ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ασφάλεια υλικού σε συσκευές διαδικτύου των πραγμάτων(Internet of things)

Διπλωματική Εργασία

Ραφαήλ Κυριάκου

Επιβλέπων: Γεώργιος Σταμούλης

Βόλος 2023

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Hardware Security in Internet of Things(IoT) Devices

Diploma Thesis

Rafael Kyriakou

Supervisor: George Stamoulis

Volos 2023

Στην οικογένεια και στους φίλους μου.

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων/πουσα	**Γεώργιος Σταμούλης** Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Νέστωρ Ευμορφόπουλος** Αναπληρωτής Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Ασπασία Δασκαλοπούλου** Αναπληρώτρια Καθηγήτρια, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελούν αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλουν οποιασδήποτε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχουν έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Δηλώνω επίσης ότι τα αποτελέσματα της εργασίας δεν έχουν χρησιμοποιηθεί για την απόκτηση άλλου πτυχίου. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο Δηλών

Ραφαήλ Κυριάκου

DISCLAIMER ON ACADEMIC ETHICS AND INTELLECTUAL PROPERTY RIGHTS

Being fully aware of the implications of copyright laws, I expressly state that this diploma thesis, as well as the electronic files and source codes developed or modified in the course of this thesis, are solely the product of my personal work and do not infringe any rights of intellectual property, personality and personal data of third parties, do not contain work / contributions of third parties for which the permission of the authors / beneficiaries is required and are not a product of partial or complete plagiarism, while the sources used are limited to the bibliographic references only and meet the rules of scientific citing. The points where I have used ideas, text, files and / or sources of other authors are clearly mentioned in the text with the appropriate citation and the relevant complete reference is included in the bibliographic references section. I also declare that the results of the work have not been used to obtain another degree. I fully, individually and personally undertake all legal and administrative consequences that may arise in the event that it is proven, in the course of time, that this thesis or part of it does not belong to me because it is a product of plagiarism.

The Declarant

Rafael Kyriakou

Πίνακας περιεχομένων

ΠΕΡΙΛΗΨΗ

Το Διαδίκτυο των Πραγμάτων (IoT) έχει μεταμορφώσει την ανθρώπινη κοινωνία και τις δραστηριότητες της. Από τα έξυπνα σπίτια μέχρι τον βιομηχανικό αυτοματισμό, ο πολλαπλασιασμός των συσκευών IoT έχει επιφέρει ευκολία και αποτελεσματικότητα. Ωστόσο, αυτό το διασυνδεδεμένο τοπίο εισάγει επίσης πολλές προκλήσεις ασφαλείας, καθιστώντας επιτακτική την ενσωμάτωση ισχυρών μέτρων ασφαλείας υλικού σε συσκευές IoT. Σε αντίθεση με τα παραδοσιακά συστήματα υπολογιστών, οι συσκευές IoT συχνά λειτουργούν στην άκρη των δικτύων, συλλέγοντας και μεταδίδοντας ευαίσθητα δεδομένα. Η ασφάλεια υλικού σε αυτό το πλαίσιο περιλαμβάνει την προστασία των φυσικών στοιχείων αυτών των συσκευών από ένα φάσμα απειλών, συμπεριλαμβανομένων κακόβουλων επιθέσεων, μη εξουσιοδοτημένης πρόσβασης και παραβίασης. Μία από τις κύριες ανησυχίες στην ασφάλεια υλικού IoT είναι η αποτροπή μη εξουσιοδοτημένης πρόσβασης. Δεδομένης της ποικιλίας των εφαρμογών IoT, οι συσκευές ενδέχεται να χειρίζονται ευαίσθητες πληροφορίες, όπως προσωπικά δεδομένα υγείας ή κρίσιμες βιομηχανικές παραμέτρους. Επιπλέον, η φυσική ασφάλεια των συσκευών IoT είναι πρωταρχικής σημασίας. Τα τρωτά σημεία στο επίπεδο υλικού μπορεί να έχουν επικίνδυνα αποτελέσματα, θέτοντας σε κίνδυνο το συνολικό δίκτυο και ενδεχομένως επιτρέποντας μεγάλης κλίμακας επιθέσεις στον κυβερνοχώρο.

Λέξεις κλειδιά: *Διαδίκτυο, διαδίκτυο των πραγμάτων, κυβερνοεπιθέσεις, ασφάλεια υλικού, λογισμικό, ετικέτες αναγνώρισης, δίκτυα επικοινωνίας, ασύρματα δίκτυα, τεχνητή νοημοσύνη, τεχνολογία blockchain*

ABSTRACT

The Internet of Things (IoT) has transformed human society and its activities. From smart homes to industrial automation, the proliferation of IoT devices has brought convenience and efficiency. However, this interconnected landscape also introduces many security challenges, making it imperative to incorporate strong hardware security measures into IoT devices. Unlike traditional computing systems, IoT devices often operate at the edge of networks, collecting and transmitting sensitive data. Hardware security in this context involves protecting the physical components of these devices from a range of threats, including malicious attacks, unauthorized access and tampering. One of the main concerns in IoT hardware security is preventing unauthorized access. Given the variety of IoT applications, devices may handle sensitive information such as personal health data or critical industrial parameters. Additionally, the physical security of IoT devices is paramount. Vulnerabilities at the hardware level can have dangerous effects, compromising the entire network and potentially enabling large-scale cyber-attacks.

Keywords: *Internet, internet of things, cyber-attacks, hardware security, software, identification tags, communication networks, wireless networks, artificial intelligence, blockchain technology*

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ - ΔΙΑΓΡΑΜΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΕΔΙΑΓΡΑΜΜΑΤΩΝ - ΕΙΚΟΝΩΝ

Εισαγωγή

Ο όρος Internet of Things (IoT) χρησιμοποιείται για να περιγράψει ένα διευρυνόμενο οικοσύστημα φυσικών αντικειμένων ή στοιχείων που διασυνδέονται μεταξύ τους και το Διαδίκτυο. Οι συσκευές IoT αποτελούνται από ένα ευρύ και ετερογενές φάσμα έμψυχων ή άψυχων αντικειμένων και, σε αυτό το πλαίσιο, ένα άτομο με εμφύτευμα που παρακολουθεί τον καρδιακό ρυθμό ή ακόμα και ένα κατοικίδιο που έχει βιοτσίπ μπορεί να ανήκει στο IoT.

Αυτές οι συσκευές κυμαίνονται από οικιακές συσκευές, όπως μηχανές καφέ ή έξυπνους λαμπτήρες, έως εξελιγμένα εργαλεία για χρήση στον βιομηχανικό αυτοματισμό. Το IoT έχει φέρει επανάσταση και προκαλεί αλλαγές σε όλους σχεδόν τους κλάδους της οικονομίας και των ανθρωπίνων δραστηριοτήτων και οι επιχειρήσεις υιοθετούν αυτήν την τεχνολογία για να αυξήσουν τα ανταγωνιστικά τους πλεονεκτήματα.

Κυριότερος τομέας εφαρμογής είναι το Industrial IoT (IIoT) ή το βιομηχανικό Διαδίκτυο ή το Industry 4.0, δηλαδή μια εφαρμογή του IoT στον βιομηχανικό τομέα, όπου τα συστήματα διασυνδέονται με διάφορες τεχνολογίες προκειμένου να αποκτήσουν έλεγχο, να λειτουργήσουν και να κατευθύνουν μέσω ασύρματου δικτύου, διάφορες εργασίες. Το IoT έχει τις ρίζες του στην αυτοματοποίηση της δεκαετίας του 1950, όπου για πρώτη φορά χρησιμοποιήθηκαν ρομπότ σε βιομηχανικές παραγωγές, ενώ με την εξέλιξη των υπολογιστών και του λογισμικού δημιουργήθηκαν τα πρώτα κλειστά εσωτερικά δίκτυα που λειτουργούσαν τις ρομποτικές συσκευές και τις συσκευές ελέγχου. Η διάθεση του διαδικτύου στο κόσμο ελεύθερα και η καθολική του χρήση επέτρεψε την διασύνδεση όλο και περισσοτέρων συσκευών με αποτέλεσμα τα δημιουργηθεί ο όρος διαδίκτυο των πραγμάτων (Internet of Things), ενώ σήμερα ο τεράστιος αριθμός διασυνδεμένων συσκευών, ανθρώπων και διαδικασιών σε κάθε ανθρώπινη δραστηριότητα έχει δημιουργήσει τον όρο διαδίκτυο των πάντων (Internet of Everything - IoE).

Οι εφαρμογές IoT αυξάνονται και χρησιμοποιούνται σε πολλούς τομείς με τη χρήση έξυπνων εφαρμογών όπως η υγειονομική περίθαλψη, οι έξυπνες πόλεις, τα δίκτυα

υποδομών, η γεωργία, τα συστήματα εφοδιασμού, η ναυτιλία, οι μεταφορές, η άμυνα κ.λ.π.

Με τον ίδιο τρόπο, το IoT μεταμορφώνει τον τρόπο ζωής και την εργασία και για το λόγο αυτό η ζήτηση για έξυπνα προϊόντα αυξάνεται συνεχώς. Μεγάλες βιομηχανίες και νεοφυείς επιχειρήσεις ανταγωνίζονται μεταξύ τους για να κυριαρχήσουν στην αγορά με τις νέες υπηρεσίες και τα προϊόντα IoT τους, ξεκλειδώνοντας την επιχειρηματική αξία του IoT.

Παρά την αυξανόμενη δημοτικότητά του, τα οφέλη και τις αποδεδειγμένες δυνατότητές του, το IoT βρίσκεται ακόμα στην έναρξη της αξιοποίησης του σε ευρεία κλίμακα και αντιμετωπίζει πολλές τεχνικές προκλήσεις. Μεταξύ αυτών, ζητήματα συνδεσιμότητας, συμβατότητα/διαλειτουργικότητα μεταξύ συσκευών και συστημάτων, έλλειψη τυποποίησης, διαχείριση τεράστιων ποσοτήτων δεδομένων και ακόμη έλλειψη εργαλείων για ελέγχους και έρευνες. Η απουσία ενιαίων προτύπων και πρωτοκόλλων ασφαλείας για συσκευές IoT έχει δημιουργήσει ένα κατακερματισμένο τοπίο όπου διαφορετικοί κατασκευαστές εφαρμόζουν διαφορετικά μέτρα ασφαλείας. Αυτή η έλλειψη τυποποίησης περιπλέκει τις προσπάθειες ρύθμισης και διασφάλισης της συνολικής ασφάλειας του IoT. Καθώς οι συσκευές IoT διασυνδέονται και μοιράζονται δεδομένα, τα τρωτά σημεία σε μία συσκευή μπορούν να επηρεάσουν ένα ολόκληρο δίκτυο ή σύστημα. Η ενσωμάτωση συσκευών IoT τρίτων σε υπάρχοντα συστήματα χωρίς τα αναγκαία επίπεδα ασφάλειας μπορεί να δημιουργήσει άγνωστους κινδύνους και δυσλειτουργία ολόκληρου του συστήματος.

Οι κυριότερες όμως ανησυχίες εστιάζονται στις επιπτώσεις ασφάλειας των πολιτών από τις εφαρμογές αυτών των συστημάτων αλλά και για το απόρρητο των δεδομένων και την παραβίαση της ιδιωτικής ζωής. Οι συσκευές IoT συλλέγουν τεράστιες ποσότητες δεδομένων από χρήστες, συχνά χωρίς ρητή συναίνεση ή ενημέρωση. Οι ευαίσθητες προσωπικές πληροφορίες, τα δεδομένα τοποθεσίας και τα μοτίβα συμπεριφοράς ενδέχεται να συλλέγονται και να εκμεταλλεύονται δυνητικά για εμπορικούς σκοπούς ή κακόβουλη πρόθεση.

Σε ορισμένες εφαρμογές IoT, όπως ιατρικές συσκευές και αυτόνομα οχήματα, οι

παραβιάσεις της ασφάλειας θα μπορούσαν να έχουν απειλητικές συνέπειες για τη ζωή των ανθρώπων. Η παραβίαση ή ο μη εξουσιοδοτημένος έλεγχος τέτοιων συσκευών μπορεί να οδηγήσει σε ατυχήματα ή επιβλαβείς ενέργειες.

Σε ένα ακόμη χειρότερο σενάριο, διατυπώνονται ανησυχίες για την αυτοματοποιημένη χρήση IoT συσκευών που επεμβαίνουν σε κρίσιμες αποφάσεις λειτουργίας συσκευών ή και συστημάτων που έχουν αντίκτυπο σε χιλιάδες ή και εκατομμύρια ανθρώπους. Μια επίθεση σε ένα δίκτυο αισθητήρων που ελέγχουν τη διανομή του ρεύματος, ή του νερού για τα νοικοκυριά μπορεί να έχει καταστροφικές συνέπειες για μεγάλα τμήματα πληθυσμού.

Η πολύπλοκη αλυσίδα εφοδιασμού που εμπλέκεται στην κατασκευή συσκευών IoT αφήνει περιθώρια για συμβιβασμούς σε διάφορα στάδια, από την προμήθεια εξαρτημάτων έως τη συναρμολόγηση. Πολλές συσκευές IoT έχουν σχεδιαστεί με πρωταρχική έμφαση στη λειτουργικότητα και τη σχέση κόστους-αποτελεσματικότητας, γεγονός που οδηγεί σε ανεπαρκή επίπεδα της ασφάλειας των συσκευών και κατ΄ επέκταση των δικτύων που χρησιμοποιούνται.

Ο τεράστιος όγκος και η ποικιλομορφία των συσκευών IoT καθιστούν πρόκληση για τους κατασκευαστές να διατηρήσουν συνεπή πρότυπα ασφαλείας σε όλους τους τομείς. Η ραγδαία ανάπτυξη της τεχνολογίας IoT συχνά ξεπερνά τα ρυθμιστικά πλαίσια, γεγονός που καθιστά δύσκολο για τις εθνικές αρχές να συμβαδίζουν με τα αναδυόμενα ζητήματα ασφάλειας. Η παγκόσμια φύση του IoT μέσω της συνδεσιμότητας του με το διαδίκτυο, παρουσιάζει εμπόδια στην επιβολή ενιαίων κανονισμών ασφάλειας και απορρήτου.

Δομή της εργασίας

Στο πρώτο κεφάλαιο αναλύεται το διαδίκτυο των πραγμάτων, το ιστορικό εμφάνισης του, ορισμοί και έννοιες, καθώς και οι εφαρμογές και περιπτώσεις χρήσης IoT.

Στο δεύτερο κεφάλαιο αναλύεται η λειτουργία και οι επικοινωνίες του IoT, μέσω ετικετών RFID.

Στο τρίτο κεφάλαιο παρουσιάζονται οι βασικές αρχές ασφάλειας Υλικού IoT, με τα μοντέλα και την αναγνώριση απειλών.

Στο τέταρτο κεφάλαιο αναλύεται η σχεδίαση δοκιμή και αξιολόγηση ασφάλειας και η κρυπτογράφηση σε επίπεδο υλικού.

Στο πέμπτο κεφάλαιο παρουσιάζονται οι αναδυόμενες τάσεις στην ασφάλεια υλικού για το IoT, η ασφάλεια υλικού IoT και η τεχνητή νοημοσύνη, η ασφάλεια υλικού IoT και λύσεις με την τεχνολογία Blockchain και οι Επιπτώσεις και κίνδυνοι από την ευρεία χρήση του IoT.

ΚΕΦΑΛΑΙΟ 1. Διαδίκτυο των πραγμάτων IoT

1.1 Εισαγωγή

Η ταχεία επέκταση του Διαδικτύου των Πραγμάτων (IoT) ενσωματώνεται όλο και περισσότερο στις καθημερινές λειτουργίες των ανθρώπων και των διαφόρων δραστηριοτήτων. Τα δίκτυα IoT αυτοματοποιούν σημαντικές υπηρεσίες σε διάφορες εργασίες, εργασίες από τις οποίες εξαρτώνται άτομα, επιχειρήσεις, δημόσιοι οργανισμοί, υποδομές και δίκτυα υποστήριξης, υπογραμμίζοντας την αυξημένη σημασία της διασφάλισης της ασφάλειας για συσκευές και δεδομένα (Parsons, et al, 2023).

Ο όρος διαδίκτυο των πραγμάτων δεν αναφέρεται σε συγκεκριμένες συσκευές ή τεχνολογία, αλλά περιλαμβάνει ένα τεράστιο πεδίο με μια ποικιλία καινοτόμων τεχνολογιών, η καθεμία συχνά διαφορετική από τις άλλες. Ο πρωταρχικός στόχος είναι η απρόσκοπτη ενσωμάτωση της συνδεσιμότητας και της ευφυΐας σε ένα ευρύ φάσμα συσκευών και λειτουργιών. Στον πυρήνα του IoT είναι η ικανότητα συλλογής δεδομένων σε πραγματικό χρόνο από πολλές έξυπνες συνδεδεμένες συσκευές. Αυτά τα δεδομένα στη συνέχεια μεταδίδονται μέσω του Διαδικτύου ή μέσω του cloud, όπου υποβάλλονται σε επεξεργασία, ανάλυση και εφαρμογή εξελιγμένων τεχνικών για τη δημιουργία μοναδικών προτάσεων αξίας. Μέσω αυτών των προηγμένων μεθόδων ανάλυσης και μεγάλων δεδομένων, το IoT έχει τη δυνατότητα να παράγει περίπλοκα συστήματα πληροφοριών που ξεπερνούν τις συλλογικές δυνατότητες μεμονωμένων στοιχείων.

1.2 Ιστορικό του διαδικτύου των πραγμάτων

Η χρήση του Διαδικτύου των Πραγμάτων (IoT) όπως είναι γνωστή σήμερα, είναι μια σχετικά πρόσφατη εξέλιξη που άρχισε να εφαρμόζεται στα τέλη του 20ου αιώνα. Η ιδέα του IoT περιστρέφεται γύρω από την ιδέα της σύνδεσης καθημερινών αντικειμένων και συσκευών στο διαδίκτυο, επιτρέποντάς τους να επικοινωνούν, να μοιράζονται δεδομένα και να εκτελούν ενέργειες χωρίς άμεση ανθρώπινη παρέμβαση (Wang, et al, 2021)

Η έννοια όμως των διασυνδεμένων συσκευών δημιουργήθηκε από τη δεκαετία του 1950, ειδικά στην βιομηχανία και θεωρείται κεντρικό συστατικό της 3ης βιομηχανικής επανάστασης, παράλληλα με την ανάπτυξη των υπολογιστών και του λογισμικού εκείνη την εποχή. Ο αυτοματισμός και η ρομποτική τεχνολογία με τη βοήθεια των πρώτων υπολογιστών μεταμόρφωσαν τη βιομηχανία, αλλά παρόλα αυτά δεν έπαυαν να είναι μια κλειστή και εξειδικευμένη διαδικασία, που αφορούσε γραμμές παραγωγής και μηχανήματα. (Nilanjan et al, 2018).

Η εξέλιξη των πληροφοριακών συστημάτων από την δεκαετία του 1960 – 1990 δημιούργησε τη πλατφόρμα ανάπτυξης των διασυνδεμένων συσκευών, πριν ακόμη και από την διάθεση του διαδικτύου για ευρεία χρήση. Η διασύνδεση συσκευών υπάρχει εδώ και χρόνια, σε διάφορες μορφές. Οι τράπεζες διαχειριζόταν και διαχειρίζονται μεγάλα, κατανεμημένα δίκτυα αυτοματοποιημένων ταμειακών μηχανών (ATM). Οι έμποροι λιανικής διαχειρίζονται μεγάλα δίκτυα σημείων πώλησης (POS), καθώς και εκτεταμένες αναπτύξεις ετικετών αναγνώρισης ραδιοσυχνοτήτων (RFID) για την παρακολούθηση της κίνησης εκατομμυρίων ειδών αποθέματος. Οι βιομηχανικοί κατασκευαστές συνδέουν χιλιάδες συσκευές για την παρακολούθηση και τη διαχείριση της παραγωγής ενώ βοηθητικά προγράμματα αναπτύσσουν συνδεδεμένους αισθητήρες και μετρητές για να επιτρέψουν τα πάντα, από τη χρέωση πελατών έως την αντιμετώπιση προβλημάτων συντήρησης. Κάθε δίκτυο θα μπορούσε να ανέρχεται σε δεκάδες χιλιάδες συνδεδεμένες συσκευές. Κανείς μέχρι το 1999 δεν αναφερόταν σε αυτά τα αρχικά δίκτυα ως IoT καθώς υπήρχαν σημαντικές διαφορές μεταξύ τους (Kranz, 2016).

