Layer Protocols: Challenges and Findings. *Future Internet*.

[40] Hammood, M. N., 2016. *BIG DATA SECURITY AND CHALLENGES,* s.l.: RESEARCH GATE.

[41] Hannah, A. A. S., 2020. Examining the Concept of Smart Home Technologies (IoT Systems). *Innovative Systems Design and Engineering*.

[42] Hassan OUAHI & Abdenbi MAZOUL, 2021. *Traffic optimization in IOT networks.* s.l., s.n.

[43] Hooman Mohajeri Moghaddam, και συν., 2019. *Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices.* s.l., s.n.

[44] Hyunsik Yang & Younghan Kim, 2019. Design and Implementation of High-Availability Architecture for IoT-Cloud Services. *Sensors*.

[45] Ibtissame KANDROUCH, Manale BOUGHANJA, Nabil HMINA & Habiba CHAOUI, October 29 – November 1, 2018. *Big Data Security Proposed Solution.* Pretoria / Johannesburg, South Africa, s.n.

[46] Ismail Butun, Alparslan Sari & Patrik Österberg, 2020. Hardware Security of Fog End-Devices for the Internet of Things. *sensors*.

[47] J. Cynthia, H. Parveen Sultana, M. N. Saroja & J. Senthil, 2019. Security Protocols for IoT. *Ubiquitous Computing and Computing Security of IoT*.

[48] Jonathan Tournier, et al., 2020. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things Journal*, p. pp.100264.

[49] José V. V. Sobral, και συν., 2019. Routing Protocols for Low Power and Lossy Networks in Internet of Things Applications. *SENSORS*.

[50] Julio Moreno, Manuel A. Serrano & Eduardo Fernández-Medina, 2016. Main Issues in Big Data Security. *future internet*.

[51] K. Kavitha, Dr.G. Suseendran & Suseendran G., 2018. A Review on Security Issues of IOT Based on Various Technologies. *Journal of Advanced Research in Dynamical and Control Systems*.

[52] Kamalanathan Kandasamy, Sethuraman Srinivas, Krishnashree Achuthan & Venkat P. Rangan , 2020. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security volume*.

[53] Kaustav Ghosh & Asoke Nath, 2016. *Big Data: Security Issues and Challenges.* s.l., s.n., pp. PP 1-9.

[54] Kurdistan Ali & Shavan Askar, 2021. Security Issues and Vulnerability of IoT Devices. *Science and Business*, pp. 101-115.

[55] LEI XU, et al., 2014. Information Security in Big Data:Privacy and Data Mining. *IEEE ACCESS*.

[56] Marisa Paryasto, Andry Alamsyah, Budi Rahardjo & Kuspriyanto, 2014. *Big-Data Security Management Issues.* Bandung, s.n.

[57] Md Husamuddin & Mohammed Qayyum, 2017. *Internet of Things :A Study on Security and Privacy Threats.* s.l., s.n.

[58] Mohammad Aazam, Pham Phuoc Hung & Eui-nam Huh, 2014. *Smart gateway based communication for cloud of things.* Singapore, 21–24 April 2014, s.n.

[59] Mohammad Erfan Momken, 2017. *IoT Protocols Survey*, s.l.: s.n.

[60] Morta Vitunskaite, Y. H. ∗. T. B. H. J., 2019. *Smart cities and cyber security*, s.l.: The Gateway House.

[61] Nallapaneni Manoj Kumara, P. K. M., 2018. *Blockchain technology for security issues and challenges in IoT.* s.l., International Conference on Computational Intelligence and Data Science (ICCIDS 2018).

[62] Nawazuddin Mohd1, P. C. S. S. P. N. W. G. K., 2018. Emerging Technologies and Smart Integration of Internet of Things (IoT) in Communication and Software Engineering. *Journal of Emerging Technologies and Innovative Research (JETIR*.

[63] Neelam Saleem Khan & Ahsan Chishti, 2020. Security Challenges in Fog and IoT, Blockchain Technology and Cell Tree Solutions: A Review. *Scalable Computing*.

[64] Ninny Bhogal & Shaveta Jain, 2017. A REVIEW ON BIG DATA SECURITY AND HANDLING. *International Research Based Journal*.

[65] Niranjan & Nitish, D. S. V., 2016. Security in Data Mining- A Comprehensive Survey. *Global Journal of Computer Science and Technology: C*.

[66] Niroshinie Fernando, και συν., 2019. Opportunistic Fog for IoT: Challenges and Opportunities. *IEEE Internet of Things Journal*.

[67] Otuoze, A., 2018. *Journal of Electrical Systems and Information Technology 5*, pp. 468-483.