Τα δίκτυα αυτά, ασχολούνταν μόνο με έναν τύπο συνδεδεμένης συσκευής ή μίας εφαρμογής, είχαν ένα πολύ περιορισμένο και αυστηρά καθορισμένο σύνολο λειτουργιών και συχνά χρησιμοποιούσαν ιδιόκτητα πρωτόκολλα αντί IP ή το cloud, που έχουν γίνει οι κυρίαρχες επιλογές δικτύωσης και υπολογιστών σήμερα. Ωστόσο, αυτά ισοδυναμούσαν με πρώιμες προσπάθειες μεγάλης κλίμακας για σύνδεση συσκευών με κάποιο επίπεδο ενσωματωμένης νοημοσύνης και επικοινωνίας με σκοπό τη διαχείριση κρίσιμων επιχειρηματικών λειτουργιών. Ήταν οι πρόδρομοι αυτού που θεωρείται ως IoT σήμερα. Όπως ήταν αναμενόμενο, δεν ήταν επιτυχείς όλες οι αρχικές

προσπάθειες που βασίζονται στο IoT. Από την κοινοπραξία GE-Cisco Industrial Ethernet, στις πλατφόρμες ψηφιακής διαφήμισης βάσει τοποθεσίας, στις ενεργές εφαρμογές RFID στο λιανικό εμπόριο και στα φιλόδοξα σχέδια για έξυπνες πόλεις, πολλές ιδέες που γεννήθηκαν και χρησιμοποιήθηκαν στις αρχές της δεκαετίας του 2000 ήταν για τον ένα ή τον άλλο λόγο μπροστά από την εποχή τους (Kranz, 2016).

Η προέλευση του IoT εντοπίζεται στις δεκαετίες του 1980 και του 1990, όταν ερευνητές άρχισαν να συζητούν τις δυνατότητες σύνδεσης συσκευών στο διαδίκτυο, το οποίο ακόμη ήταν ένα κλειστό δίκτυο των ακαδημαϊκών ιδρυμάτων και των στρατιωτικών οργανισμών των κρατών. Ο Βρετανός επιστήμονας υπολογιστών Kevin Ashton επινόησε τον όρο «Internet of Things» το 1999 (Ashton, 2009), ενώ εργαζόταν στην Procter & Gamble. Ο Ashton εργαζόταν σε ένα πρόγραμμα χρήσης της τεχνολογίας RFID[1] (Radio-Frequency Identification) για την παρακολούθηση και τη διαχείριση του αποθέματος στις αλυσίδες εφοδιασμού (Patel, & Nishant, 2019).

Η ανάπτυξη και η ολοένα μεγαλύτερη χρήση αντικειμένων και συσκευών IoT ξεκίνησε ουσιαστικά από το βιομηχανικό τομέα, που ήδη χρησιμοποιούσε αισθητήρες για να ελέγχει ρομποτικά μηχανήματα από απόσταση με τη βοήθεια υπολογιστικών συστημάτων, αλληλοεπιδρώντας μεταξύ τους, το οποίο είναι επίσης γνωστό ως μηχανή προς- επικοινωνία μηχανής - machine-to-machine (M2M) Communication (M2M). Η εμφάνιση των κινητών τηλεφώνων στην αρχή και αργότερα τα τελευταία χρόνια, η παγκόσμια επικράτηση των έξυπνων τηλεφώνων έχει φέρει επανάσταση στις συνδεδεμένες συσκευές. Οι απλοί χρήστες με κινητό τηλέφωνο μπορούν να συνδεθούν στο ψηφιακό περιβάλλον και σε οποιαδήποτε συσκευή χρησιμοποιώντας το διαδίκτυο. Εάν αυτό επεκταθεί σε οποιαδήποτε συσκευή που είναι ψηφιακή και έχει τη δυνατότητα σύνδεσης στο διαδίκτυο, με αποτέλεσμα το εύρος των δυνατοτήτων συνδεσιμότητας να είναι τεράστιο (Salih, et al, 2022).

[1] Η αναγνώριση ραδιοσυχνοτήτων - Radio Frequency Identification (RFID) είναι μια τεχνολογία που χρησιμοποιεί ραδιοκύματα για την παθητική αναγνώριση ενός αντικειμένου με ετικέτα. Χρησιμοποιείται σε πολλές εμπορικές και βιομηχανικές εφαρμογές, από την παρακολούθηση αντικειμένων κατά μήκος μιας αλυσίδας εφοδιασμού έως την παρακολούθηση των αντικειμένων σε οποιαδήποτε ανθρώπινη δραστηριότητα. https://www.investopedia.com/terms/r/radio-frequency-identification-rfid.asp (Ανάκτηση 25.7.2023).

Η ανάπτυξη και κυρίως η πρακτική εφαρμογή του διαδικτύου των πραγμάτων (IoT), δεν ήταν εύκολη και ακόμη και σήμερα συνεχίζει να είναι μια πολύπλοκη διαδικασία καθώς εξαρτάται από την ταυτόχρονη εξέλιξη και συνεργασία πολλών άλλων καινοτόμων ψηφιακών τεχνολογιών, μια περίπλοκη συγχώνευση πολλών τεχνολογιών και εννοιών. Το IoT δεν θα μπορούσε να εξελιχθεί, αν δεν είχαν γίνει επενδύσεις στις ασύρματες τεχνολογίες επικοινωνιών και στην ανάπτυξη των δικτύων 4G, 5G και 6G στο μέλλον. Δεν θα μπορούσε να υλοποιηθεί σε τέτοιο βαθμό, αν δεν είχε αναπτυχθεί η τεχνολογία του cloud, του Blockchain, της τεχνητής νοημοσύνης και άλλων νέων τεχνολογιών που αναπτύχθηκαν και αναπτύσσονται για να αντιμετωπίσουν τις προκλήσεις και τα θέματα που δημιουργούνται συνεχώς. (Biswas & Wang, 2023).

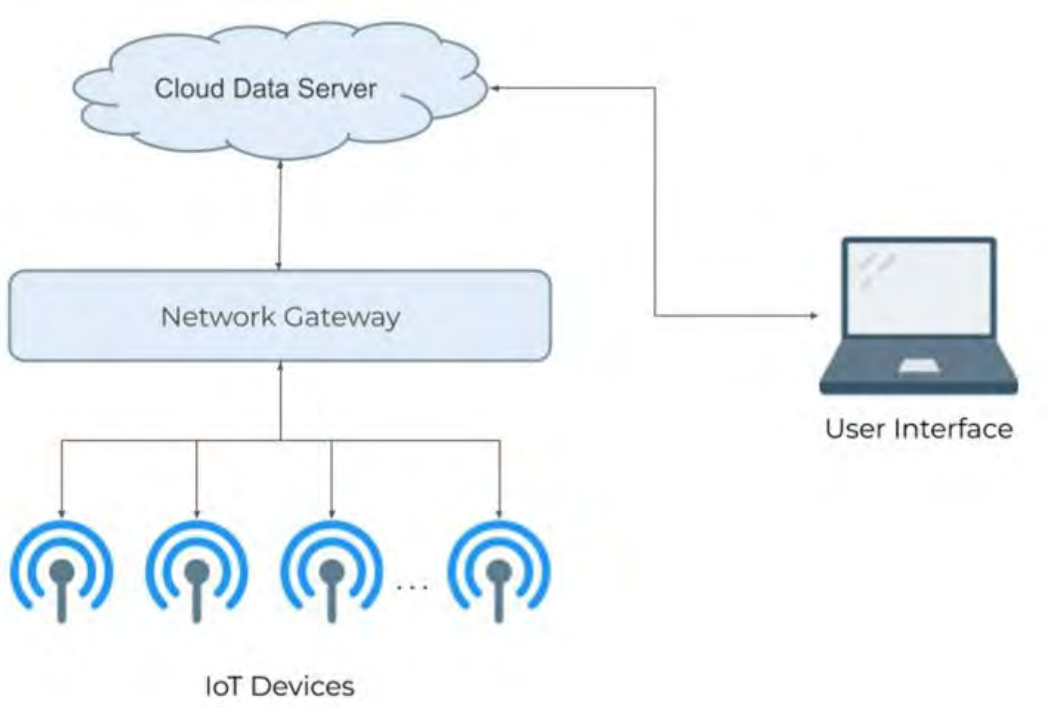
Το ασύρματο δίκτυο αισθητήρων (WSN) είναι ένας τομέας μεγάλης σημασίας τόσο για την βιομηχανία, τις υπόλοιπες οικονομικές δραστηριότητες, τις κυβερνητικές υπηρεσίες, αλλά και τους απλούς πολίτες. Ανοίγει την πόρτα σε μεγάλο αριθμό στρατιωτικών, βιομηχανικών, επιστημονικών, πολιτικών και εμπορικών εφαρμογών. Επιτρέπουν την οικονομικά αποδοτική ανίχνευση, ειδικά σε εφαρμογές όπου η ανθρώπινη παρατήρηση ή οι παραδοσιακοί αισθητήρες θα ήταν ανεπιθύμητοι, αναποτελεσματικοί, δαπανηροί ή επικίνδυνοι. Οι ασύρματοι αισθητήρες έχουν περιορισμένες δυνατότητες ενέργειας και υπολογιστικής, καθιστώντας πολλές παραδοσιακές μεθοδολογίες ασφαλείας δύσκολες ή αδύνατο να χρησιμοποιηθούν. (Oreku & Pazynyuk, 2016).

1.3 Ορισμός και χαρακτηριστικά του IoT

Ένας απλοποιημένος ορισμός του IoT είναι η γέφυρα από τον φυσικό κόσμο στον κόσμο του κυβερνοχώρου (Patel, & Nishant, 2019).

Το Internet of Things (IoT) είναι ένα δίκτυο έξυπνων πραγμάτων που μοιράζονται πληροφορίες μέσω του Διαδικτύου. Τα έξυπνα πράγματα χρησιμοποιούνται για την ανάπτυξη σε διαφορετικό περιβάλλον για την καταγραφή των πληροφοριών και ενεργοποιούνται ορισμένα συμβάντα. Διασυνδεμένες συσκευές, και αντικείμενα (πράγματα) καθώς και οι εφαρμογές τους εντοπίζονται σε μια έξυπνη πόλη, ένα έξυπνο

σπίτι, ένα ευφυές σύστημα μεταφορών, στη γεωργία και κτηνοτροφία, στην υγεία, σε ολόκληρη τη βιομηχανία, την αεροπορία, την ναυτιλία, στο σύστημα εφοδιαστικής αλυσίδας, στην ανίχνευση σεισμών, στη ρύθμιση των υποδομών σε ένα σύστημα έξυπνου δικτύου τηλεπικοινωνιών (Stergiou, et al, 2023), ουσιαστικά πλέον σε κάθε ανθρώπινη δραστηριότητα που εντάσσεται και μεταμορφώνεται στο ψηφιακό περιβάλλον (Mohanta, et al, 2020).



Σχεδιάγραμμα 1. Τυπική δομή ενός IoT συστήματος

Ανεξάρτητα από το μέγεθος ενός συστήματος IoT, η βασική δομή του είναι αυτή που εμφανίζεται στο σχεδιάγραμμα 1. IoT συσκευές που επικοινωνούν μέσω δικτύου (το οποίο μπορεί να είναι ιδιωτικό (εταιρικό ή κλειστό ελεγχόμενο), ή ακόμη και μέσω του διαδικτύου, με ένα υπολογιστή ή μια οποιαδήποτε ψηφιακή συσκευή (όπως ένα έξυπνο κινητό τηλέφωνο), που μπορεί να επεξεργαστεί και να αναλύσει τα δεδομένα και να εξάγει πληροφορίες σε λογικό χρονικό διάστημα ώστε να είναι αξιοποιήσιμες (Patel, & Nishant, 2019).

Τα χαρακτηριστικά του IoT είναι αυτά που το καθιστούν μια καινοτόμο τεχνολογία που μετασχηματίζει όλους τους κλάδους της οικονομίας και τις ανθρώπινες δραστηριότητες. Τα βασικά χαρακτηριστικών του IoT είναι:

- Συνδεσιμότητα: Οι συσκευές IoT χαρακτηρίζονται από την ικανότητά τους να συνδέονται στο διαδίκτυο ή άλλες συσκευές, επιτρέποντας την απρόσκοπτη ανταλλαγή δεδομένων. Αυτή η συνδεσιμότητα μπορεί να επιτευχθεί με διάφορα μέσα, όπως Wi-Fi, δίκτυα κινητής τηλεφωνίας, Bluetooth και ασύρματες τεχνολογίες. Αυτή η δυνατότητα επιτρέπει την επικοινωνία σε πραγματικό χρόνο και τον απομακρυσμένο έλεγχο συσκευών, καθιστώντας το IoT κατάλληλο για εφαρμογές που κυμαίνονται από έξυπνες οικίες και αυτοκίνητα έως βιομηχανικούς αυτοματισμούς και την υγεία (Anuradha & Tripathy, 2018).
- Συλλογή δεδομένων και αισθητήρες: Οι συσκευές IoT είναι εξοπλισμένες με διάφορους αισθητήρες που συλλέγουν δεδομένα από το περιβάλλον τους. Αυτοί οι αισθητήρες μπορούν να μετρήσουν θερμοκρασία, υγρασία, πίεση, φως, κίνηση και πολλά άλλα. Επιτρέπουν στις συσκευές IoT να παρακολουθούν και να συλλαμβάνουν πληροφορίες σε πραγματικό χρόνο, οι οποίες μπορούν να χρησιμοποιηθούν για ανάλυση, λήψη αποφάσεων και αυτοματισμό.
- Επεξεργασία δεδομένων και ανάλυση: Το IoT δημιουργεί τεράστιο όγκο δεδομένων. Για την εξαγωγή σημαντικών πληροφοριών από αυτά τα δεδομένα, τα συστήματα IoT συχνά ενσωματώνουν δυνατότητες επεξεργασίας δεδομένων και ανάλυσης. Οι αλγόριθμοι μηχανικής μάθησης, η τεχνητή νοημοσύνη και η ανάλυση μεγάλων δεδομένων χρησιμοποιούνται για την επεξεργασία δεδομένων στη συσκευή ή στο υπολογιστικό νέφος - cloud (Nilanjan et al, 2018).
- Διαλειτουργικότητα: Η διαλειτουργικότητα είναι ένα κρίσιμο χαρακτηριστικό του IoT, που επιτρέπει σε συσκευές διαφορετικών κατασκευαστών και οικοσυστημάτων να συνεργάζονται απρόσκοπτα. Οι προσπάθειες τυποποίησης και τα ανοιχτά πρωτόκολλα επιτρέπουν στις συσκευές IoT να επικοινωνούν και να μοιράζονται δεδομένα αποτελεσματικά, μειώνοντας τα προβλήματα συμβατότητας και ενισχύοντας ένα πιο συνδεδεμένο οικοσύστημα. Στην πράξη όμως η διαλειτουργικότητα αυτή θεωρείται μια από τις κυριότερες προκλήσεις και μια από τις μεγαλύτερες δυσκολίες που έχει να αντιμετωπίσει το IoT.
- Απομακρυσμένη παρακολούθηση και έλεγχος: Ένα από τα κύρια πλεονεκτήματα του IoT είναι η δυνατότητα απομακρυσμένης παρακολούθησης

και ελέγχου συσκευών και διαδικασιών. Αυτό το χαρακτηριστικό επιτρέπει την απομακρυσμένη συντήρηση εξοπλισμού, τον οικιακό αυτοματισμό, την παρακολούθηση υγείας από απόσταση, τα βιομηχανικά συστήματα ελέγχου, τον ασφαλή απομακρυσμένο έλεγχο κρίσιμων και επικίνδυνων υλικών και εγκαταστάσεων, τον απομακρυσμένο έλεγχο οπλικών συστημάτων κ.α. Το χαρακτηριστικό αυτό ενισχύει την αποτελεσματικότητα, μειώνει το λειτουργικό κόστος και μπορεί ακόμη και να σώσει ζωές σε κρίσιμες καταστάσεις (Anuradha & Tripathy, 2018).

- Επεκτασιμότητα: Οι λύσεις IoT μπορούν να επεκταθούν για να χρησιμοποιήσουν έναν αυξανόμενο αριθμό συσκευών και πηγών δεδομένων. Είτε πρόκειται για ένα μικρό έξυπνο οικιακό δίκτυο είτε για μια μεγάλης κλίμακας βιομηχανική ανάπτυξη, τα συστήματα IoT έχουν σχεδιαστεί για να χειρίζονται ένα διαρκώς διευρυνόμενο οικοσύστημα συνδεδεμένων συσκευών και χρηστών (Misra, et al, 2021)

- Επικοινωνία σε πραγματικό χρόνο: Πολλές εφαρμογές IoT απαιτούν επικοινωνία και απόκριση σε πραγματικό χρόνο. Για παράδειγμα, τα αυτόνομα οχήματα βασίζονται σε αποφάσεις σε κλάσματα δευτερολέπτου που βασίζονται σε δεδομένα από αισθητήρες και άλλα οχήματα. Ένα αεροσκάφος ειδικά τη στιγμή της απογείωσης – προσγείωσης λαμβάνει μεγάλο όγκο δεδομένων και εξωτερικών μετρήσεων και η ανταπόκριση του πρέπει να είναι ακαριαία. Τα δεδομένα ενός πυρηνικού εργοστασίου πρέπει να είναι διαθέσιμα σε μηδενικό χρόνο. Το χαρακτηριστικό αυτό των συσκευών IoT να παρέχει επικοινωνία σε πραγματικό χρόνο χαμηλής καθυστέρησης είναι ζωτικής σημασίας σε τέτοια σενάρια.

- Ασφάλεια και απόρρητο: Η ασφάλεια αποτελεί πρωταρχικό μέλημα στο IoT. Καθώς περισσότερες συσκευές συνδέονται, γίνονται πιθανοί στόχοι κυβερνοεπιθέσεων. Τα συστήματα IoT ενσωματώνουν χαρακτηριστικά ασφαλείας όπως κρυπτογράφηση, έλεγχος ταυτότητας και έλεγχος πρόσβασης για την προστασία δεδομένων και συσκευών. Το απόρρητο είναι εγείρει ανησυχίες και προβληματισμούς, ειδικά όταν πρόκειται για προσωπικά δεδομένα (Patel, & Nishant, 2019).

- Ενεργειακή απόδοση: Πολλές συσκευές IoT λειτουργούν με ισχύ μπαταρίας ή σε απομακρυσμένες τοποθεσίες με περιορισμένες πηγές ενέργειας. Η ενεργειακή απόδοση είναι ένα κρίσιμο χαρακτηριστικό και οι συσκευές IoT έχουν σχεδιαστεί για να ελαχιστοποιούν την κατανάλωση ενέργειας, χρησιμοποιώντας συχνά ασύρματες τεχνολογίες χαμηλής κατανάλωσης και λειτουργίες χαμηλής ενέργειας όταν δεν βρίσκονται σε χρήση.

Οι υποκείμενες τεχνολογίες περιλαμβάνουν κατανεμημένους υπολογιστές, υπολογιστικό νέφος, μηχανική μάθηση και τεχνητή νοημοσύνη, ανάλυση δεδομένων και επικοινωνία από μηχανή σε μηχανή. Ένα τυπικό σύστημα IoT αποτελείται από έξυπνα συστήματα (εφαρμογές, ελεγκτές, αισθητήρες και μηχανισμούς ασφαλείας), υποδομές επικοινωνίας δεδομένων και το πιο σημαντικό τον ανθρώπινο παράγοντα (Mahmood, 2019).

Το Διαδίκτυο των Πραγμάτων (IoT) χαρακτηρίζεται από την παρουσία διαφορετικών συσκευών. Αυτές οι συσκευές ποικίλλουν από μικρούς, ελαφρούς αισθητήρες με μικροελεγκτές (MCU) 8 bit έως πιο ισχυρούς επεξεργαστές 32/64 bit. Τα υπάρχοντα παραδοσιακά λειτουργικά συστήματα στο Διαδίκτυο και τα τυπικά λειτουργικά συστήματα για δίκτυα αισθητήρων δεν επαρκούν για να καλύψουν τις ποικίλες ανάγκες αυτής της εκτεταμένης σειράς συσκευών. Ως απάντηση σε αυτήν την πρόκληση, το RIOT OS ξεχωρίζει ως λειτουργικό σύστημα που έχει σχεδιαστεί ρητά για συσκευές χαμηλών πόρων, επιτρέποντας την ανάπτυξη σε ένα ευρύ φάσμα συσκευών. Το RIOT OS[2] υποστηρίζει τυπικό προγραμματισμό C και C++, προσφέρει δυνατότητες πολλαπλών αντιγράφων και πραγματικού χρόνου και απαιτεί μόνο ένα ελάχιστο 1,5 kB μνήμης RAM.

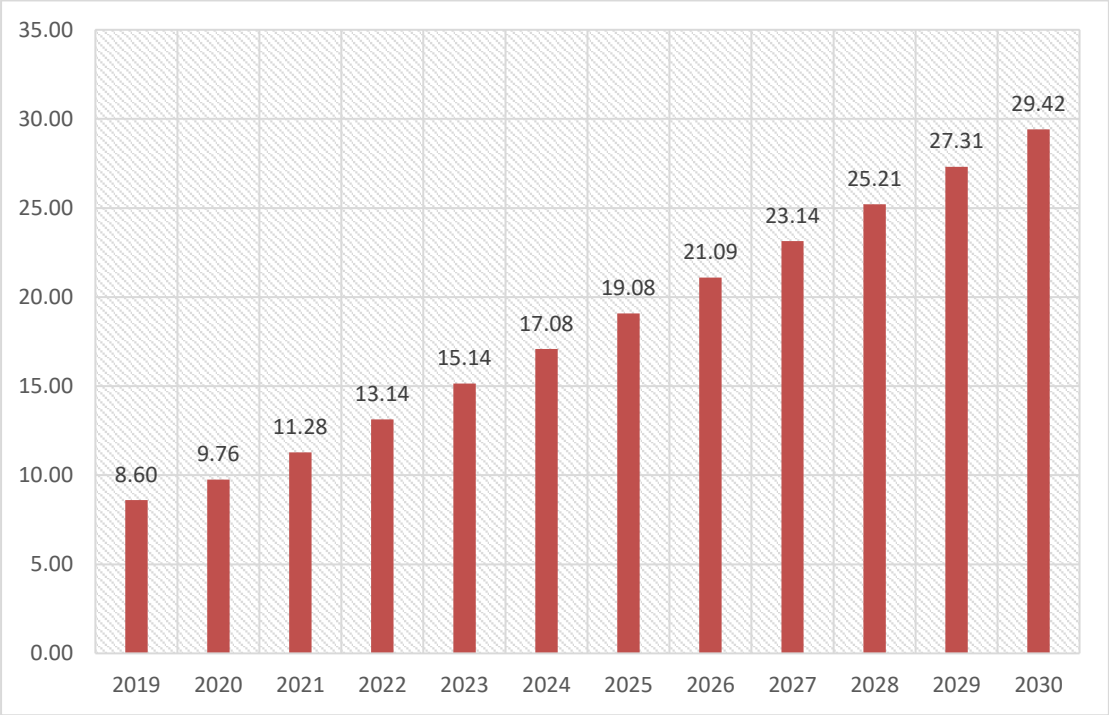
1.4 Στοιχεία χρήσης συσκευών IoT σε παγκόσμια κλίμακα

Το Διαδίκτυο των πραγμάτων είναι μία από τις τεχνολογίες που οδηγούν το Industry 4.0 και δεν αποτελεί έκπληξη το γεγονός ότι η αγορά βλέπει ένα CAGR άνω του 16% σε μια περίοδο 10 ετών (2018-2028). Παρόλο που η παγκόσμια έλλειψη ημιαγωγών

[2] https://www.riot-os.org/ RIOT OS, (Ανάκτηση 25.7.2023).

έχει επιβραδύνει την προσφορά και την ανάπτυξη της αγοράς από τα προ της πανδημίας επίπεδα, η ζήτηση για έξυπνες λύσεις που κυμαίνονται από βιομηχανικές έως περιπτώσεις χρήσης ασφαλείας εξακολουθεί να αυξάνεται. Με έσοδα άνω των 141 δισεκατομμυρίων δολαρίων ΗΠΑ το 2022, οι ΗΠΑ είναι ο ηγέτης της αγοράς, ακολουθούμενη από την Κίνα, η οποία είναι ο κορυφαίος κατασκευαστής συσκευών IoT[3].

Διάγραμμα 1. Αριθμός συνδεδεμένων συσκευών Internet of Things (IoT) παγκοσμίως από το 2019 έως το 2023, με προβλέψεις από το 2022 έως το 2030 (σε δισεκατομμύρια)



(πηγή: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ - ιδία επεξεργασία).

Ο αριθμός των συσκευών Internet of Things (IoT) παγκοσμίως προβλέπεται να διπλασιαστεί σχεδόν από 15,1 δισεκατομμύρια το 2020 σε περισσότερες από 29 δισεκατομμύρια συσκευές IoT το 2030. Το 2030, ο μεγαλύτερος αριθμός συσκευών

[3] https://www.statista.com/outlook/tmo/internet-of-things/worldwide Internet of Things - Worldwide. (Ανάκτηση 26.7.2023).

IoT θα βρίσκεται στην Κίνα με περίπου 8 δισεκατομμύρια καταναλωτές συσκευές.

Οι σημαντικότεροι κλάδοι της βιομηχανίας[4] με περισσότερες από 100 εκατομμύρια συνδεδεμένες συσκευές IoT είναι η ηλεκτρική ενέργεια, το φυσικό αέριο, η παροχή νερού και η διαχείριση απορριμμάτων, η λιανική και χονδρική πώληση, η μεταφορά και αποθήκευση και η κυβερνητικές υπηρεσίες. Η ανάπτυξη της αγοράς του Internet of Things συμπίπτει με την ανάπτυξη άλλων σημαντικών τεχνολογιών, όπως το 5G και το cloud computing. Η ανάπτυξη προτύπων επικοινωνίας 5G ανοίγει το δρόμο για ταχύτερη και ομαλότερη σύνδεση μεταξύ έξυπνων συσκευών.

Πριν την περίοδο του Covid-19, οι εκτιμήσεις για την εγκατάσταση IoT συσκευών ανέβαζαν τον αριθμό σε 50 δισεκατομμύρια το 2020-2021, αριθμός που όπως φάνηκε ήταν πολύ μεγάλος, καθώς δεν λήφθηκαν υπ' όψιν διάφοροι παράγοντες. Σύμφωνα με έρευνες η πανδημία του Covid ήταν ένας από τους παράγοντες που συνετέλεσαν στην μείωση εγκατάστασης των εκτιμωμένων συσκευών IoT (Beg, et al, 2022)

Εκτός από την πανδημία, ήδη από το 2018 η ανάπτυξη του IoT αποδείχθηκε ότι είχε υπερεκτιμηθεί[5]. Κατακερματισμένες αγορές, διαφορετικά οικοσυστήματα και οργανισμοί, παραβιάσεις ασφάλειας και απώλειες δεδομένων, έλλειψη δεξιοτήτων, προκλήσεις διαδικασιών και ολοκλήρωσης, ήταν μόνο μερικοί από τους παράγοντες που έκαναν την υιοθέτηση του IoT πιο περίπλοκη, πιο δαπανηρή και πιο επικίνδυνη. Σε πολλούς ειδικούς υπήρχε η πεποίθηση ότι το IoT θα έφερνε έναν κόσμο όπου δισεκατομμύρια συσκευές θα μπορούσαν να συνδέονται και να επικοινωνούν απρόσκοπτα. Αλλά η γεφύρωση του χάσματος μεταξύ του ψηφιακού και του φυσικού κόσμου αποδείχθηκε δυσκολότερο από το αναμενόμενο. Οι περισσότερες αναπτύξεις και εφαρμογές απαιτούσαν τεχνολογική, αρχιτεκτονική και οργανωτική ενοποίηση με παλαιού τύπου λύσεις, κάτι πολύ δύσκολο. Σε μια έρευνα που πραγματοποιήθηκε σε πάνω από 1.800 διευθυντές επιχειρήσεων και πληροφορικής έδειξε ότι το κόστος και η διάρκεια υλοποίησης ήταν τα κύρια εμπόδια που εμποδίζουν την υιοθέτηση του IoT.

[4] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ Number of connected Internet of Things (IoT) devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030, (Ανάκτηση 26.7.2023).

[5] https://www.forbes.com/sites/forbestechcouncil/2019/05/02/the-iot-yesterdays-predictions-vs-todays-reality/?sh=4d0eed11512b The IoT: Yesterday's Predictions Vs. Today's Reality, (Ανάκτηση 29.7.2023).

1.5 Εφαρμογές και περιπτώσεις χρήσης IoT

Η εξάπλωση του δικτύου IoT και οι ποικίλες εφαρμογές του, έχει πλέον καθοριστική επίδραση στα άτομα, τη κοινωνία, την υγεία, τη βιομηχανία και τις επιχειρηματικές δραστηριότητες και το περιβάλλον (Mocnej, et al, 2018).

1.5.1 Βιομηχανικοί αισθητήρες και ελεγκτές IoT

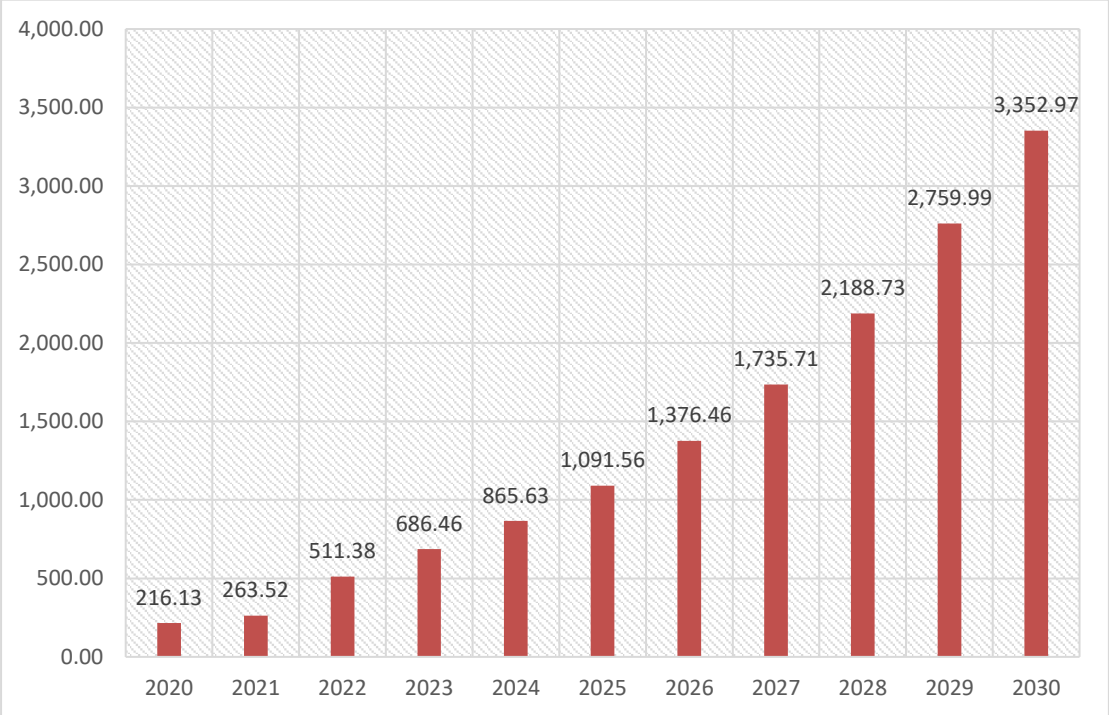
Όπως αναφέρθηκε μορφές διασυνδεμένων ρομποτικών συσκευών και αισθητήρων χρησιμοποιείται εδώ και πολλά χρόνια στη βιομηχανία. Η εξειδικευμένη μορφή του IoT που φέρνει επανάσταση στον βιομηχανικό χώρο είναι το βιομηχανικό διαδίκτυο των πραγμάτων - Industrial Internet of Things (IIoT), το οποίο επιτρέπει τη σύνδεση στο διαδίκτυο όλων των επιμέρους βιομηχανικών μονάδων (Mukherjee, et al, 2021).

Η ευρεία χρήση ψηφιακών καινοτόμων τεχνολογιών στη βιομηχανία δημιούργησε τον όρο βιομηχανία 4.0 - Industry 4.0[6], μια ψηφιακή βιομηχανική επανάσταση, όπου στόχος είναι η ψηφιοποίηση ολόκληρης της διαδικασίας παραγωγής με ελάχιστη ανθρώπινη ή χειροκίνητη παρέμβαση. Έννοιες όπως η έξυπνη κατασκευή, τα έξυπνα εργοστάσια και το Industrial Internet of Things (IIoT) (Boyes, et al, 2018), είναι μερικές από τις βασικές λέξεις-κλειδιά της βιομηχανίας 4.0. Η επιτυχία του Industrial 4.0 έγκειται σε μεγάλο βαθμό στην επιτυχή ενσωμάτωση και προσαρμογή διαφόρων υφιστάμενων και αναδυόμενων τεχνολογιών με την τρέχουσα διαδικασία παραγωγής. Εκτός από τη μεγαλύτερη αποτελεσματικότητα και παραγωγικότητα, τα οφέλη του IIoT περιλαμβάνουν σημαντική μείωση του κόστους και των ζημιών για τις εταιρείες. Μια πολλά υποσχόμενη περίπτωση χρήσης του IIoT είναι η προγνωστική συντήρηση, η οποία επιτρέπει στις εταιρείες να εντοπίζουν πιθανές αστοχίες και να αποφεύγουν δαπανηρούς χρόνους διακοπής λειτουργίας. (Nayyar & Kumar, 2020).

[6] Το Industry 4.0 φέρνει επανάσταση στον τρόπο με τον οποίο οι εταιρείες κατασκευάζουν, βελτιώνουν και διανέμουν τα προϊόντα τους. Οι κατασκευαστές ενσωματώνουν νέες τεχνολογίες, συμπεριλαμβανομένου του Διαδικτύου των πραγμάτων (IoT), του υπολογιστικού νέφους και της ανάλυσης δεδομένων, καθώς και της τεχνητής νοημοσύνης και της μηχανικής μάθησης στις εγκαταστάσεις παραγωγής τους και σε όλες τις δραστηριότητές τους. https://www.ibm.com/topics/industry-4-0 (Ανάκτηση 26.7.2023).

Εφαρμογές IIoT που σχετίζονται με έξυπνα εργοστάσια, έξυπνη αποθήκευση, πρόγνωση και απομακρυσμένη συντήρηση, παρακολούθηση εμπορευμάτων και μεταφορών, παρακολούθηση αποθεμάτων, παρακολούθηση περιουσιακών στοιχείων και διαχείριση απόδοσης, παρακολούθηση βιομηχανικού περιβάλλοντος, η παρακολούθηση της ασφάλειας και πολλά άλλα, προβλέπεται να γίνουν πιο αποτελεσματικά και παραγωγικά και με τη σειρά τους, να επιτρέψουν τον ψηφιακό μετασχηματισμό στις εταιρείες, στην πραγματικότητα σε ολόκληρο τον βιομηχανικό κλάδο (Boyes, et al, 2018).

Διάγραμμα 2. Μέγεθος της αγοράς του Industrial Internet of Things (IIoT) παγκοσμίως από το 2020 έως το 2030 (σε δισεκατομμύρια δολάρια ΗΠΑ)



(πηγή: https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/ - ιδία επεξεργασία)

Ενώ υπήρξαν συστήματα που μπορούν να παρακολουθούν την πρόοδο της κατασκευής και της παραγωγής, το Industrial IoT παρέχει πολύ πιο περίπλοκο έλεγχο στους διαχειριστές. Στο περιβάλλον του IIoT, πολλές τεχνολογίες ενσωματώνονται στις εργοστασιακές μηχανές, στα υλικά και στις μεθόδους, όπως η μηχανική εκμάθηση, η τεχνητή νοημοσύνη (AI), η επικοινωνία μηχανής με τη μηχανή (M2M), ο

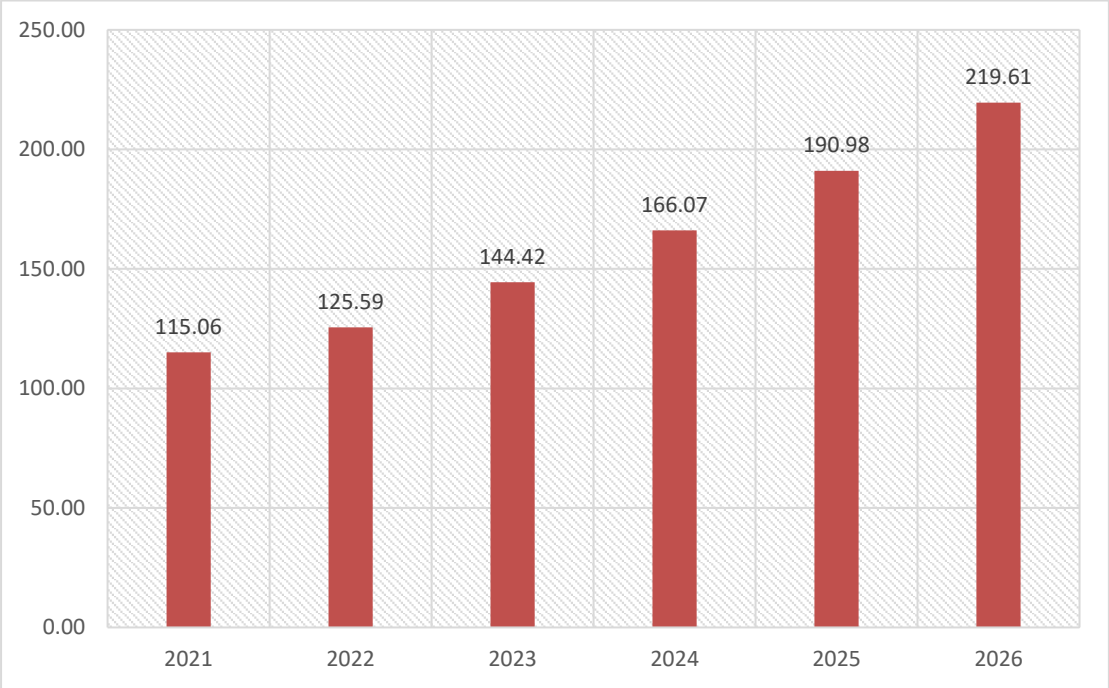
κατανεμημένος υπολογισμός, ο υπολογισμός νέφους, ο υπολογισμός αιχμής και η ανάλυση δεδομένων. Για το λόγο αυτό η τεχνολογία IIoT είναι μια συγχώνευση διαφορετικών τεχνολογιών, τεχνολογιών που αναπτύχθηκαν και αναπτύσσονται τα τελευταία χρόνια αλλά και βελτίωση τεχνολογιών που υπάρχουν στο βιομηχανικό υπόβαθρο εδώ και πολλά χρόνια (Mahmood, 2019).

1.5.2 Συστήματα IoT στην αυτοκινητοβιομηχανία

Η αυτοκινητοβιομηχανία είναι ένας από τους μεγαλύτερους κλάδους παραγωγής στον κόσμο, παράγοντας πάνω από 70 εκατομμύρια μονάδες ετησίως. Σε παγκόσμιο επίπεδο, η αυτοκινητοβιομηχανία απέφερε έσοδα 3 τρισεκατομμυρίων δολαρίων, που αντιστοιχεί στο 3,65% του συνολικού παγκόσμιου ΑΕΠ. Η εισαγωγή της τεχνολογίας IoT στον τομέα της αυτοκινητοβιομηχανίας έχει ανοίξει νέες ευκαιρίες τόσο για τους κατασκευαστές αυτοκινήτων όσο και για τους καταναλωτές παγκοσμίως. Το IoT στην αυτοκινητοβιομηχανία έχει γίνει σημαντικός κόμβος για διάφορες ευέλικτες εφαρμογές, εξυπηρετώντας βιομηχανικούς και εμπορικούς σκοπούς. Αυτές οι εφαρμογές IoT, που κυμαίνονται από διασυνδεδεμένα οχήματα έως αυτοματοποιημένα συστήματα μεταφορών, έχουν επηρεάσει σε μεγάλο βαθμό την παγκόσμια αυτοκινητοβιομηχανία, οδηγώντας σε πρωτοποριακές καινοτομίες όπως συνδεδεμένα και αυτόνομα οχήματα (Beg, et al, 2022).