[68] Pal , A. & Purushothaman, B., 2017. *Iot Technical challenges and Solution.* Artech House επιμ. s.l.:s.n.

[69] Papadimitriou, P., χ.χ. *Privacy Aspects for Cloud Computing*, s.l.: s.n.

[70] Peter Wlodarczak, Mustafa Ally & Jeffrey Soar, 2017. *Data mining in IoT: data analysis for a new paradigm on the internet.* 2nd Int. Workshop on Knowledge Management of Web Social Media, Leipzig, Germany, August 2017 (KMWSM '17), 4 pages., s.n.

[71] Preeti Agarwal & Mansaf Alam, 2018. *IoT Cloud Platforms: an Application Development Perspective*, s.l.: s.n.

[72] Qi Jing, et al., 2014. Security of the Internet of Things: perspectives and challenges. *Wireless Netw*.

[73] Rhitabrat Pokharel, Sarthak Agarwal, Aanchal Khatri & Shefali Singhal, 2018. *A Survey on Secure Routing Protocols Based on Trust Management in.* s.l., 4th International Conference on Cyber Security and privacy in communication networks (ICCS).

[74] Rute C. Sofia & DANIEL MANIGLIA AMANCIO DA SILVA, 2020. A Discussion on Context-Awareness to Better Support the IoT Cloud/Edge Continuum. *IEEE ACCESS*.

[75] Saleem, T. J., 2016. A Detailed Study of Routing in Internet of Things. *International Journal of Engineering Science and Innovative Technology (IJESIT)*.

[76] Santosh Kulkarni, P. S. K., 2017. *Communication Models in Internet of Things: A survey,* s.l.: s.n.

[77] Sarada Prasad Gochhayat, et al., 2020. Reliable and secure data transfer in IoT networks. *Wireless Networks*.

[78] Sarada Prasad Gochhayat, και συν., 2020. Reliable and secure data transfer in IoT networks. *Wireless Networks*.

[79] Shivansh Upadhyay, Shashwat Kumar & Sagnik Dutta, 2019. *Vulnerability scanning in IOT Devices Introduction: Vulnerability scanning in IOT Devices.* s.l., s.n.

[80] Skouloudi, C. & Gema Fernández, 2018. *Towards secure convergence of Cloud and IoT,* s.l.: European Union Agency for Network and Information Security.

[81] Sriram Sankaran, R. S., 2015. *Modeling and Analysis of Routing in IoT Networks.* s.l., 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India.

[82] Stylianos Kavalarisa, b. F.-E. K. K. K. E. S., 2015. *Development of a Multi-Vector Information Security Rating Scale for Smart Devices as a Means for Raising Public InfoSec Awareness,* s.l.: International Conference on Communication, Management and Information Technology (ICCMIT.

[83] Suchetha K N & H S Guruprasad, 2015. Integration of IOT, Cloud and Big Data. *Global Journal of Engineering Science and Researches*.

[84] Sufian Hameed, Faraz Idris Khan, & Bilal Hameed2, 2019. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *Journal of Computer Networks and Communications*.

[85] Sunil Kumar Singh & Sumit Kumar, 2021. Blockchain Technology: Introduction, Integration and Security Issues with IoT. *Computer Science*.

[86] Susan Y.L. Wakenshaw1*, C. M. m. S. R. G. †. a. K. G., 2018. *Mechanisms for Meaningful Consent in Internet of Things,* s.l.: s.n.

[87] Syed Rizvi, και συν., 2020. Identifying the Attack Surface for IoT Network. *Internet of Things.*

[88] Sylvia, W., 2016. *IOT Applications, Technology, Privacy Issues.* s.l.:s.n.

[89] Syrine Sahmim & Hamza Gharsellaoui, 2017. *Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review.* France, s.n.

[90] T. Pflanzner & A. Kertesz, 2018. A Taxonomy and Survey of IoT Cloud Applications. *EAI Endorsed Transactions on Internet of Things*.

[91] Tamas Szadeczky & Gergely Kovacs, 2018. *Known security issues of IoT systems.* Budapest, Hungary, s.n.

[92] Tanweer Alam & Mohamed Benaida, 2020. Blockchain, Fog and IoT Integrated Framework:Review, Architecture and Evaluation. *Faculty of Computer and Information Systems*.

[93] Tara Salman, R. J., 2017. *A Survey of Protocols and Standards for Internet of Things,* s.l.: s.n.

[94] Theodoros Aivaliotis, και συν., 2020. *Smart Homes: Security Challenges and Privacy Concerns,* s.l.: Research Gate.