Οι τελευταίες έρευνες και πρακτικές στην αυτοκινητοβιομηχανία περιλαμβάνουν εφαρμογή τεχνολογιών όπως ασύρματος κατανεμημένος αισθητήρας, ενσωματωμένο σύστημα ελέγχου βλαβών, υψηλότερης απόδοσης και εξαιρετικά χαμηλές εκπομπές κινητήρων εσωτερικής καύσης, τεχνολογία μπαταρίας και κυψελών καυσίμου υψηλής απόδοσης και έξυπνος μετατροπέας, δίνοντας τη δυνατότητα παραγωγής ασφαλέστερων, εξυπνότερων, μηδενικών εκπομπών και ενεργειακά αποδοτικών οχημάτων τα επόμενα χρόνια (Ghosh, et al, 2022)

Διάγραμμα 3. Μέγεθος αγοράς του Internet of Things (IoT) για αυτοκίνητα το 2021, με πρόβλεψη έως το 2026 (σε δισεκατομμύρια δολάρια ΗΠΑ)



(πηγή: https://www.statista.com/statistics/423083/iot-units-installed-base-within-automotive-segment/ - ιδία επεξεργασία)

Αν και υπάρχουν πλήθος εφαρμογών IoT που χρησιμοποιούνται στα σύγχρονα αυτοκίνητα, τη μεγάλη πρόκληση για την αυτοκινητοβιομηχανία είναι η εισαγωγή των αυτόνομων οχημάτων (χωρίς επέμβαση οδηγού) και τα μεγάλα ζητήματα ασφάλειας που καλείται να επιλύσει ο κλάδος. Τα αυτόνομα οχήματα - Autonomous Vehicles (AV) αντιμετωπίζουν συνεχώς κινδύνους ασφαλείας που σχετίζονται με μη εξουσιοδοτημένη πρόσβαση και ανεπαρκή προστασία έναντι κακόβουλων παραγόντων, γεγονός που μπορεί να θέσει σε κίνδυνο τις ευαίσθητες πληροφορίες του κατόχου του αυτοκινήτου. Η περιορισμένη υιοθέτηση και η εμπιστοσύνη του κοινού στα AV παρεμποδίζονται κυρίως από ανησυχίες για την ασφάλεια στον κυβερνοχώρο και το απόρρητο (Biswas & Wang, 2023).

Σε έρευνα που πραγματοποιήθηκε το 2015 με 5.000 ερωτηθέντες σε 109 χώρες (Kyriakidis, et al, 2015), αποκάλυψε την επιφυλακτικότητα και τις ανησυχίες των ανθρώπων σχετικά με την κατάχρηση προσωπικών πληροφοριών μέσω του λογισμικού των οχημάτων με όλα τα επίπεδα αυτοματισμού. Η κατάσταση δεν είχε βελτιωθεί πολύ μέχρι το 2022, καθώς οι κύριες απειλές δεν είχαν εξαλειφθεί (Biswas & Wang, 2023).

1.5.3 Έξυπνες πόλεις με τη χρήση συσκευών IoT

Η μεγάλη αστικοποίηση που συμβαίνει τα τελευταία χρόνια σε ολόκληρο το κόσμο, απόρροια της αύξησης του πληθυσμού του πλανήτη, οδήγησε τις μεγάλες πόλεις να στραφούν στις καινοτόμες ψηφιακές τεχνολογίες, προκειμένου να αντιμετωπίσουν τα προβλήματα οργάνωσης, λειτουργικότητας, μετακίνησης και προστασίας του περιβάλλοντος, δημιουργώντας την έννοια της έξυπνης πόλης (Augusto, 2021, (Halegoua, 2020).

Το παγκόσμιο μέγεθος της αγοράς του IoT στις Έξυπνες Πόλεις[7] αναμένεται να αυξηθεί από 130,6 δισεκατομμύρια δολάρια ΗΠΑ το 2021 σε 312,2 δισεκατομμύρια δολάρια ΗΠΑ έως το 2026, με σύνθετο ετήσιο ρυθμό ανάπτυξης (CAGR[8]) 19,0% κατά την περίοδο πρόβλεψης. Διάφοροι παράγοντες, όπως η αύξηση της υιοθέτησης της τεχνολογίας IoT για τη διαχείριση υποδομών και την παρακολούθηση της πόλης και η εκθετική αύξηση του αστικού πληθυσμού αναμένεται να οδηγήσουν την υιοθέτηση του IoT σε λύσεις και υπηρεσίες έξυπνων πόλεων.

Οι έξυπνες πόλεις, που χρησιμοποιούν συσκευές Internet of Things (IoT), αντιπροσωπεύουν ένα μετασχηματιστικό παράδειγμα στον αστικό σχεδιασμό και τη διακυβέρνηση. Εφαρμογές με τη βοήθεια του IoT εντοπίζονται στις παρακάτω λειτουργίες :

- Βελτιωμένη απόδοση και βιωσιμότητα: Οι συσκευές IoT σε έξυπνες πόλεις παρέχουν δεδομένα σε πραγματικό χρόνο για διάφορες λειτουργίες της αστικής ζωής, όπως ο έλεγχος της κυκλοφορίας, η κατανάλωση δημόσιας ενέργειας, η διαχείριση απορριμμάτων και η ποιότητα του αέρα. Αυτά τα δεδομένα επιτρέπουν στους πολεοδόμους να βελτιστοποιήσουν την κατανομή των πόρων

[7] https://www.marketsandmarkets.com/Market-Reports/iot-smart-cities-market-215714954.html IoT in Smart Cities, (Ανάκτηση 10.8.2023).

[8] Ο σύνθετος ετήσιος ρυθμός ανάπτυξης (CAGR) είναι ο ρυθμός απόδοσης (RoR) που θα απαιτούνταν για να αυξηθεί μια επένδυση από το αρχικό της υπόλοιπο στο τελικό υπόλοιπό της, υποθέτοντας ότι τα κέρδη επανεπενδύθηκαν στο τέλος κάθε περιόδου της διάρκειας ζωής της επένδυσης. (Ανάκτηση 10.8.2023, από https://www.investopedia.com/terms/c/cagr.asp)

και να μειώσουν τα απόβλητα, οδηγώντας τελικά σε πιο βιώσιμα και αποδοτικά αστικά περιβάλλοντα.

- Βελτιωμένη υποδομή: Οι έξυπνες υποδομές, όπως τα φανάρια με δυνατότητα IoT και τα συστήματα δημόσιων μεταφορών, ενισχύουν την κινητικότητα και μειώνουν τη κυκλοφοριακή συμφόρηση των δρόμων Τα συστήματα διαχείρισης της κυκλοφορίας μπορούν να επανά-δρομολογήσουν τα οχήματα με βάση δεδομένα κυκλοφορίας σε πραγματικό χρόνο, μειώνοντας τους χρόνους μετακίνησης και μειώνοντας τις εκπομπές ρύπων. Η ενσωμάτωση αυτόνομων οχημάτων σε έξυπνα συστήματα μεταφορών πόλεων θα μειώσει την κυκλοφοριακή συμφόρηση και θα ενισχύσει την κινητικότητα. Οι αισθητήρες IoT θα διευκολύνουν την επικοινωνία και τον συντονισμό μεταξύ οχημάτων και υποδομών (Powell, 2021).

- Περιβαλλοντικά οφέλη: Με την παρακολούθηση και τον έλεγχο της χρήσης ενέργειας σε δημόσια κτίρια, φωτισμό δρόμων και επιχειρήσεις κοινής ωφέλειας, οι έξυπνες πόλεις μπορούν να μειώσουν σημαντικά την κατανάλωση ενέργειας και τις εκπομπές αερίων του θερμοκηπίου. Αυτό συμβάλλει στην περιβαλλοντική βιωσιμότητα και βοηθά στην καταπολέμηση της κλιματικής αλλαγής (Albino, et al, 2015).

- Δημόσια ασφάλεια: Οι συσκευές IoT υποστηρίζουν την παρακολούθηση σε όλη την πόλη, με συστήματα έγκαιρης προειδοποίησης και την απόκριση έκτακτης ανάγκης. Αυτές οι τεχνολογίες μπορούν να ανιχνεύσουν ταχύτερα ατυχήματα, πυρκαγιές ή φυσικές καταστροφές, διασφαλίζοντας ταχύτερη και αποτελεσματικότερη απόκριση για την προστασία των κατοίκων και των υποδομών.

- Συμμετοχή του Πολίτη: Οι μελλοντικές έξυπνες πόλεις θα δώσουν προτεραιότητα στη συμμετοχή των πολιτών στη λήψη αποφάσεων. Οι πλατφόρμες που τροφοδοτούνται από το IoT θα επιτρέψουν στους κατοίκους να παρέχουν σχόλια και να συμβάλλουν στη διαμόρφωση αστικών πολιτικών και υπηρεσιών (Augusto, 2021).

Οι προκλήσεις όμως που αντιμετωπίζουν οι έξυπνες πόλεις, προκαλούν ανησυχία και προβληματισμό, παρόλες τις θετικές πλευρές των εφαρμογών IoT.

Οι προκλήσεις εντοπίζονται κυρίως σε:

- Ανησυχίες για το απόρρητο και την ασφάλεια: Καθώς οι έξυπνες πόλεις συλλέγουν τεράστιες ποσότητες δεδομένων, η προστασία του απορρήτου των ατόμων και η διασφάλιση της ασφάλειας αυτών των δεδομένων είναι πρωταρχικής σημασίας. Η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες ή οι παραβιάσεις της ασφάλειας του IoT θα μπορούσαν να έχουν σοβαρές συνέπειες (Powell, 2021).
- Ψηφιακό χάσμα ανάμεσα στους κατοίκους: Δεν έχουν όλοι οι κάτοικοι ίση πρόσβαση στις υπηρεσίες IoT, κάτι που οδηγεί σε ψηφιακό χάσμα. Η γεφύρωση αυτού του χάσματος είναι ζωτικής σημασίας για να διασφαλιστεί ότι όλοι οι πολίτες μπορούν να επωφεληθούν από τις εξελίξεις μιας έξυπνης πόλης.
- Επεκτασιμότητα και Διαλειτουργικότητα: Η ενσωμάτωση διαφόρων συσκευών και συστημάτων IoT από διαφορετικούς προμηθευτές μπορεί να είναι δύσκολη. Οι πόλεις πρέπει να επενδύσουν σε ανοιχτά πρότυπα και δια λειτουργικές τεχνολογίες για να εξασφαλίσουν ένα απρόσκοπτο και επεκτάσιμο οικοσύστημα έξυπνων πόλεων (Albino, et al, 2015).
- Κόστος: Η υλοποίηση και η διατήρηση μιας ολοκληρωμένης υποδομής IoT είναι ένα σημαντικό οικονομικό εγχείρημα. Οι προϋπολογισμοί των πόλεων πρέπει να κατανέμονται προσεκτικά για να επιτευχθεί μια ισορροπία μεταξύ του άμεσου κόστους και των μακροπρόθεσμων οφελών.

Η αντιμετώπιση των ανησυχιών για την προστασία της ιδιωτικής ζωής, της ασφάλειας και της ισότητας, αξιοποιώντας το πλήρες δυναμικό των αναδυόμενων τεχνολογιών, θα είναι το κλειδί για την υλοποίηση του οράματος για πραγματικά έξυπνες και συνδεδεμένες πόλεις (Sharma, et al, 2021).

1.5.4 Έξυπνο σπίτι και έξυπνες οικιακές συσκευές

Οι έξυπνες οικιακές συσκευές και ειδικά αυτές που στηρίζονται στο περιβάλλον IoT, έχουν γίνει γρήγορα ο ακρογωνιαίος λίθος της σύγχρονης ζωής, φέρνοντας

επανάσταση στον τρόπο με τον οποίο αλληλοεπιδρούν και διαχειρίζονται οι άνθρωποι τις κατοικίες τους (Carvalho, 2023).

Σύμφωνα με την έκθεση του Fortune Business Insights, το μέγεθος της παγκόσμιας αγοράς έξυπνων κατοικιών[9] που στηρίζεται σε συσκευές IoT προβλέπεται να φτάσει τα 338,28 δισεκατομμύρια δολάρια ΗΠΑ έως το 2030, με CAGR 20,1% κατά την περίοδο πρόβλεψης.

Οι κυριότερες καινοτομίες σε ένα έξυπνο σπίτι εντοπίζονται παρακάτω:

- Ευκολία και αυτοματισμός: Οι έξυπνες οικιακές συσκευές προσφέρουν απαράμιλλη ευκολία. Επιτρέπουν στους ιδιοκτήτες σπιτιού να ελέγχουν διάφορες λειτουργίες των σπιτιών τους από απόσταση, από τη ρύθμιση των θερμοστατών και του φωτισμού μέχρι το κλείδωμα των θυρών και ακόμη και την προετοιμασία γεύματος.
- Ενεργειακή απόδοση: Ένα από τα πιο σημαντικά πλεονεκτήματα των έξυπνων οικιακών συσκευών είναι οι δυνατότητές τους για εξοικονόμηση ενέργειας. Οι έξυπνοι θερμοστάτες μπορούν να βελτιστοποιήσουν τη θέρμανση και την ψύξη, μειώνοντας την κατανάλωση ενέργειας και τους λογαριασμούς κοινής ωφελείας. Ομοίως, τα έξυπνα συστήματα φωτισμού μπορούν να προσαρμόσουν αυτόματα τη φωτεινότητα και να σβήσουν τα φώτα σε δωμάτια που δεν χρησιμοποιούνται.
- Βελτιωμένη ασφάλεια: Οι έξυπνες συσκευές οικιακής ασφάλειας, όπως εσωτερικές κάμερες, κάμερες κυρίας εισόδου και αισθητήρες κίνησης, παρέχουν στους ιδιοκτήτες κατοικιών παρακολούθηση και ειδοποιήσεις σε πραγματικό χρόνο. Αυτό όχι μόνο ενισχύει την ασφάλεια, αλλά παρέχει και ψυχική ηρεμία, ειδικά αυτοί λείπουν από το σπίτι (Anuradha & Tripathy, 2018).
- Προσβασιμότητα: Η τεχνολογία έξυπνου σπιτιού μπορεί να κάνει τους χώρους διαβίωσης πιο προσιτούς για άτομα με αναπηρία. Οι συσκευές με φωνητικό

[9] https://www.globenewswire.com/news-release/2023/07/17/2705500/0/en/Smart-Home-Market-Size-to-Surpass-USD-338-28-billion-by-2030-exhibiting-a-CAGR-of-20-1.html Smart Home Market Size, (Ανάκτηση 14.8.2023).

έλεγχο και οι λειτουργίες αυτοματισμού επιτρέπουν σε άτομα με κινητικά προβλήματα να ελέγχουν ανεξάρτητα διάφορες λειτουργίες του σπιτιού τους.

Αντίστοιχα και σε αυτό το τομέα υπάρχουν προκλήσεις που πρέπει να αντιμετωπίζονται όπως:

- Προβλήματα απορρήτου και ασφάλειας: Όπως συμβαίνει με οποιαδήποτε τεχνολογία που είναι συνδεδεμένη στο διαδίκτυο, οι έξυπνες οικιακές συσκευές εγείρουν ανησυχίες για το απόρρητο και την ασφάλεια. Η μη εξουσιοδοτημένη πρόσβαση σε κάμερες ή η παραβίαση δεδομένων μπορεί να θέσει σε κίνδυνο τις προσωπικές πληροφορίες και την ασφάλεια (Carvalho, 2023).
- Κόστος: Ενώ οι έξυπνες οικιακές συσκευές μπορούν να οδηγήσουν σε μακροπρόθεσμη εξοικονόμηση, το αρχικό κόστος αγοράς και εγκατάστασης αυτών των συσκευών μπορεί να αποτελέσει εμπόδιο για ορισμένους ιδιοκτήτες σπιτιού (Anuradha & Tripathy, 2018).
- Συμβατότητα και κατακερματισμός: Η αγορά του έξυπνου σπιτιού είναι γεμάτη με διάφορες μάρκες και πλατφόρμες, με αποτέλεσμα να δημιουργούνται προβλήματα συμβατότητας μεταξύ συσκευών διαφορετικών κατασκευαστών.
- Εξάρτηση από τη συνδεσιμότητα: Οι έξυπνες οικιακές συσκευές βασίζονται στη συνδεσιμότητα στο Διαδίκτυο. Διακοπές δικτύου ή δυσλειτουργίες της συσκευής μπορεί να διαταράξουν τη λειτουργικότητά τους.

1.5.4 Συσκευές IoT στην υγεία

Όπως και με την βιομηχανία, η υγεία και ο ιατρικός κλάδος ήταν από τους πρωτοπόρους στην χρησιμοποίηση ρομποτικών συσκευών και ιατρικών μηχανημάτων διατήρησης ζωής που ελεγχόταν από υπολογιστικά συστήματα. Η έλευση του διαδικτύου και του διαδικτύου των πραγμάτων, άνοιξε νέους ορίζοντες στο τομέα της υγείας. Με την πάροδο του χρόνου, πιο εξειδικευμένες μορφές του διαδικτύου των πραγμάτων αναπτύσσονται σε κάθε κλάδο, δίνοντας βαρύτητα στις ιδιαιτερότητες, στο επίπεδο ασφάλειας και στην πρακτική εφαρμογή των καινοτόμων ψηφιακών τεχνολογιών (Beranger & Rizoulieres, 2021).

Το παγκόσμιο διαδίκτυο των πραγμάτων (IoT) στην αγορά υγειονομικής περίθαλψης[10] προβλέπεται να αυξηθεί από 89,07 δισεκατομμύρια δολάρια το 2021 σε 446,52 δισεκατομμύρια δολάρια το 2028 με CAGR 25,9%. Η παγκόσμια αγορά παρουσίασε σημαντική ανάπτυξη 24,1% το 2020 σε σύγκριση με τη μέση ετήσια αύξηση κατά την περίοδο 2017-2019. Η άνοδος του CAGR αποδίδεται στη ζήτηση και την ανάπτυξη αυτής της αγοράς, επιστρέφοντας στα προ της πανδημίας επίπεδα. Ο παγκόσμιος αντίκτυπος του COVID-19 ήταν άνευ προηγουμένου και συγκλονιστικός, με το Διαδίκτυο των πραγμάτων στον τομέα της υγείας να έχει θετικό αντίκτυπο στη ζήτηση σε όλες τις περιοχές εν μέσω της πανδημίας.

Μια κατηγορία του IoT είναι το Internet of Medical Things (IoMT) – Διαδίκτυο των ιατρικών πραγμάτων, γνωστό και ως Healthcare IoT, όπου δίνεται ιδιαίτερη προσοχή στη λειτουργία και σύνδεση των συστημάτων και αισθητήρων λόγω της λειτουργίας του στον ευαίσθητο τομέα της υγείας των ανθρώπων, ενώ τα στοιχεία και τα δεδομένα μπορούν να τύχουν περαιτέρω επεξεργασία και ανάλυση προκειμένου να εφαρμοστούν διαγνωστικές, θεραπευτικές και χειρουργικές διαδικασίες (Misra, et al, 2021)

Το Internet of Medical Things (IoMT) δίνει τη δυνατότητα στο ιατρικό προσωπικό να επιβλέπουν εξ αποστάσεως τους ασθενείς τους χρησιμοποιώντας ένα δίκτυο φορητών ψηφιακών συσκευών ή μικροσκοπικών εμφυτευμένων συσκευών (Kraus, et al, 2021). Αυτές οι συσκευές είναι εξοπλισμένες με λογισμικό και αισθητήρες που τους επιτρέπουν να μεταδίδουν και να λαμβάνουν πληροφορίες μέσω του Διαδικτύου δίνοντας δυνατότητα παρακολούθησης μετρήσεων υγείας, χορήγησης φαρμάκων παρακολούθηση μετεγχειρητικής κατάστασης ασθενούς και να προσφέρουν κατευθυντήριες γραμμές ή στρατηγικές θεραπείας με βάση τα τελευταία δεδομένα του ασθενή (Pani, et al, 2022)

Μία από τις κυριότερες προκλήσεις που αντιμετώπισε ο ψηφιακός τομέας υγείας ήταν η διαχείριση δεδομένων υγειονομικής περίθαλψης. Στο παρελθόν, τα παραδοσιακά συστήματα δημόσιας υγειονομικής περίθαλψης σχεδιάζονταν κυρίως με αυστηρά

[10] https://www.fortunebusinessinsights.com/internet-of-things-iot-in-healthcare-market-102188 Internet of things (IoT) in Healthcare Market Size, (Ανάκτηση 17.8.2023).

μέτρα ασφαλείας, επιτρέποντας την πρόσβαση αποκλειστικά στο εξουσιοδοτημένο ιατρικό και νοσηλευτικό προσωπικό, καθώς και στους ίδιους τους ασθενείς. Ενώ αυτά τα συστήματα δεν είχαν τη δυνατότητα ενσωμάτωσης προληπτικών και σχετικών με τον έλεγχο πληροφοριών, ήταν γενικά ασφαλή και προστατευμένα από πρόσβαση τρίτων ή μη εξουσιοδοτημένων ατόμων. Η εμφάνιση του Διαδικτύου και η ικανότητά του για εργασίες σε πραγματικό χρόνο και ανταλλαγή δεδομένων εισήγαγε ζητήματα ασφάλειας στο σύστημα της ψηφιακής υγείας. Το αποτέλεσμα ήταν να έχουν επενδυθεί σημαντικοί πόροι και να εξακολουθούν να επενδύονται για τη διαφύλαξη των ιατρικών δεδομένων και τη προστασία του ιατρικού απορρήτου (Mesko, 2018).

Το πρόβλημα στην ψηφιακή υγεία επεκτείνεται επίσης στο τεράστιο εύρος των ιατρικών συσκευών που χρησιμοποιούνται μέσω του διαδικτύου για τη διατήρηση της ζωής αλλά και για εγχειρήσεις. Μια παραβίαση ασφάλειας, μια διακοπή ρεύματος μπορεί να επιφέρει σοβαρότατους κινδύνους για την ίδια τη ζωή των ασθενών. Η ασφάλεια του του IoMT – Διαδικτύου των ιατρικών πραγμάτων θεωρείται από τις πιο κρίσιμες και πιο πολύπλοκες εφαρμογές (Hemanth, 2019).

1.5.6 Συσκευές IoT στους υπόλοιπους τομείς δραστηριοτήτων

Οι συσκευές IoT χρησιμοποιούνται πλέον σε κάθε κλάδο και σε όλες τις ανθρώπινες δραστηριότητες. Εκτεταμένες εφαρμογές εντοπίζονται στην:

- Ναυτιλία με Αυτόνομους και συνδεδεμένους στόλους με δυνατότητες απομακρυσμένης διαχείρισης.
- Διαχείριση ασφάλειας σε κάθε επίπεδο σε όλους τους κλάδους
- Διαχείριση εφοδιαστικής αλυσίδας
- Απομακρυσμένη παρακολούθηση και συντήρηση
- Περιβαλλοντική παρακολούθηση και έλεγχος ποιότητας του αέρα
- Έξυπνα δίκτυα και διαχείριση ενέργειας

- Αγροτικός τομέας με παρακολούθηση και ειδοποιήσεις λειτουργιών αγροκτημάτων, στην κτηνοτροφία και στη γεωργία
- Απομακρυσμένη παρακολούθηση τοποθεσίας
- Αμυντικός και στρατιωτικός τομέας

ΚΕΦΑΛΑΙΟ 2. Λειτουργία και επικοινωνίες του IoT

2.1 Εισαγωγή

Μετάδοση δεδομένων: Οι συσκευές IoT χρησιμοποιούν διάφορα πρωτόκολλα επικοινωνίας, όπως Wi-Fi, Bluetooth, ZigBee[11], LoRaWAN[12], δίκτυα κινητής τηλεφωνίας (3G, 4G, 5G) και δορυφόρους, για τη μετάδοση δεδομένων σε κεντρικούς διακομιστές ή άλλες συσκευές. Η επιλογή της μεθόδου επικοινωνίας εξαρτάται από παράγοντες όπως το εύρος, ο ρυθμός δεδομένων, η κατανάλωση ενέργειας και η διαθεσιμότητα δικτύου.

Μια κρίσιμη απαίτηση του IoT είναι ότι οι συσκευές πρέπει να είναι διασυνδεδεμένες, γεγονός που το καθιστά ικανό να εκτελεί συγκεκριμένες εργασίες, όπως ανίχνευση, επικοινωνία, επεξεργασία πληροφοριών κ.λπ. Το IoT είναι σε θέση να αποκτά, να μεταδίδει και να επεξεργάζεται τις πληροφορίες από τελικούς κόμβους (όπως συσκευές RFID, αισθητήρες, πύλες, έξυπνες συσκευές κ.λπ.) μέσω δικτύου για την εκτέλεση εξαιρετικά πολύπλοκων εργασιών (Li & Xu, 2017).

2.2 Επικοινωνία συσκευών IoT μέσω ετικετών RFID

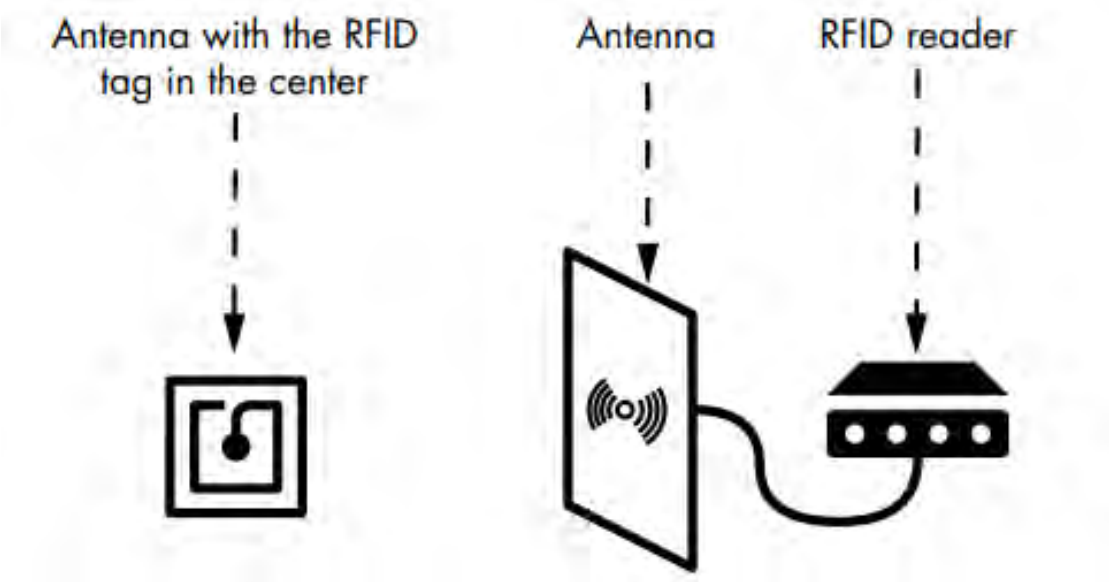
Όλα τα φυσικά στοιχεία στο Διαδίκτυο πρέπει να περιλαμβάνουν τεχνολογίες αυτόματης αναγνώρισης για τη μοναδική τους αναγνώριση. Μία από τις κοινώς χρησιμοποιούμενες τεχνολογίες για το σκοπό αυτό είναι η Αναγνώριση Ραδιοσυχνοτήτων (RFID). Η τεχνολογία RFID ενσωματώνει βασικά στοιχεία επικοινωνίας, αποθήκευσης και υπολογισμού σε ετικέτες που είναι προσαρτημένες σε

[11] Το ZigBee είναι μια ασύρματη τεχνολογία βασισμένη σε πρότυπα που αναπτύχθηκε για να επιτρέπει χαμηλού κόστους, χαμηλής κατανάλωσης ασύρματα δίκτυα μηχανής-προς-μηχανή (M2M) και internet of things (IoT). (Ανάκτηση 20.8.2023 από https://www.techtarget.com/iotagenda/definition/ZigBee)

[12] LoRaWAN είναι ένα «πρωτόκολλο δικτύωσης χαμηλής ισχύος, ευρείας περιοχής (LPWA) που έχει σχεδιαστεί για να συνδέει ασύρματα «πράγματα» που λειτουργούν με μπαταρία στο Διαδίκτυο σε περιφερειακά, εθνικά ή παγκόσμια δίκτυα καλύπτοντας βασικές απαιτήσεις του IoT, όπως δι- υπηρεσίες κατευθυντικής επικοινωνίας, ασφάλειας από άκρο σε άκρο, κινητικότητας και εντοπισμού. (Ανάκτηση 20.8.2023 από https://docs.aws.amazon.com/iot/latest/developerguide/connect-iot-lorawan-what-is-lorawan.html)

αντικείμενα, επιτρέποντας την ασύρματη επικοινωνία με τους αναγνώστες από απόσταση (Bolic, et al, 2010). Ως αποτέλεσμα, η RFID παρέχει ένα οικονομικά αποδοτικό και απλό μέσο σύνδεσης φυσικών αντικειμένων με το Διαδίκτυο των Πραγμάτων (IoT). Εφόσον ένα αντικείμενο φέρει μια ετικέτα RFID, μπορεί εύκολα να αναγνωριστεί και να παρακολουθηθεί από συσκευές ανάγνωσης RFID. Η τεχνολογία RFID βρίσκει εκτεταμένη χρήση σε διάφορες εφαρμογές, όπως η διαχείριση αποθεμάτων, η παρακολούθηση προϊόντων στην αλυσίδα εφοδιασμού, η παρακολούθηση των μεταφορών, η διαχείριση των logistics, μεταξύ άλλων. (Chen & Chen, 2016).

Το RFID σχεδιάστηκε για να αντικαταστήσει την τεχνολογία barcode. Λειτουργεί μεταδίδοντας κωδικοποιημένα δεδομένα μέσω ραδιοκυμάτων, χρησιμοποιώντας αυτά τα δεδομένα για να αναγνωρίσει μια οντότητα με ετικέτα. Αυτή η οντότητα μπορεί να είναι άνθρωπος, όπως ένας υπάλληλος που θέλει να αποκτήσει πρόσβαση σε ένα εταιρικό κτίριο, αυτοκίνητα που διέρχονται από διόδια ή ακόμη διάφορα αγαθά σε μια αποθήκη. Τα συστήματα RFID διατίθενται σε διάφορα σχήματα και μεγέθη ανάλογα τη χρήση τους, αλλά συνήθως η βασική αρχιτεκτονική τους αναγνωρίζεται στα κύρια στοιχεία που φαίνονται στο Σχήμα 1 (Chantzis, et al, 2021).



Σχήμα 1. Κοινά εξαρτήματα συστήματος RFID

2.3 Τύποι ετικετών RFID

Η μνήμη της ετικέτας RFID περιέχει πληροφορίες που προσδιορίζουν μια οντότητα. Ο αναγνώστης μπορεί να διαβάσει τις πληροφορίες της ετικέτας χρησιμοποιώντας μια κεραία σάρωσης, η οποία είναι συνήθως εξωτερικά συνδεδεμένη και δημιουργεί το σταθερό ηλεκτρομαγνητικό πεδίο που απαιτείται για αυτήν την ασύρματη σύνδεση. Όταν η κεραία της ετικέτας βρίσκεται εντός εμβέλειας από αυτήν της συσκευής ανάγνωσης, το ηλεκτρομαγνητικό πεδίο της συσκευής ανάγνωσης στέλνει ένα ηλεκτρικό ρεύμα για να ενεργοποιήσει την ετικέτα RFID. Η ετικέτα μπορεί στη συνέχεια να λάβει εντολές από τη συσκευή ανάγνωσης RFID και να στείλει απαντήσεις που περιέχουν τα δεδομένα αναγνώρισης (Chantzis, et al, 2021).

Κάθε μία από αυτές τις τεχνολογίες RFID ακολουθεί ένα συγκεκριμένο πρωτόκολλο. Η καλύτερη τεχνολογία για χρήση σε ένα σύστημα εξαρτάται από παράγοντες όπως το εύρος του σήματος, ο ρυθμός μεταφοράς δεδομένων, η ακρίβεια και το κόστος υλοποίησης (Song, 2022).

Υπάρχουν δύο κύριοι τύποι ετικετών RFID, αυτές που λειτουργούν με μπαταρία και οι παθητικές.

Οι ετικέτες RFID που λειτουργούν με μπαταρίες περιέχουν μια ενσωματωμένη μπαταρία η οποία τις τροφοδοτεί με ρεύμα και για το λόγο αυτό ονομάζονται ενεργές ετικέτες RFID. Η μπαταρία σε μια ενεργή ετικέτα RFID θα πρέπει να παρέχει αρκετή ισχύ για να διαρκέσει για 3-5 χρόνια. Όταν η μπαταρία εξαντληθεί, ολόκληρη η μονάδα θα πρέπει να αντικατασταθεί, καθώς οι μπαταρίες δεν μπορούν να αντικατασταθούν (Song, 2022).

Εικόνα 1. Ενεργές ετικέτες RFID

Οι παθητικές ετικέτες RFID δεν τροφοδοτούνται από μπαταρία και λειτουργούν χρησιμοποιώντας ηλεκτρομαγνητική ενέργεια που μεταδίδεται από τη συσκευή ανάγνωσης RFID.

Εικόνα 2. Παθητικές ετικέτες RFID

Οι παθητικές ετικέτες RFID χρησιμοποιούν συχνότητες για τη μετάδοση πληροφοριών. Η συχνότητα που χρησιμοποιείται για τη μετάδοση πληροφοριών επηρεάζει το εύρος της ετικέτας. Σε ορισμένες συσκευές χρησιμοποιείται μεγαλύτερο εύρος συχνοτήτων όπως φαίνεται στο πίνακα 1 (Chantzis, et al, 2021).

Πίνακας 1. Συχνότητες ετικετών

Ζώνη συχνοτήτων	**Εύρος σήματος**
Very Low frequency (VLF)	(3 KHz–30 KHz)
Low frequency (LF)	(30 kHz–300 kHz)
Medium frequency (MF)	(300 kHz–3,000 kHz)
High frequency (HF)	(3,000 kHz–30 MHz)
Very high frequency (VHF)	(30 MHz–300 MHz)
Ultra-high frequency (UHF)	(300 MHz–3,000 MHz)
Super high frequency (SHF)	(3,000 MHz–30 GHz)
Extremely high frequency (EHF)	(30 GHz–300 GHz)
Uncategorized	(300 GHz–3,000 GHz)

2.4 Θεμελιώδεις αρχές Λειτουργίας των RFID

Ένα σύστημα RFID αποτελείται από έναν πομποδέκτη (Transponders) ή RFID ετικέτες (RFID tags) και από τον αναγνώστη (Reader). Μια ετικέτα RFID είναι ένα μικρό ολοκληρωμένο κύκλωμα, που περιλαμβάνει μνήμη, για να αποθηκεύει δεδομένα, και κεραία, για να επικοινωνεί με τον αναγνώστη. ο οποίος εκπέμπει σήμα RF μέσω κεραίας. Η μνήμη της ετικέτας τροφοδοτείται ηλεκτρικά από τον αναγνώστη, αλλά υπάρχουν και ετικέτες RFID που μπορούν να αντλούν ενέργεια από κάποια πηγή, όπως μια μπαταρία. (Παρασκευάς, κ.α., 2015).

Αναγνώριση μέσω ραδιοκυμάτων: Το RFID (Radio Frequency Identification) λειτουργεί χρησιμοποιώντας ραδιοκύματα για τον εντοπισμό και την παρακολούθηση αντικειμένων. Αυτή η τεχνολογία βασίζεται σε ηλεκτρομαγνητικά πεδία για την επικοινωνία μεταξύ μιας συσκευής ανάγνωσης RFID και μιας ετικέτας RFID που είναι συνδεδεμένη σε ένα αντικείμενο (Chen & Chen, 2016).

Μοναδικές ετικέτες: Σε κάθε ετικέτα RFID εκχωρείται ένα μοναδικό αναγνωριστικό, επιτρέποντας τη διακριτή αναγνώριση μεμονωμένων στοιχείων. Αυτό το αναγνωριστικό είναι ζωτικής σημασίας για την παρακολούθηση και τη διαχείριση στοιχείων σε διάφορες εφαρμογές (Bolic, et al, 2010).

Ασύρματη επικοινωνία: Οι ετικέτες RFID και οι αναγνώστες επικοινωνούν ασύρματα, επιτρέποντας την ανταλλαγή δεδομένων χωρίς άμεση φυσική επαφή. Αυτή η πτυχή ασύρματου δικτύου απλοποιεί τη διαδικασία παρακολούθησης και την καθιστά κατάλληλη για ένα ευρύ φάσμα εφαρμογών (Li & Xu, 2017).

Μεταβλητότητα απόστασης: Τα συστήματα RFID μπορούν να λειτουργήσουν σε διάφορες αποστάσεις, από πολύ μικρής εμβέλειας, όπως μερικά εκατοστά, έως μεγάλης εμβέλειας, που εκτείνονται αρκετά μέτρα ή περισσότερο. Το συγκεκριμένο εύρος εξαρτάται από τον τύπο της τεχνολογίας RFID που χρησιμοποιείται, όπως RFID κοντινού ή μακρινού πεδίου.

Δεδομένα σε πραγματικό χρόνο: Το RFID παρέχει δυνατότητες λήψης και επεξεργασίας δεδομένων σε πραγματικό χρόνο. Όταν ένας αναγνώστης RFID στέλνει

ένα σήμα, οι κοντινές ετικέτες ανταποκρίνονται αμέσως με τις μοναδικές τους πληροφορίες. Αυτή η ταχεία ανταλλαγή δεδομένων είναι πολύτιμη για σκοπούς παρακολούθησης και παρακολούθησης (Chen & Chen, 2016).

Διαλειτουργικότητα: Η τεχνολογία RFID είναι τυποποιημένη, διασφαλίζοντας ότι οι ετικέτες RFID και οι αναγνώστες διαφορετικών κατασκευαστών μπορούν να συνεργάζονται απρόσκοπτα. Αυτή η διαλειτουργικότητα είναι απαραίτητη για την ευρεία υιοθέτηση και συμβατότητα εντός των αλυσίδων εφοδιασμού και άλλων εφαρμογών.

Παθητικές και ενεργές ετικέτες: Οι ετικέτες RFID διατίθενται σε δύο βασικούς τύπους: παθητικές και ενεργές. Οι παθητικές ετικέτες δεν έχουν δική τους πηγή ενέργειας και βασίζονται στην ενέργεια που μεταδίδεται από τον αναγνώστη RFID για να λειτουργήσουν. Οι ενεργές ετικέτες, από την άλλη πλευρά, έχουν την πηγή ενέργειας τους (συνήθως μια μπαταρία) και μπορούν να μεταδώσουν σήματα ανεξάρτητα σε μεγαλύτερες αποστάσεις (Li & Xu, 2017).

Διαφορετικές εφαρμογές: Η τεχνολογία RFID είναι ευέλικτη και εφαρμόζεται σε διάφορους κλάδους, συμπεριλαμβανομένης της διαχείρισης αποθεμάτων, της βελτιστοποίησης της αλυσίδας εφοδιασμού, του ελέγχου πρόσβασης, της παρακολούθησης περιουσιακών στοιχείων, της υγειονομικής περίθαλψης, του λιανικού εμπορίου και άλλων. Η προσαρμοστικότητά του το καθιστά πολύτιμο εργαλείο σε ένα ευρύ φάσμα σεναρίων (Bolic, et al, 2010).

Ασφάλεια δεδομένων: Για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και τη διασφάλιση του απορρήτου των δεδομένων, τα συστήματα RFID συχνά ενσωματώνουν μηχανισμούς κρυπτογράφησης και ελέγχου ταυτότητας. Αυτά τα χαρακτηριστικά ασφαλείας βοηθούν στην προστασία των ευαίσθητων πληροφοριών που περιέχονται στις ετικέτες RFID. Από την άλλη πλευρά αυτή είναι και η αρνητική πλευρά της χρήσης τους, καθώς δεν ενσωματώνουν όλες οι ετικέτες ικανοποιητικά επίπεδα ασφάλειας με αποτέλεσμα να δημιουργούνται προβλήματα.