[95] Usman, M., 2020. Lightweight Encryption for the Low Powered IoT Devices. *Computer Science*.

[96] Vaibhav Hans & Neelu J.Ahuja, 2016. Big Data Security – Challenges and Recommendations. *International Journal of Computer Sciences and Engineering.*

[97] Vasudeva Pai & Nikshepa, 2018. Survey on IoT Security Issues and Security Protocols. *International Journal of Computer Applications*.

[98] Verma, R. & Shalini Chandra, 2019. Security and Privacy Issues in Fog driven IoT Environment. *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING.*

[99] Vito Albino, U. B. a. R. M. D., 2015. Smart Cities: Definitions, Dimensions,Performance, and Initiatives. *Journal of Urban Technology*.

[100] Vitor A. Cunha, και συν., 2019. *A Network Service for Preventing Data Leakage from IoT Cloud-assisted Equipment.* s.l., IEEE.

[101] William M. S. Stout & Vincent Urias, 2016. *Challenges to securing the Internet of Things.* s.l., s.n.

[102] Yana Krytska, Tetiana Biloborodova & Skarga-Bandurova I.S., 2019. Data mining techniques for IoT analytics. *ВІСНИК СХІДНОУКРАЇНСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ імені Володимира Даля*.

[103] Ye-Jin Choi, Hee-Jung Kang & Il-Gu Lee, 2019. Scalable and Secure Internet of Things Connectivity. *electronics*.

[104] Yichao Jin, Sedat Gormus, Parag Kulkarni & Mahesh Sooriyabandara , 2016. Κεντρική δρομολόγηση περιεχομένου σε δίκτυα IoT και ενσωμάτωσή της σε RPL. Στο: *COMPUTER COMMUNICATIONS ON SCIENCE DIRECT.* s.l.:s.n.

[105] Youyang Qu, L. C. X. G. Y., 2017. *Security and Privacy in Smart Cities: Challenges and Opportunities,* s.l.: IEEE ACCESS.

[106] Zhao, L., 2020. Privacy-Preserving Distributed Analytics in Fog-Enabled IoT Systems. *sensors*.

[107] Zibuyisile Magubane, Paul Tarwireyi & Mathew .O Adigun, 21-22 Nov. 2019. *Evaluating the Energy Efficiency of IoT Routing Protocols.* s.l., IEEE.

[108] Zibuyisile Magubane, Paul Tarwireyi & Matthew Adigun, 2020. *Evaluating the Energy Efficiency of IoT Routing Protocols.* s.l., IEEE.

[109] Benefits and risks of smart home technologies,Charlie Wilsona,∗, Tom Hargreavesb,, Richard Hauxwell-Baldwinb

[110] Development of a Multi-Vector Information Security Rating Scale,for Smart Devices as a Means for Raising Public InfoSec Awareness,Stylianos Kavalarisa,b*, Fragkiskos-Emmanouil Kioupakisa, Konstantinos Kaltsasa,Dr Emmanouil Serrelisa,c

[111] International Conference on Computational Intelligence and Data Science (ICCIDS 2018),Blockchain technology for security issues and challenges in IoT,Nallapaneni Manoj Kumara,Pradeep Kumar Mallickb,*

[112] Faculty of Electrical and Electronics Engineering, Universiti Malaysia Pahang, 26600 Pekan, Pahang, Malaysia, Vignana Bharathi Institute of Technology, Ranga Reddy-501301, Telangana, India, ScienceDirect.

[113] 8th International Conference on Sustainability in Energy and Buildings, SEB-16, 11-13 September,2016, Turin, ITALY ,Insights on Smart Home concept and occupants' interaction with building controls,Valentina Fabi*a, Giorgia Spigliantinia, Stefano Paolo Corgnatia.

[114] 8th International Conference on Sustainability in Energy and Buildings, SEB-16, 11-13 September 2016, Turin, ITALY,A review on Internet of Things solutions for intelligent energy,control in buildings for smart city applications,Iman Khajenasiria,*, Abouzar Estebsarib, Marian Verhelsta, Georges Gielena.

[115] International Conference on Communication, Management and Information Technology (ICCMIT 2015) Development of a Multi-Vector Information Security Rating Scale for Smart Devices as a Means for Raising Public InfoSec Awareness Stylianos Kavalarisa,b*, Fragkiskos-Emmanouil Kioupakisa, Konstantinos Kaltsasa,
[116] Dr Emmanouil Serrelisa,c.