Επεκτασιμότητα: Τα συστήματα RFID μπορούν να κλιμακωθούν προς τα πάνω ή προς τα κάτω για να ικανοποιήσουν διαφορετικές ανάγκες. Είτε παρακολουθείτε μερικά στοιχεία σε μια μικρή επιχείρηση είτε διαχειρίζεστε εκατομμύρια προϊόντα σε μια παγκόσμια αλυσίδα εφοδιασμού, η τεχνολογία RFID μπορεί να προσαρμοστεί ώστε να ταιριάζει στο εύρος της λειτουργίας (Chen & Chen, 2016).

2.4 Η χρήση των RFID

Η ενσωμάτωση της τεχνολογίας RFID σε συσκευές IoT έχει δημιουργήσει ένα μεγάλο πεδίο εφαρμογών σε διάφορους κλάδους:

- Εφοδιαστική αλυσίδα: Οι συσκευές IoT με δυνατότητα RFID διαδραματίζουν κεντρικό ρόλο στη διαχείριση της εφοδιαστικής αλυσίδας, παρέχοντας ορατότητα σε πραγματικό χρόνο στην κίνηση των αγαθών. Αυτό διασφαλίζει την αποτελεσματική διαχείριση του αποθέματος, μειώνει την κλοπή και ελαχιστοποιεί τα σφάλματα. Οι παλέτες και τα εμπορευματοκιβώτια με δυνατότητα RFID, μαζί με τη συνδεσιμότητα IoT, επιτρέπουν στις εταιρείες εφοδιαστικής αλυσίδας να παρακολουθούν τη θέση, τη θερμοκρασία, την υγρασία και άλλες περιβαλλοντικές συνθήκες των αγαθών κατά τη μεταφορά. Αυτά τα δεδομένα διασφαλίζουν την ακεραιότητα του ευαίσθητου ή ευπαθούς φορτίου και επιτρέπουν την προληπτική επίλυση προβλημάτων (Παρασκευάς, κ.α., 2015).
- Υγειονομική περίθαλψη: Στην υγειονομική περίθαλψη, οι ετικέτες RFID χρησιμοποιούνται για την παρακολούθηση της θέσης του ιατρικού εξοπλισμού, την παρακολούθηση των αρχείων ασθενών και τη διασφάλιση της σωστής χορήγησης φαρμάκων, βελτιώνοντας την ασφάλεια των ασθενών και τη λειτουργική αποτελεσματικότητα (Chen & Chen, 2016).
- Λιανικό εμπόριο: Οι συσκευές IoT με δυνατότητα RFID βοηθούν τους λιανοπωλητές να διαχειρίζονται το απόθεμα, να μειώνουν τις καταστάσεις εκτός αποθέματος, να βελτιώνουν την εμπειρία αγορών με συστήματα self-checkout και να καταπολεμούν την κλοπή μέσω αντικλεπτικών ετικετών.

- Γεωργία: Η γεωργία επωφελείται από τις εφαρμογές IoT RFID παρακολουθώντας τα ζώα, παρακολουθώντας τις συνθήκες των καλλιεργειών τη διαχείριση πόρων όπως το νερό και τα λιπάσματα πιο αποτελεσματικά, διασφαλίζοντας την ακεραιότητα της αλυσίδας εφοδιασμού, οδηγώντας σε αυξημένη παραγωγικότητα και ασφάλεια τροφίμων.
- Διαχείριση απορριμμάτων: Οι ετικέτες RFID στους κάδους απορριμμάτων μπορούν να συνδεθούν με συστήματα IoT για βελτιστοποιημένη συλλογή απορριμμάτων. Οι αισθητήρες μπορούν να ανιχνεύσουν πότε οι κάδοι είναι γεμάτοι, επιτρέποντας στις εταιρείες διαχείρισης απορριμμάτων να προγραμματίζουν αποτελεσματικά τις παραλαβές και να μειώνουν την κατανάλωση καυσίμου (Li & Xu, 2017).
- Διαχείριση ενέργειας: Τα συστήματα RFID που συνδέονται με το IoT μπορούν να βοηθήσουν στην παρακολούθηση και τον έλεγχο της κατανάλωσης ενέργειας στα κτίρια. Για παράδειγμα, οι κάρτες πρόσβασης με δυνατότητα RFID μπορούν να ενεργοποιήσουν συστήματα φωτισμού και κλιματισμού μόνο όταν απαιτείται, μειώνοντας τη σπατάλη ενέργειας (Chen & Chen, 2016).
- Έλεγχος πρόσβασης: Ο συνδυασμός καρτών RFID ή σημάτων με συστήματα ελέγχου πρόσβασης με δυνατότητα IoT ενισχύει την ασφάλεια. Αυτά τα συστήματα μπορούν να παραχωρήσουν ή να αρνηθούν πρόσβαση με βάση τον έλεγχο ταυτότητας σε πραγματικό χρόνο, να παρακολουθούν τους χρόνους εισόδου και εξόδου και να παρέχουν λεπτομερή αρχεία καταγραφής πρόσβασης για σκοπούς ελέγχου.

Πλεονεκτήματα της χρήσης ετικετών RFID

Αποτελεσματική και γρήγορη συλλογή δεδομένων: Η τεχνολογία RFID επιτρέπει τη γρήγορη και αυτοματοποιημένη συλλογή δεδομένων. Πολλαπλές ετικέτες RFID μπορούν να διαβαστούν ταυτόχρονα, μειώνοντας τον χρόνο και την προσπάθεια που απαιτείται για την εισαγωγή δεδομένων.
Ακρίβεια στη συλλογή δεδομένων: Τα συστήματα RFID παρέχουν υψηλό επίπεδο ακρίβειας στη συλλογή δεδομένων, ελαχιστοποιώντας τα σφάλματα που σχετίζονται

με τη χειροκίνητη εισαγωγή δεδομένων. Αυτό είναι ζωτικής σημασίας για εφαρμογές όπως η διαχείριση αποθεμάτων και η παρακολούθηση της αλυσίδας εφοδιασμού.

Αυτοματισμός και παρακολούθηση σε πραγματικό χρόνο: Οι ετικέτες RFID επιτρέπουν την παρακολούθηση σε πραγματικό χρόνο των αντικειμένων καθώς κινούνται σε διαφορετικά στάδια μιας διαδικασίας ή μιας αλυσίδας εφοδιασμού.

Ενώ το αρχικό κόστος της εφαρμογής συστημάτων RFID μπορεί να είναι υψηλότερο σε σύγκριση με τις παραδοσιακές μεθόδους παρακολούθησης, τα μακροπρόθεσμα οφέλη συχνά υπερτερούν του κόστους. Η RFID μπορεί να οδηγήσει σε εξοικονόμηση κόστους μέσω βελτιωμένης απόδοσης, μειωμένου κόστους εργασίας και καλύτερης διαχείρισης αποθεμάτων.

Οι ετικέτες RFID μπορούν να χρησιμοποιηθούν για σκοπούς ελέγχου πρόσβασης και ασφάλειας. Παρέχουν έναν ασφαλή τρόπο παρακολούθησης και διαχείρισης της πρόσβασης σε απαγορευμένες περιοχές ή ευαίσθητες πληροφορίες.

Η τεχνολογία RFID είναι ευέλικτη και μπορεί να προσαρμοστεί ώστε να ταιριάζει σε συγκεκριμένες επιχειρηματικές ανάγκες. Μπορεί να ενσωματωθεί με άλλα συστήματα και τεχνολογίες για μια πιο ολοκληρωμένη λύση.

Οι ετικέτες RFID μπορούν να χρησιμοποιηθούν για τον έλεγχο ταυτότητας προϊόντων και την καταπολέμηση της παραχάραξης. Αυτό είναι ιδιαίτερα σημαντικό σε βιομηχανίες όπου η αυθεντικότητα των προϊόντων είναι κρίσιμης σημασίας, όπως τα φαρμακευτικά προϊόντα και τα είδη πολυτελείας.

Η τεχνολογία RFID διευκολύνει τη συμμόρφωση με τους κανονισμούς και τα πρότυπα του κλάδου. Επιτρέπει επίσης την ιχνηλασιμότητα, επιτρέποντας στις επιχειρήσεις να παρακολουθούν την προέλευση και την κίνηση των προϊόντων σε όλη την αλυσίδα εφοδιασμού.

Εικόνα 3. Χρήσεις των ετικετών RFID.

Από τεχνολογική άποψη, οι ετικέτες RFID σε πολλές περιπτώσεις είναι προβληματικές καθώς δεν υπάρχουν πραγματικά παγκόσμια ή βιομηχανικά πρότυπα. Δεδομένου ότι λειτουργούν σε ραδιοσυχνότητες, οι ετικέτες RFID και τα συστήματά τους μπορούν επίσης εύκολα να μπλοκάρουν ή να διαταραχθούν, μειώνοντας τη χρηστικότητά τους. Για το λόγο αυτό τα επίπεδα ασφάλειας ανάλογα και με το σκοπό χρήσης τους πρέπει να είναι προσεκτικά σχεδιασμένα και να εφαρμόζονται με σχολαστικότητα λόγω της ευρείας χρήσης τους σαν μονάδες μέσα σε πολυπλοκότερα δίκτυα (Song, 2022).

ΚΕΦΑΛΑΙΟ 3. Βασικές αρχές ασφάλειας Υλικού IoT

3.1 Εισαγωγή

Το Διαδίκτυο των πραγμάτων έχει εισχωρεί πλέον στον πραγματικό κόσμο με τρόπους που ενισχύουν την ασφαλή ζωή των ανθρώπων αλλά και μπορούν να θέσουν σε κίνδυνο την προσωπική ασφάλεια και την ασφάλεια του κοινωνικού συνόλου. Η επέκταση του Διαδικτύου σε καθημερινά αντικείμενα είναι ένα νέο περιβάλλον απειλών αλλά και κίνδυνος για την εθνική ασφάλεια των κρατών Οι εξαρτήσεις από τη σταθερότητα και την ασφάλεια του κυβερνοχώρου, που είναι ήδη απαραίτητες για την ψηφιακή οικονομία και τη δημόσια διακυβέρνηση, επεκτείνονται βαθύτερα στην ανθρώπινη ασφάλεια και στη βασική λειτουργία των υλικών υποδομών των συστημάτων νερού, ενέργειας και μεταφορών (DeNardis, 2020).

Το διακύβευμα της κυβερνοασφάλειας στο σύνολο της, αλλά και της ασφάλειας των ίδιων των συσκευών IoT, στο επίπεδο του πολίτη, επίσης αυξάνεται καθώς οι διακοπές ή η δυσλειτουργία στο Διαδίκτυο δεν αφορά πλέον την απώλεια πρόσβασης στην επικοινωνία και το περιεχόμενο των χρηστών (Parsons, et al, 2023), αλλά για την απώλεια κρίσιμων καθημερινών λειτουργιών και διαδικασιών στον πραγματικό κόσμο, από την ικανότητα οδήγησης αυτοκινήτου έως την πρόσβαση στην ιατρική περίθαλψη (Stergiou, et al, 2023)

3.2 Σημασία της ασφάλειας υλικού σε συσκευές IoT

Η εκθετικά αυξανόμενη εγκατάσταση και χρήση συσκευών IoT έχει αυξήσει και την σημασία ασφάλειας όλου του ψηφιακού περιβάλλοντος που έχει δημιουργηθεί στην σημερινή εποχή. Μέχρι την έλευση του διαδικτύου, τα πληροφοριακά συστήματα που έλεγχαν κρίσιμες υποδομές μπορούσαν πιο εύκολα να ελεγχθούν, ή ακόμη και να απομονωθούν και οι κυβερνοεπιθέσεις απαιτούσαν πολύ ισχυρά συστήματα υπολογισμών και εξελιγμένα λογισμικά για να «σπάσουν» κωδικούς ή να αποκτήσουν πρόσβαση σε υπολογιστικά συστήματα (Mohanta, et al, 2020)

Η διάθεση του διαδικτύου σε πρώτη φάση και η ολοένα και μεγαλύτερη ενσωμάτωση διαφόρων ψηφιακών συσκευών και αισθητήρων, τα οποία χρησιμοποιούν αφενός το διαδίκτυο για να επικοινωνήσουν και αφετέρου τις ασύρματες επικοινωνίες, καταστούν πιο τρωτά τα διάφορα σημεία αυτού του γιγάντιου δικτύου (Stergiou, et al, 2023). Τα επίπεδα ασφάλειας για παράδειγμα ενός κεντρικού υπολογιστικού συστήματος που ελέγχει ένα βιομηχανικό συγκρότημα, η μια κρίσιμη υποδομή όπως ένα εργοστάσιο ενέργειας, ενός δικτύου πόσιμου ύδατος κ.λ.π., ενδέχεται να είναι κορυφαία και εξαιρετικά δύσκολο να παρακαμφθούν (Sidhu, et al, 2019), αλλά χιλιάδες άλλες συσκευές από απλούς διακόπτες και αισθητήρες είναι συνδεμένοι στο δίκτυο και είναι πολύ πιο εύκολο να υποπέσουν σε απειλές και κινδύνους επιθέσεων, αποτελώντας το αδύνατο σημείο όπου θα αποκτήσουν πρόσβαση κακόβουλοι χρήστες, ή μορφές λογισμικού ιών, μολύνοντας το σύστημα ή υποκλέπτοντας δεδομένα, ή στη χειρότερη περίπτωση καταστρέφοντας την λειτουργία της εγκατάστασης (Parsons, et al, 2023)

Ένα επιπλέον πρόβλημα είναι η σύνθεση και το μέγεθος των συσκευών IoT, συμπεριλαμβανομένων των συστημάτων ασφαλείας, που δημιουργεί περιορισμούς που δεν συναντώνται σε τυπικά περιβάλλοντα πληροφορικής. Για παράδειγμα, οι περιορισμοί μεγέθους και ισχύος σε έναν βηματοδότη όπως είναι φυσικό δημιουργούν προκλήσεις για την εφαρμογή συμβατικών προσεγγίσεων ασφάλειας που χρησιμοποιούνται στα κεντρικά συστήματα πληροφορικής τα οποία απαιτούν μεγάλες ποσότητες αποθήκευσης ή υπολογιστικής ισχύος. Ένας αισθητήρας σε ένα αυτοκίνητο δεν μπορεί από τη φύση του να έχει το επίπεδο ασφάλειας ενός υπολογιστή, αλλά μπορεί να χρησιμοποιηθεί σαν το σημείο πρόσβασης από κακόβουλους χρήστες για να συνδεθούν στο κεντρικό σύστημα του αυτοκινήτου και να πάρουν τον έλεγχο του με καταστροφικές συνέπειες (Chantzis, et al, 2021).

Αντίστοιχα υπάρχουν χιλιάδες περιπτώσεις μικρών συσκευών IoT οι οποίες χρησιμοποιούνται σε διάφορα μέρη ενός δικτύου και δημιουργούν κινδύνους για την ασφάλεια και ενός δικτύου αλλά και ολόκληρου του περιβάλλοντος που λειτουργεί αυτό (DeNardis, 2020).

3.3 Μοντέλα απειλών

Η διαδικασία μοντελοποίησης απειλών εντοπίζει συστηματικά πιθανές επιθέσεις εναντίον μιας συσκευής και στη συνέχεια ιεραρχεί ορισμένα ζητήματα με βάση τη σοβαρότητά τους. Επειδή η μοντελοποίηση απειλών μπορεί να είναι χρονοβόρα και δύσκολη να εφαρμοστεί, μερικές φορές παραβλέπεται. Είναι όμως ζωτικής σημασίας για την κατανόηση των απειλών, τον αντίκτυπό τους και την εφαρμογή των κατάλληλων διαδικασιών για να αποτραπούν (Chantzis, et al, 2021).

Οι κύριοι στόχοι της ασφάλειας, που επισημαίνονται από διάφορα μοντέλα είναι η εμπιστευτικότητα, η ακεραιότητα, ο έλεγχος ταυτότητας, η εξουσιοδότηση, η μη άρνηση και η διαθεσιμότητα. Η εφαρμογή διαφορετικών κρυπτογραφικών μηχανισμών μπορεί να βοηθήσει στο να επιτευχθούν αυτά τα χαρακτηριστικά ασφαλείας. Ωστόσο, είναι πολύ δύσκολο να εφαρμοστούν αυτοί οι κρυπτογραφικοί αλγόριθμοι σε συσκευές IoT. Πολλές συσκευές IoT όπως αναφέρθηκε είναι εξαιρετικά μικρού μεγέθους ή εμπίπτουν στην κατηγορία των συσκευών χαμηλού και περιορισμένου κόστους. Ο φυσικός αυτός περιορισμός τους, επιτρέπει στις συσκευές να διαθέτουν μόνο πόρους χαμηλής κατανάλωσης (ρεύμα από μπαταρία), γεγονός που καθιστά δύσκολη την προσθήκη περισσότερων επιπέδων ασφάλειας (Sidhu, et al, 2019).

Η συστηματική διαδικασία μοντελοποίησης απειλών για μια συγκεκριμένη συσκευή και τις διάφορες εφαρμογές της περιλαμβάνει τον εντοπισμό ευαίσθητων στοιχείων, και των πιθανών απειλών για αυτά τα στοιχεία και τρωτών σημείων που ενισχύουν αυτές τις απειλές. Ο στόχος είναι να θεσπιστούν απαιτήσεις ασφάλειας που να εξουδετερώνουν αποτελεσματικά αυτές τις απειλές και κατά συνέπεια να προστατεύουν τα στοιχεία του IoT (Hu, 2016). Για βέλτιστα αποτελέσματα, μια συσκευή θα πρέπει να υποβληθεί στα στάδια του σχεδιασμού, της κατασκευής, της δοκιμής και της πιστοποίησης με βάση το μοντέλο απειλής που χρησιμοποιείται στην αρχιτεκτονική και τη σχεδίασή της. Αυτή η προσέγγιση όχι μόνο ελαχιστοποιεί το κόστος στα μεταγενέστερα στάδια ανάπτυξης, αλλά δημιουργεί επίσης ένα θεμέλιο ασφάλειας από τις αρχικές φάσεις της δημιουργίας της συσκευής. Αυτό διασφαλίζει ότι τα σωστά μέτρα ασφαλείας έχουν σχεδιαστεί, ελεγχθεί και δοκιμαστεί πριν από την ανάπτυξη του προϊόντος (Russell & Van Duren, 2016).

Υπάρχουν περισσότεροι διάφορα μοντέλα απειλών αλλά οι κύριες στρατηγικές που συνήθως εφαρμόζονται περιλαμβάνουν τη μοντελοποίηση απειλών των στοιχείων (υλικό μέρος – συσκευές, κόμβοι, συστήματα), τη μοντελοποίηση απειλών από επιτιθέμενους και η μοντελοποίηση απειλών στο λογισμικό που χρησιμοποιείται σε ολόκληρη την αλυσίδα λειτουργίας (Shostack, 2014).

Οι αρχιτεκτονικές δικτύου, υπολογιστών, εφαρμογών και διαχείρισης δεδομένων που είναι υπάρχουν καλύπτουν όλο το φάσμα της μοντελοποίησης αλλά όσον αφορά το δίκτυο IoT απαιτείται ένα διαφορετικό μοντέλο επικοινωνίας και επεξεργασίας. Σήμερα, δεν υπάρχει ένας τυπικός τρόπος κατανόησης ή περιγραφής αυτών των μοντέλων για το IoT. Το αποτέλεσμα είναι να μην υπάρχουν ξεκάθαρες γραμμές μεταξύ συσκευών και συστημάτων IoT και συσκευών και συστημάτων που δεν ανήκουν στο IoT. Το γεγονός είναι ότι δεν είναι κάθε δίκτυο, δίκτυο IoT. Ούτε χρειάζεται να είναι. Και δεν είναι κάθε εφαρμογή, εφαρμογή IoT. Γενικά, όταν τα δεδομένα παράγονται υπό τον έλεγχο μηχανών ή εξοπλισμού και αποστέλλονται μέσω ενός δικτύου, είναι πιθανώς ένα σύστημα IoT. Αλλά στο IoT, ακόμη και οι γενικεύσεις μπορεί να είναι ακατάλληλες. Μπορεί να υπάρχουν πολλές εξαιρέσεις (Cisco, 2014).

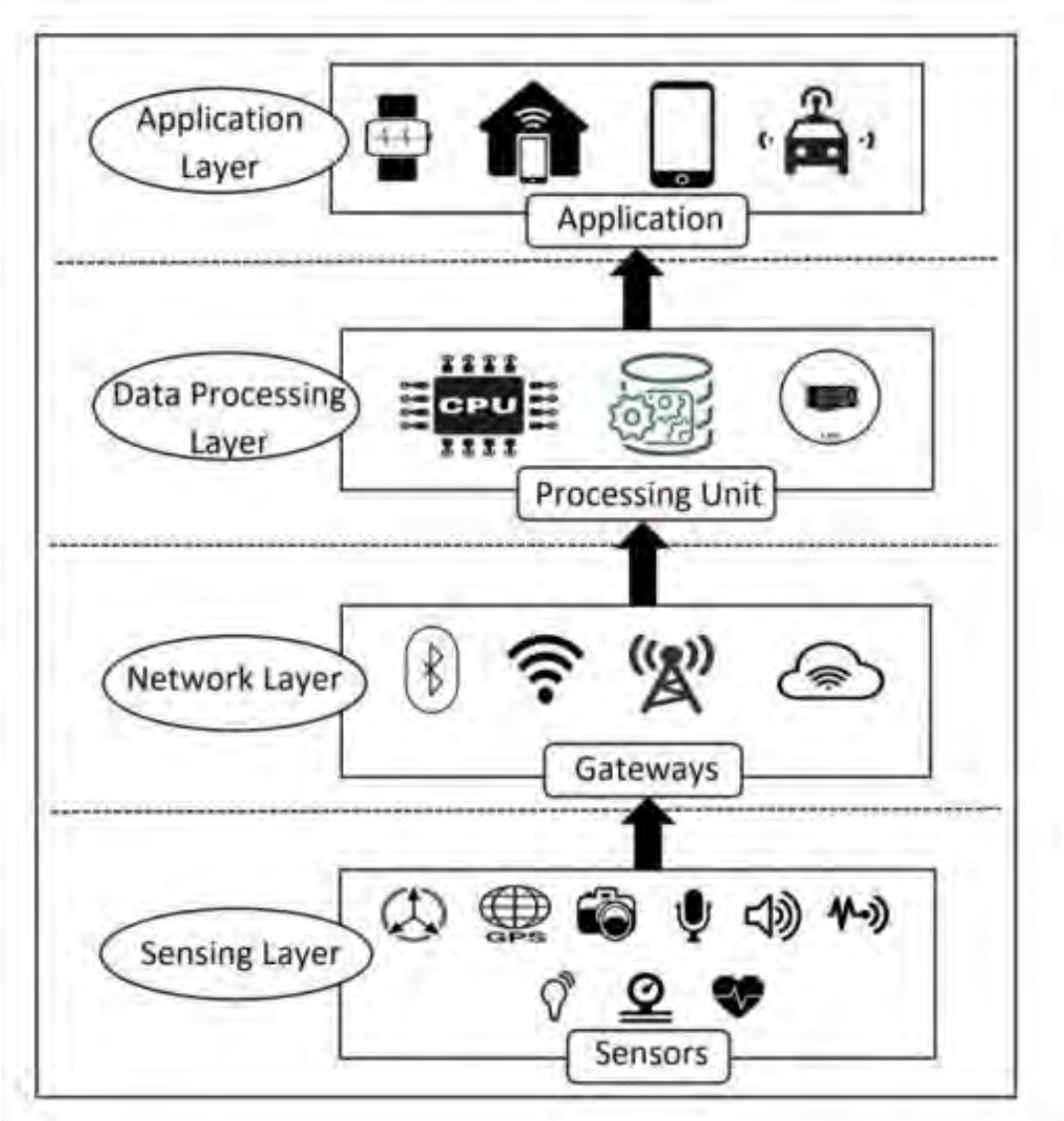
Οι περισσότεροι ερευνητές αναλύουν τα 4 βασικά επίπεδα της αρχιτεκτονικής του IoT όπου εστιάζονται οι διαδικασίες ασφάλειας και αντιμετώπισης των απειλών (Alaali, & Elmedany, 2022).

Το πρώτο επίπεδο αφορά το υλικό μέρος, τις συσκευές του IoT που τις περισσότερες φορές θεωρούνται οι πιο εύκολες στο να δεχτούν επιθέσεις ασφάλειας.

Το δεύτερο επίπεδο αφορά το περιβάλλον δικτύου που χρησιμοποιείται για την επικοινωνία και την αλληλοενημέρωση των συσκευών IoT με κεντρικά συστήματα, περιλαμβάνοντας Το διαδίκτυο, τα ασύρματα δίκτυα, το σύννεφο και όλες τις υποκατηγορίες τους.

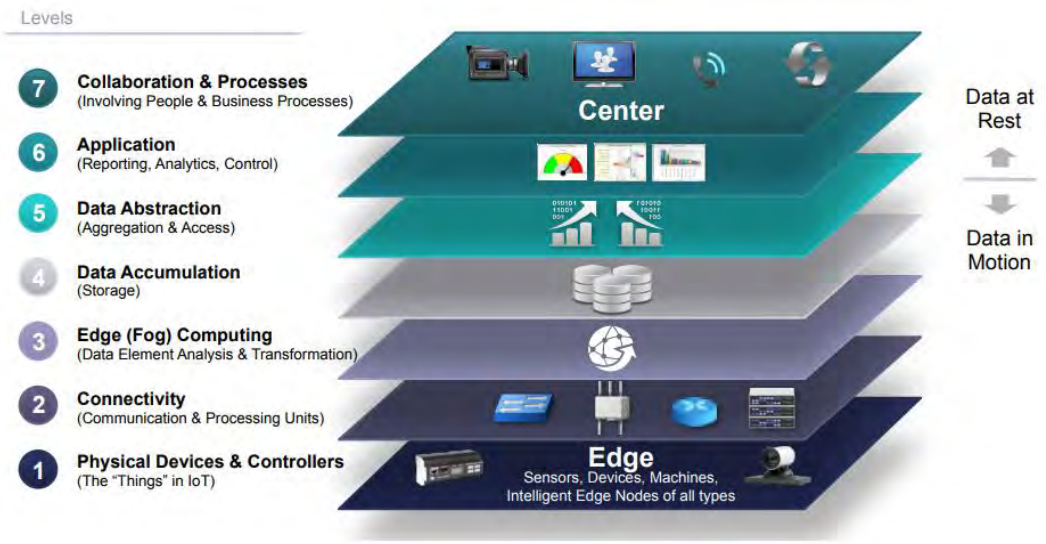
Το τρίτο επίπεδο περιλαμβάνει τις συσκευές επεξεργασίας των δεδομένων (υπολογιστικά κέντρα, βάσεις δεδομένων και αποθήκευσης).

Το τέταρτο επίπεδο περιλαμβάνει το τελικό επίπεδο εφαρμογής των συσκευών IoT όπως ένα αυτοκίνητο, ένα έξυπνο σπίτι, μια τελική συσκευή, ένα κινητό τηλέφωνο, μία βιομηχανική μηχανή κ.λ.π. (Alaali, & Elmedany, 2022).



Σχήμα 4. Τα 4 βασικά επίπεδα αρχιτεκτονικής του περιβάλλοντος IoT

Η CISCO έχει δημιουργήσει το δικό της μοντέλο αναφοράς για το IoT, το οποίο έχει προκύψει απευθείας από τη βιομηχανία και αφορά 7 επίπεδα. Η πρόθεση είναι να γίνει σαφής διάκριση μεταξύ κανονικών δικτύων και IoT όπου εφαρμόζονται διαδικασίες ελέγχου και ασφάλειας (Aufner, 2020).



Σχήμα 3. Μοντέλο αναφοράς 7 επιπέδων μοντελοποίησης Internet of Things

Το πρώτο επίπεδο περιγράφει τις κανονικές φυσικές συσκευές - Physical Devices & Controllers. Αυτοί μπορεί να είναι απλοί αισθητήρες αλλά και πιο σύνθετες συσκευές όπως κάμερες ή πιο πολύπλοκοι αισθητήρες (Cisco, 2014). Αυτά είναι τα «πράγματα» στο IoT και περιλαμβάνουν ένα ευρύ φάσμα συσκευών τελικού σημείου που στέλνουν και λαμβάνουν πληροφορίες. Σήμερα, ο κατάλογος των συσκευών είναι ήδη εκτενής. Θα γίνει σχεδόν απεριόριστος όσο περισσότερος εξοπλισμός προστίθεται στο IoT με την πάροδο του χρόνου (Aufner, 2020).

Το δεύτερο επίπεδο είναι η συνδεσιμότητα - Connectivity τόσο μεταξύ συσκευών όσο και πέρα από τα όρια του δικτύου. Οι επικοινωνίες και η συνδεσιμότητα συγκεντρώνονται σε αυτό το επίπεδο. Η πιο σημαντική λειτουργία του επιπέδου 2 είναι η αξιόπιστη και έγκαιρη μετάδοση πληροφοριών (Aufner, 2020).

Το τρίτο επίπεδο είναι το πρώτο υπολογιστικό βήμα - Edge (Fog) Computing. Οι λειτουργίες του επιπέδου 3 καθοδηγούνται από την ανάγκη μετατροπής των ροών δεδομένων δικτύου σε πληροφορίες που είναι κατάλληλες για αποθήκευση και επεξεργασία στο υψηλότερο επίπεδο 4 (συσσώρευση δεδομένων). Αυτό σημαίνει ότι οι δραστηριότητες επιπέδου 3 επικεντρώνονται στην ανάλυση και μετασχηματισμό δεδομένων μεγάλου όγκου (Cisco, 2014).

Το επίπεδο τέσσερα αφορά τη συσσώρευση δεδομένων – Data Accumulation. Σε αυτό το σημείο, τα δεδομένα από διάφορες συσκευές ή δίκτυα υποβάλλονται σε επεξεργασία και αποθηκεύονται (Aufner, 2020).

Το επίπεδο πέντε, όπου οι μεγάλοι όγκοι δεδομένων από τα προηγούμενα επίπεδα αφαιρούνται και φιλτράρονται – Data Abstraction για ευκολότερη ανάλυση.

Το επίπεδο έξι παρέχει εφαρμογές (λογισμικό) για τον έλεγχο ή την ανάλυση των δεδομένων που έχουν συγκεντρωθεί μέχρι στιγμής. Τα δεδομένα πλέον βρίσκονται αποθηκευμένα και χρησιμοποιούνται από διάφορα λογισμικά τα οποία μετατρέπουν τον όγκο αυτό των δεδομένων σε πρακτικές πληροφορίες όπως σχεσιακούς πίνακες βάσης δεδομένων που μπορούν να αξιοποιηθούν από τους ανθρώπους (Cisco, 2014).

Το έβδομο επίπεδο εισάγει τη συνεργασία μεταξύ των χρηστών και των διαδικασιών από τις συσκευές IoT. Αυτό το τελικό επίπεδο μπορεί να αποτελείται από διάφορες πηγές και προσθέτει πολύπλοκες αλληλεπιδράσεις (Cisco, 2014). Η κύρια διαφορά ενός ψηφιακού δικτύου και του IoT είναι ότι το IoT περιλαμβάνει ανθρώπους και διαδικασίες. Το σύστημα IoT και οι πληροφορίες που δημιουργεί, είναι μικρής αξίας, εκτός εάν αποφέρει αλληλεπίδραση, η οποία συχνά απαιτεί ανθρώπους και διαδικασίες (Aufner, 2020).

Η ασφάλεια για κάθε επίπεδο και η διακίνηση δεδομένων μεταξύ των επιπέδων είναι η σημαντικότερη διαδικασία για ένα δίκτυο IoT. Σε κάθε επίπεδο εφαρμόζεται:

- Στο επίπεδο 1 - ασφάλεια υλικού
- Στο επίπεδο 2 - Ασφαλής πρόσβαση στο δίκτυο (υλικό και πρωτόκολλα)
- Στο επίπεδο 3 - Ασφαλείς Επικοινωνίες (πρωτόκολλα και κρυπτογράφηση)
- Στο επίπεδο 4 - Ανθεκτικό σε παραβίαση (λογισμικό)
- Στο επίπεδο 5 - Ασφαλής αποθήκευση (υλικό και λογισμικό)
- Στο επίπεδο 6 - Έλεγχος ταυτότητας/Εξουσιοδότηση (λογισμικό)

- Στο επίπεδο 7 - Διαχείριση ταυτότητας (λογισμικό)

  Το μοντέλο αναφοράς (IoT) είναι ένα αποφασιστικό πρώτο βήμα προς την τυποποίηση της έννοιας και της ορολογίας που περιβάλλει το IoT. Από τις φυσικές συσκευές και τους ελεγκτές στο Επίπεδο 1 έως τη συνεργασία και τις διαδικασίες στο Επίπεδο 7, το μοντέλο Αναφοράς IoT καθορίζει τις απαιτούμενες λειτουργίες και τις ανησυχίες που πρέπει να αντιμετωπιστούν πριν ο κλάδος μπορέσει να συνειδητοποιήσει την αξία του IoT. Με στόχο την ενεργοποίηση του IoT, αυτό το μοντέλο αναφοράς παρέχει μια βάση για την κατανόηση των απαιτήσεών ασφάλειας και των δυνατοτήτων του (Cisco, 2014).

3.4 Αναγνώριση απειλών

Η δημιουργία ασφαλών συστημάτων IoT είναι εξαιρετικά δύσκολη λόγω της εγγενούς ετερογένειας των στοιχείων του IoT και των προβλημάτων ολοκλήρωσης τους σε δίκτυα. Οι διαδικασίες απαιτούν βαθιά κατανόηση των τεχνολογιών που χρησιμοποιούνται και της διαμόρφωσης ανάπτυξης, που περιλαμβάνει τις εγκατεστημένες συσκευές, το φάσμα των τεχνολογιών δικτύου που χρησιμοποιούνται για την επικοινωνία τους, τις διαμορφωμένες αλληλεπιδράσεις με τους χρήστες και τις επιλεγμένες τεχνολογίες (Patel, & Nishant, 2019; Chantzis, et al, 2021).

Η πολυπλοκότητα ενισχύεται περαιτέρω από τις απρόβλεπτες επιπτώσεις στην ασφάλεια που προκύπτουν από την ενσωμάτωση έξυπνων συσκευών σε συμβατικές υπηρεσίες Διαδικτύου, δεδομένου ότι η πλειονότητα των υφιστάμενων τεχνολογιών Διαδικτύου και πρωτοκόλλων επικοινωνίας δεν σχεδιάστηκαν αρχικά για να εξυπηρετούν το IoT.

Ο εντοπισμός συγκεκριμένων απειλών για μια δεδομένη ανάπτυξη του IoT και η διεξαγωγή μιας διαδικασίας αξιολόγησης κινδύνου για την αξιολόγηση των υφιστάμενων κινδύνων και τον εντοπισμό των αντίστοιχων αντίμετρων είναι περίπλοκες διαδικασίες. Επιπλέον, αυτές οι εργασίες είναι συχνά πολύ δαπανηρές και απαιτούν πόρους, σε σύγκριση με το κόστος και τον χρόνο που σχετίζονται με την

απόκτηση και τη ρύθμιση ενός συστήματος IoT για εφαρμογές χαμηλού κόστους όπως τα έξυπνα σπίτια. Παρόλες αυτές τις προκλήσεις, η διασφάλιση της ασφάλειας είναι ζωτικής σημασίας, καθώς οι έξυπνες συσκευές ενσωματώνονται περισσότερο σε κοινές υπηρεσίες Διαδικτύου (Song, 2022).

Οι απειλές στα συστήματα IoT είναι πολλές και οι κακόβουλοι χρήστες επικεντρώνονται στη φύση των συσκευών που είναι ουσιαστικά ψηφιακά συστήματα που συνδέονται στο διαδίκτυο και επικοινωνούν ασύρματα. Με την ευρεία έννοια πλέον κάθε τέτοια συσκευή από ένα απλό αισθητήρα, ένα κινητό τηλέφωνο, ένας υπολογιστής, ένα σύνολο από IoT συσκευών που συνθέτουν ένα σύστημα αποτελούν στόχο από απειλές (Sidhu, et al, 2019).

Η ιδιαιτερότητα των συσκευών IoT σε αντίθεση με τις άλλες συσκευές, είναι ότι οι χρήστες (που μπορεί να είναι απλοί καταναλωτές), δεν θα έχουν τακτική πρόσβαση σε αυτές επειδή είναι σχεδιασμένες να λειτουργούν χωρίς την ανάγκη ανθρώπινης αλληλεπίδρασης, και για το λόγο αυτό εάν η συσκευή απαιτεί ενημέρωση, ο χρήστης να μην το γνωρίζει ή να ξεχάσει να το κάνει. Σήμερα η πολυπλοκότητα των επιθέσεων στον κυβερνοχώρο αυξάνεται και φτάνουν ακόμη και στο επίπεδο του βασικού κυκλώματος - Integrated Circuit (IC). Τα IC απειλούνται με κακόβουλες εισαγωγές κατά τη σχεδίαση τους και αυτό ονομάζεται Hardware Trojan (HT) και είναι δύσκολο να εντοπιστεί στη φάση της δοκιμής (Alaali, & Elmedany, 2022).

Εστιάζοντας στις απλές συσκευές IoT οι κύριες απειλές επικεντρώνονται:

- **Επιθέσεις εμπλοκής σήματος:** Σε μια επίθεση παρεμβολής σήματος, ο επιτιθέμενος παρεμβαίνει στην επικοινωνία μεταξύ δύο συστημάτων. Τα συστήματα IoT έχουν συνήθως τα δικά τους συστήματα κόμβων. Για παράδειγμα, ένα σύστημα αντλίας έγχυσης φαρμάκων στο τομέα της υγείας έχει έναν διακομιστή ελέγχου συνδεδεμένο με πολλαπλές αντλίες έγχυσης φαρμάκων. Με ειδικό εξοπλισμό, είναι δυνατή η απομόνωση του διακομιστή ελέγχου και των αντλιών μεταξύ τους. Σε κρίσιμα συστήματα όπως αυτό, αυτή η απειλή θα μπορούσε να αποδειχθεί μοιραία (Hu, 2016).

- **Επιθέσεις άρνησης υπηρεσίας (DoS):** Σε μια επίθεση επανάληψης, ο επιτιθέμενος επαναλαμβάνει κάποια λειτουργία ή στέλνει ξανά ένα μεταδιδόμενο πακέτο. Στο παραπάνω παράδειγμα της αντλίας έγχυσης φαρμάκου, αυτό θα μπορούσε να σημαίνει ότι ένας ασθενής λαμβάνει πολλαπλές δόσεις ενός φαρμάκου. Οι επιθέσεις επανάληψης, ανεξάρτητα από το αν επηρεάζουν ή όχι τις συσκευές IoT, είναι συνήθως σοβαρές.