[117] Smart Cities: Definitions, Dimensions, Performance, and Initiatives Vito Albino, Umberto Berardi and Rosa Maria Dangelico

[118] Tschofenig, H (2015) "Architectural Considerations in Smart Object Networking. Tech"., Internet Architecture Board Communication Models in Internet of Things: A Survey

[119] Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership Morta Vitunskaite, Ying He ∗, Thomas Brandstetter, Helge Janicke.

[120] Internet of Things for smart cities- security issues and challenges ,Abhishek Raghuvanshi a, Umesh Kumar Singh b

[121] Components of a smart device and smart device interactions ,Alan Davy Telecommunications Software and Systems Group

[122] What is a smart device? - a conceptualisation within the paradigm of the internet of things,Manuel Silverio-Fernández, Suresh Renukappa & Subashini Suresh

[123] Modeling and Analysis of Routing in IoT Networks ,Sriram Sankaran,Ramalingam Sridhar.

[124] A Survey of Protocols and Standards for Internet of Things Tara Salman, Raj Jain Department of Computer Science and Engineering Washington University in St. Louis

[125] 8th International Conference on Sustainability in Energy and Buildings, SEB-16, 11-13 September 2016, Turin, ITALY, A review on Internet of Things solutions for intelligent energy control in buildings for smart city applications Iman Khajenasiria,*, Abouzar Estebsarib, Marian Verhelsta, Georges Gielena.

[126] International Conference on Computational Intelligence and Data Science (ICCIDS 2018) Blockchain technology for security issues and challenges in IoT Nallapaneni Manoj Kumara,Prad.eep Kumar Mallickb,*

[127] Application Domain-Based Overview of IoT Network ,Traffic Characteristics,ADRIAN PEKAR, JOZEF MOCNEJ,WINSTON K. G. SEAH, IVETA ZOLOTOVA,ACM Computing Surveys, Vol. 53, No. 4, Article 87. Publication date: July 2020.

[128] Communication Models in Internet of Things:A Survey, Santosh Kulkarni Prof. Sanjeev Kulkarni.

[129] Review Article Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends Anna Triantafyllou ,1 Panagiotis Sarigiannidis ,1 and Thomas D. Lagkas 2.

[130] International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 5, Issue 3, May 2016,A Detailed Study of Routing in Internet of Things Tausifa Jan Saleem.

[131] Security and Privacy in Smart Cities: Issues and Current Solutions,Muhammad Afzaal,Research Gate .

[132] The International Workshop on Smart Cities Systems Engineering (SCE 2017) Cyber Security Attacks on Smart Cities and Associated Mobile Technologies,Anwaar AlDairi and Lo Ai Tawalbeh, Science Direct 2017.

[133] Security and Privacy in Smart Cities: Challenges and Opportunities,Article in IEEE Access · July 2018,Youyang Qu, RESEARCH GATE

[134] Deepti Gupta; Smriti Bhatt; Paras Bhatt; Maanak Gupta; Ali Saman Tosun, Game Theory Based Privacy Preserving Approach for Collaborative Deep Learning in IoT, Computer Science 2021

[135] Do Cuong; Nguyen H. Tran; Choong Seon Hong; Charles A. Kamhoua; KEVIN A. KWIAT; ERIK BLASCH; SHAOLEI REN; NIKI PISSINOU; SUNDARAJA SITHARAMA IYENGAR, Game Theory for Cyber Security and Privacy, ACM Computing Surveys 50(2):1-37, 2017

[136] Mohammed El-hajj; Ahmad Fadlallah; Maroun Chamoun; Ahmed Serhrouchni, A Survey of Internet of Things (IoT), Sensors 2019

ΙΣΤΟΣΕΛΙΔΕΣ

https://www.rfc-editor.org/rfc/rfc7452.txt,(πρόσβαση 26/12/2020)
https://danielelizalde.com/iot-primer/,(πρόσβαση 26/12/2020)
www.blockchain.org.gr,(πρόσβαση 26/12/2020)
el.wikipedia.org/wiki, ,(πρόσβαση 26/12/2020)
https://securityreport.gr/magazine-archive/etos-2019/item/7090-asyrmata-protokolla-epikoinonias-gia-efarmoges-iot,(πρόσβαση,01/01/2021)
https://www.i-scoop.eu/internet-of-things-guide/iot-technology-stack-devices-gateways-platforms/ (πρόσβαση,05/01/2021)

https://engineering.eckovation.com/iot-stack/,(πρόσβαση,07/02/2021)
https://docs.microsoft.com/el-gr/archive/blogs/uktechnet/what-is-the-internet-of-things-and-where-does-microsoft-sit,(πρόσβαση 10/01/2021)
https://www.postscapes.com/internet-of-things-protocols (πρόσβαση 30/12/2020)
https://slogix.in/iot-blog/what-are-the-pitfalls-in-the-design-of-iot-routing-protocols/index.html, (πρόσβαση 15/02/2021)
https://www.quora.com/What-are-the-different-layers-of-IoT-model,πρόσβαση 15/01/2021
https://cities-today.com/industry/six-ss-for-smart-city-successes/ (πρόσβαση 15/01/2021)
https://www.researchgate.net/figure/Security-threats-at-different-layers-of-the-IoT-architecture_fig2_337259162, (πρόσβαση 09/02/2021)
https://securityboulevard.com/2020/10/lack-of-security-in-iot-devices-explained-what-can-we-do-about-it/, (πρόσβαση 09/02/2021)
https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-wstation-service.html (πρόσβαση 15/01/2021)
https://wiki.crashtest-security.com/insecure-network-services-open-port-scanner, (πρόσβαση, 01/03/2021)
https://codedx.com/blog/how-to-manage-iot-application-security-vulnerabilities-more-efficiently/,(πρόσβαση 17/02/2021)
https://www.dilitrust.com/en/blog/cyber-attacks-smart-cities/ (πρόσβαση 16/01/2021)
https://informationsecuritybuzz.com/isbuzz-expert-panel/cia-triad-and-new-emerging-technologies-big-data-and-iot/, (πρόσβαση 16/01/2021)
https://www.paloaltonetworks.com/cyberpedia/how-to-secure-iot-devices-in-the-enterprise, (πρόβαση 16/03/2021)
https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained, (πρόσβαση 11/02/2021)
https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-020-00111-0 ,(πρόσβαση, 18/01/2021
https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html, (πρόσβαση 21/02/2021)
https://el.wikipedia.org/wiki/Blockchain , (πρόσβαση 21/02/2021)
https://twitter.com/ronald_vanloon/status/999282072207446021 , (πρόσβαση, 14/03/2021)
https://www.apriorit.com/dev-blog/638-blockchain-how-can-blockchain-secure-iot-networks, (πρόσβαση, 01/03/2021)
https://link.springer.com/chapter/10.1007/978-3-319-98734-7_19, (πρόσβαση, 25/03/2021)
https://el.wikipedia.org/wiki/%CE%98%CE%B5%CF%89%CF%81%CE%AF%CE%B1_%CF%80%CE%B1%CE%B9%CE%B3%CE%BD%CE%AF%CF%89%CE%BD , (πρόσβαση 15/01/2021)
https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/# , (πρόσβαση ,15/03/2021)
https://iot-analytics.com/understanding-iot-cyber-security-part-2/, (πρόσβαση, 29/03/2021)
https://www.whizlabs.com/blog/iot-and-big-data/, (πρόσβαση, 02/03/2021)
https://datafloq.com/read/why-your-big-data-iot-security-are-vulnerable/2169, (πρόσβαση, 05/03/2021)
https://en.wikipedia.org/wiki/Data_mining (πρόσβαση 18/03/2021)
https://el.wikipedia.org/wiki/%CE%9C%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 , (πρόσβαση, 15/02/2021)
https://info.opto22.com/fog-vs-edge-computing , (πρόσβαση, 16/02/2021)
https://www.cyberinsurancegreece.com/nomothesia/iot/, (πρόσβαση 15/01/2021)
https://www.lawspot.gr/gdpr/faq?lspt_context=gdpr , (πρόσβαση 15/01/2021).
https://www.lawspot.gr/nomika-blogs/vasilis_karkatzoynis/internet-things-big-data-watch-monitor-or-control (πρόσβαση 15/01/2021).
https://docs.microsoft.com/el-gr/archive/blogs/uktechnet/what-is-the-internet-of-things-and-where-does-microsoft-sit ,(πρόσβαση, 12/01/2021)

https://www.i-scoop.eu/internet-of-things-guide/iot-technology-stack-devices-gateways-platforms/, (πρόσβαση, 15/01/2021)
https://securityreport.gr/magazine-archive/etos-2020/item/8271-internet-of-things, (πρόσβαση, 05/02/2021)
https://www.networkworld.com/article/3332032/top-10-iot-vulnerabilities.html, πρόσβαση (15/03/2021)
https://securityboulevard.com/2020/10/the-top-iot-vulnerabilities-in-your-devices-keyfactor/, (πρόσβαση,15/03/2021)
https://wiki.crashtest-security.com/insecure-network-services-open-port-scanner, (πρόσβαση 11/03/2021)
https://www.networkworld.com/article/3128372/ddos-attacks-using-iot-devices-follow-the-manchurian-candidate-model.html, (πρόσβαση 18/04/2021)