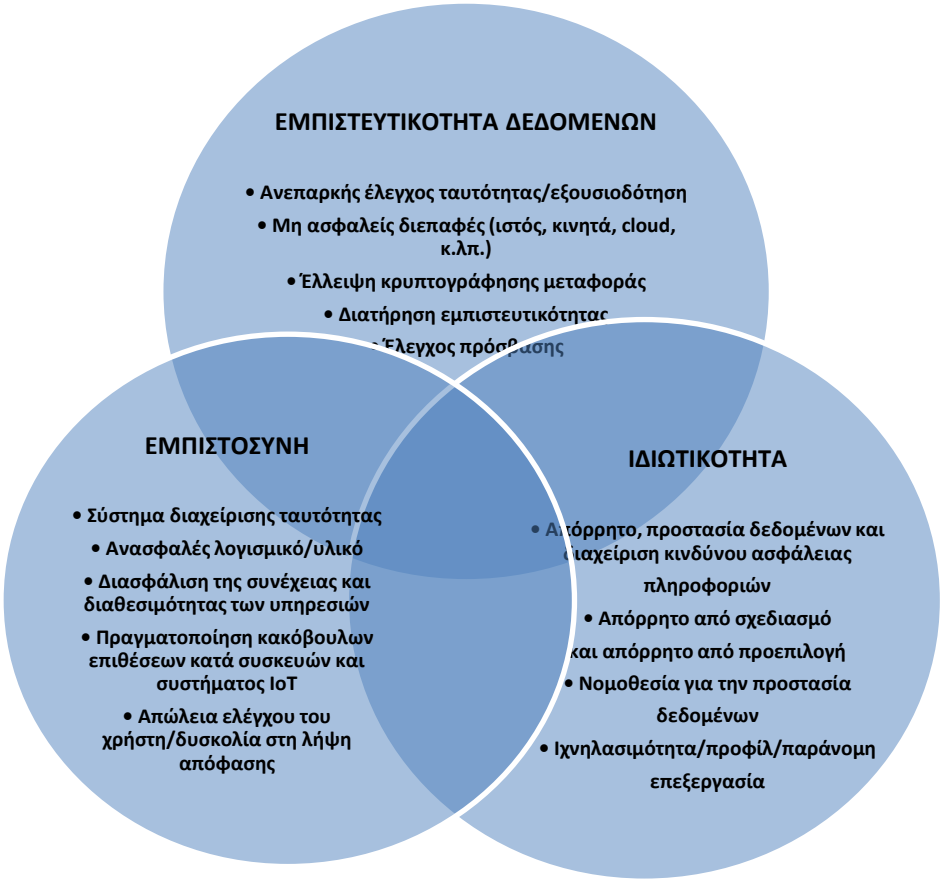
- **Επιθέσεις ακεραιότητας υλικού:** Σε επιθέσεις παραβίασης ρυθμίσεων, ο επιτιθέμενος εκμεταλλεύεται την έλλειψη ακεραιότητας ενός στοιχείου για να αλλάξει τις ρυθμίσεις του. Για την αντλία έγχυσης φαρμάκου, αυτές οι ρυθμίσεις θα μπορούσαν να περιλαμβάνουν τα εξής: ανταλλαγή του διακομιστή ελέγχου με έναν κακόβουλο διακομιστή ελέγχου, αλλαγή του κύριου φαρμάκου που χρησιμοποιείται ή αλλαγή των ρυθμίσεων δικτύου για να προκαλέσει επίθεση άρνησης υπηρεσίας (Hu, 2016).

- **Μη ασφαλή δίκτυα:** Οι συσκευές IoT ενδέχεται να επικοινωνούν μέσω μη ασφαλών δικτύων, γεγονός που τις καθιστά επιρρεπείς σε επιθέσεις.

ΚΕΦΑΛΑΙΟ 4. Σχεδίαση δοκιμή και αξιολόγηση ασφάλειας

4.1 Εισαγωγή

Ο σχεδιασμός αποτελεσματικών δοκιμών ασφάλειας IoT ξεκινά με έναν σαφή ορισμό των στόχων και του πεδίου εφαρμογής. Η κατανόηση της περίπλοκης αρχιτεκτονικής του συστήματος IoT είναι ζωτικής σημασίας. Μια ολοκληρωμένη άσκηση μοντελοποίησης απειλών εντοπίζει πιθανές ευπάθειες, επιτρέποντας την ιεράρχηση προτεραιοτήτων με βάση τον αντίκτυπο και την πιθανότητα. Η απαρίθμηση και η δημιουργία προφίλ συσκευών παρέχουν πληροφορίες για τις δυνατότητες και τις διαμορφώσεις κάθε συσκευής, αποτελώντας τη βάση για επακόλουθες δοκιμές. Η ασφάλεια πρέπει να αντιμετωπίζεται καθ' όλη τη διάρκεια του κύκλου ζωής του IoT, από τον αρχικό σχεδιασμό έως τις υπηρεσίες που εκτελούνται (Li & Xu, 2017).



Σχεδιάγραμμα 2. Θέματα ασφάλειας στο IoT.

4.2 Σχεδίαση υλικού

Ένας από τους πιο σημαντικούς φορείς επίθεσης σε μια συσκευή IoT είναι το υλικό. Εάν οι εισβολείς μπορούν να καταλάβουν τα στοιχεία υλικού ενός συστήματος, είναι συχνά σε θέση να αποκτήσουν αυξημένα προνόμια, επειδή το σύστημα σχεδόν πάντα εμπιστεύεται σιωπηρά οποιονδήποτε έχει φυσική πρόσβαση. Ακόμη και οι θύρες USB που βρίσκονται σχεδόν σε κάθε ψηφιακή συσκευή μπορούν να είναι φορείς επίθεσης (Chantzis, et al, 2021).

Η ασφάλεια στην αρχική σχεδίαση και κατασκευή μιας συσκευής IoT είναι μια προσέγγιση που επιδιώκει να ενσωματώσει εκ των προτέρων επίπεδα και δυνατότητες ασφάλειας σε προϊόντα και εφαρμογές IoT, κάτι που θα τα καταστήσει απαλλαγμένα από τρωτά σημεία και ανθεκτικά στις επιθέσεις όσο το δυνατόν περισσότερο στο μέλλον.

Λόγω της αλματώδους ανάπτυξης της αγοράς IoT, οι κατασκευαστές δημιουργούν συσκευές με γρήγορους ρυθμούς, αλλά στη διαδικασία αφήνουν κενά ασφαλείας, όπως αδύναμους κωδικούς πρόσβασης και μη αναγνωρισμένες πίσω πόρτες – backdoor[13] (κερκόπορτες). Καθώς τα προϊόντα έχουν σχεδιαστεί για να αναπτύσσονται γρήγορα και να κερδίζουν τον αγώνα για την αγορά, η ασφάλεια συχνά υποβαθμίζεται (Li & Xu, 2017).

4.3 Κρυπτογράφηση

Η χρήση πολλαπλών, μεμονωμένων σχημάτων κρυπτογράφησης είναι μια καθιερωμένη μέθοδος για την αύξηση του επιπέδου της συνολικής ασφάλειας των κρυπτογραφημένων δεδομένων. Ακρογωνιαίος λίθος της σημερινής τεχνολογίας

[13] backdoor (computing). Η επίθεση με κερκόπορτα είναι ένας τρόπος πρόσβασης σε ένα σύστημα υπολογιστή ή σε κρυπτογραφημένα δεδομένα που παρακάμπτουν τους συνήθεις μηχανισμούς ασφαλείας του συστήματος. Ένας προγραμματιστής μπορεί να δημιουργήσει μια κερκόπορτα ώστε να είναι δυνατή η πρόσβαση σε μια εφαρμογή, λειτουργικό σύστημα (OS) ή δεδομένα για αντιμετώπιση προβλημάτων ή άλλους σκοπούς. Οι επιτιθέμενοι χρησιμοποιούν backdoors που εγκαθιστούν οι προγραμματιστές λογισμικού και εγκαθιστούν επίσης οι ίδιοι backdoors ως μέρος μιας εκμετάλλευσης υπολογιστή. (Ανάκτηση 30.8.2023 από https://www.techtarget.com/searchsecurity/definition/back-door)

πληροφορικής και επικοινωνιών σε όλα τα επίπεδα είναι η σύγχρονη κρυπτογραφία. Πολλαπλή κρυπτογράφηση η οποία είναι γνωστή και ως «διπλή κρυπτογράφηση», ή «υβριδική κρυπτογράφηση», επιτρέπει τον συνδυασμό πολλαπλών, μεμονωμένων κρυπτογραφικών σχημάτων προκειμένου να δημιουργηθεί ένα νέο ασφαλές σχήμα Soroceanu, et al, (2023).

4.3.1 Κρυπτογράφηση και έλεγχος ταυτότητας βάσει υλικού στο IoT

Παραδοσιακά, η ασφάλεια σημαίνει κρυπτογράφηση, ασφαλή επικοινωνία και διασφάλιση απορρήτου. Ωστόσο, στο IoT η ασφάλεια περιλαμβάνει ένα ευρύτερο φάσμα εργασιών, όπως εμπιστευτικότητα δεδομένων, διαθεσιμότητα υπηρεσιών, ακεραιότητα πληροφοριών, προστασία απορρήτου, έλεγχος πρόσβασης κ.λπ. Η κρυπτογράφηση αποδεικνύεται χρήσιμη για τον μετριασμό των προβλημάτων επεκτασιμότητας και ευπάθειας όλων των επιπέδων. Για να δημιουργηθεί ένα αξιόπιστο IoT, απαιτούνται αναλυτικά στοιχεία ασφαλείας σε επίπεδο συστήματος και προσαρμοστικό πλαίσιο πολιτικής ασφάλειας (Li & Xu, 2017).

Οι συσκευές IoT όμως δεν θα μπορούσαν να λειτουργήσουν με πολύπλοκο μηχανισμό κρυπτογράφησης με τους περιορισμένους πόρους, την ικανότητα επεξεργασίας, τις τηλεπικοινωνίες και τον όγκο αποθήκευσης. Επομένως, θα πρέπει να αναπτυχθεί μια ελαφριά κρυπτογράφηση, η οποία είναι εύκολη στη μεταφορά, με λιγότερο κόστος πόρων και μικρότερη κλίμακα (Song, 2022).

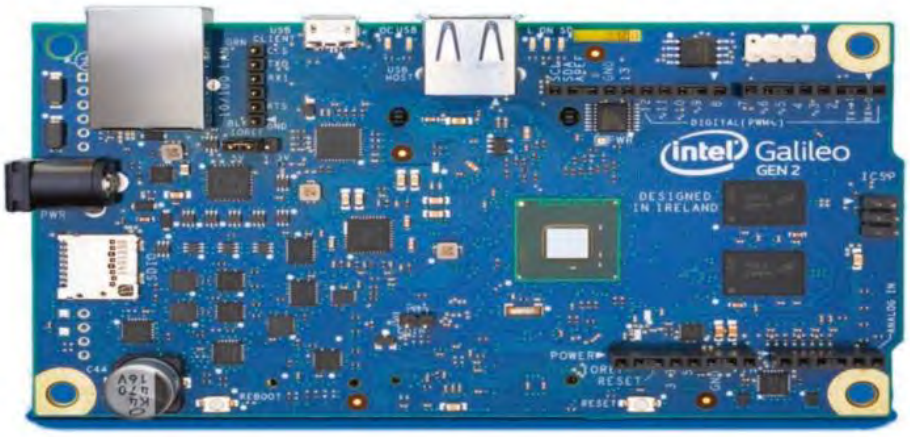
Η κρυπτογράφηση και ο έλεγχος ταυτότητας που βασίζεται σε υλικό είναι κρίσιμα στοιχεία των στρατηγικών ασφάλειας IoT. Διαδικασίες κρυπτογράφηση με βάση το υλικό:

Κρυπτογράφηση με βάση το υλικό

- **Secure Elements (SE) ή Hardware Security Modules (HSM):** Πρόκειται για εξειδικευμένα στοιχεία υλικού που παρέχουν ένα ασφαλές περιβάλλον για κρυπτογραφικές λειτουργίες. Μπορούν να αποθηκεύουν ευαίσθητες

πληροφορίες όπως κρυπτογραφικά κλειδιά ώστε να μπορούν να εκτελούν λειτουργίες κρυπτογράφησης/αποκρυπτογράφησης σε προστατευμένο περιβάλλον.

- Η Microchip και η Google συνεργάστηκαν για να σας προσφέρουν την ιδανική βάση για τη δημιουργία του επόμενου σχεδιασμού σας που συνδέεται με το cloud. Συνδυάζοντας έναν ισχυρό μικροελεγκτή AVR®, ένα IC ασφαλούς στοιχείου CryptoAuthentication και έναν πλήρως πιστοποιημένο ελεγκτή δικτύου Wi-Fi, αυτές οι πλακέτες προσφέρουν τον πιο απλό και αποτελεσματικό τρόπο σύνδεσης ενσωματωμένων εφαρμογών στην βασική πλατφόρμα Cloud IoT της Google όπως διακρίνεται στην εικόνα 2 που δείχνει το κιτ ανάπτυξης AVR IoT (Khaled, 2019).



Εικόνα 4. Κιτ ανάπτυξης Intel Galileo Gen. 2

❖ **Λειτουργική μονάδα αξιόπιστης πλατφόρμας (TPM):** Το TPM είναι μια δυνατότητα ασφαλείας που βασίζεται σε υλικό και συχνά ενσωματώνεται σε συστήματα υπολογιστών, συμπεριλαμβανομένων συσκευών IoT. Παρέχει ασφαλή χώρο αποθήκευσης κλειδιών και εκτελεί κρυπτογραφικές λειτουργίες (Cheruvu, et al, 2020)

Ασφαλής αποθήκευση κλειδιού:

❖ Διαχείριση κλειδιών: Η ασφαλής διαχείριση κρυπτογραφικών κλειδιών είναι απαραίτητη. Οι λύσεις που βασίζονται σε υλικό διασφαλίζουν ότι τα κλειδιά

αποθηκεύονται σε περιβάλλον ανθεκτικό σε παραβιάσεις, γεγονός που καθιστά δύσκολη την εξαγωγή τους από τους εισβολείς. Οι ασφαλείς εγκαταστάσεις αποθήκευσης (γνωστές και ως αποθήκες κλειδιών) αυξάνουν την εμπιστοσύνη όταν χρησιμοποιούνται τόσο σε ένα σύστημα IoT όσο και στην υποδομή διαχείρισης. Οι παθητικές αποθήκες κλειδιών παρέχουν ένα μέσο για την ασφαλή αποθήκευση και ανάκτηση διαπιστευτηρίων. Οι κρυπτογραφικές λειτουργίες εκτελούνται εκτός αυτών των αποθηκών από την CPU της συσκευής. Αντίθετα, οι ενεργοί χώροι αποθήκευσης κλειδιών επιτρέπουν την εσωτερική εκτέλεση κρυπτογραφικών λειτουργιών μέσω μιας διεπαφής προγράμματος εφαρμογής (API), έτσι τα διαπιστευτήρια δεν εκτίθενται ποτέ (Hu, 2016).

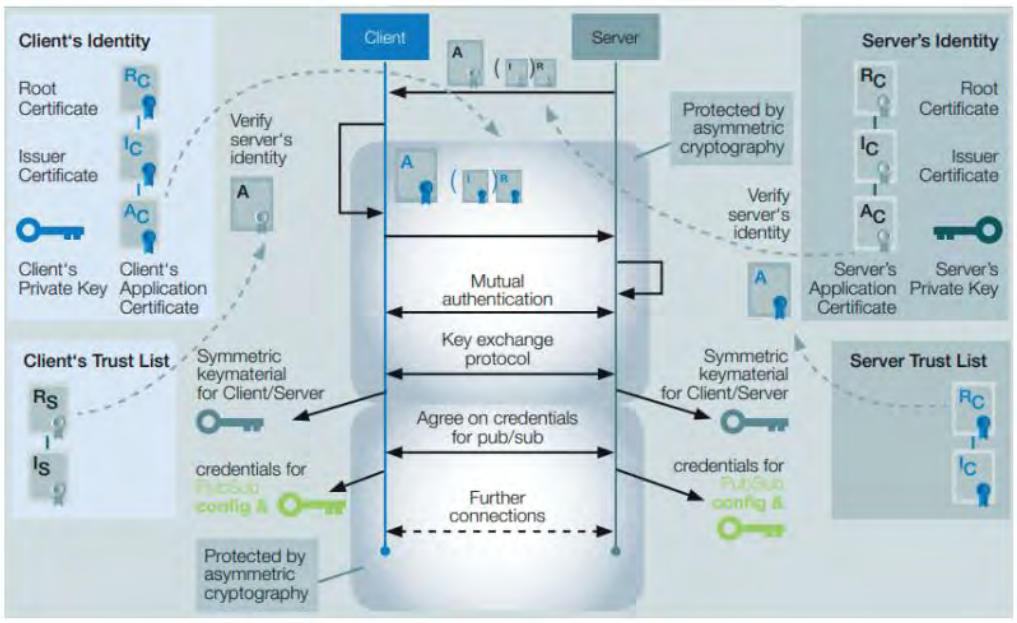
- Δημιουργία κλειδιών: Οι μονάδες που βασίζονται σε υλικό μπορούν επίσης να βοηθήσουν στη δημιουργία τυχαίων κλειδιών υψηλής ποιότητας, τα οποία είναι απαραίτητα για ισχυρή κρυπτογράφηση. Η δημιουργία κλειδιών αναφέρεται στο πώς, πότε και σε ποιες συσκευές δημιουργούν τα κρυπτογραφικά κλειδιά και χρησιμοποιώντας ποιους αλγόριθμους. Η παραγωγή κλειδιού μπορεί να πραγματοποιηθεί απευθείας στη συσκευή ή σε ένα πιο κεντρικό σύστημα, το οποίο απαιτεί μετέπειτα διανομή στη συσκευή (Russell & Van Duren, 2016).

Μηχανισμοί ελέγχου ταυτότητας:

- **Ψηφιακά πιστοποιητικά - Digital Certificates:** Η εφαρμογή ψηφιακών πιστοποιητικών βοηθά στον έλεγχο ταυτότητας συσκευών IoT. Οι συσκευές εκδίδουν πιστοποιητικά και μια υποδομή δημόσιου κλειδιού - Public Key Infrastructure (PKI) μπορεί να χρησιμοποιηθεί για τη διαχείριση πιστοποιητικών (Song, 2022). Τα πιστοποιητικά δημόσιου κλειδιού (ονομάζονται επίσης ψηφιακά πιστοποιητικά ή πιστοποιητικά ταυτότητας), οι διαδικασίες και οι τεχνολογίες κρυπτογράφησης δημόσιου κλειδιού που τα τεκμηριώνουν και οι σχέσεις εμπιστοσύνης αποτελούν τη βάση ενός PKI. Οι σχέσεις εμπιστοσύνης που βασίζονται στην έκδοση πιστοποιητικών, τα οποία με τη σειρά τους βασίζονται στην κρυπτογραφία δημόσιου κλειδιού, είναι αυτά που διαφοροποιούν τα PKI από άλλες μορφές κατασκευών ασφαλείας και αυτό που καθορίζει τις ιδιότητές τους. Ο κύκλος ζωής των πιστοποιητικών βρίσκεται στον πυρήνα των PKI. Συνήθως, μια οντότητα που ονομάζεται αρχή

πιστοποίησης (CA) εκδίδει πιστοποιητικά ταυτότητας υπογράφοντας ψηφιακά ένα σύνολο χαρακτηριστικών (σχετικά με την ταυτότητα και άλλα) συμπεριλαμβανομένου ενός δημόσιου κλειδιού (ζεύγους δημόσιου-ιδιωτικού κλειδιού στο πλαίσιο της κρυπτογραφίας δημόσιου κλειδιού). Η πράξη έκδοσης ενός τέτοιου πιστοποιητικού αποτελεί απόδειξη της σύνδεσης μεταξύ των χαρακτηριστικών και της κατοχής του δημόσιου κλειδιού (Hu, 2016).

- **Αμοιβαίος έλεγχος ταυτότητας - Mutual Authentication:** Τόσο η συσκευή IoT όσο και ο διακομιστής ελέγχουν ο ένας τον άλλον, διασφαλίζοντας ότι πραγματοποιείται επικοινωνία μεταξύ αξιόπιστων οντοτήτων. Είναι ένας προεπιλεγμένος τρόπος ελέγχου ταυτότητας σε ορισμένα πρωτόκολλα και προαιρετικός σε άλλα (Song, 2022). Η θεμελιώδης ιδέα πίσω από αυτή τη διαδικασία ελέγχου ταυτότητας, η οποία είναι κοινή σε διαδικτυακές και διαδικτυακές εφαρμογές, είναι ότι κανένα από τα μέρη δεν μπορεί να εμπιστευτεί το άλλο έως ότου επαληθευτούν οι ταυτότητες. Αυτό γίνεται για να διασφαλιστεί ότι οι χρήστες επικοινωνούν μόνο με νόμιμες οντότητες ή διακομιστές και έτσι ώστε οι διακομιστές να μπορούν να επιβεβαιώσουν ότι ο χρήστης (πελάτης) που προσπαθεί να αποκτήσει πρόσβαση έχει νόμιμο σκοπό (Anuradha & Tripathy, 2018).



Σχεδιάγραμμα 3. Αμοιβαίος έλεγχος ταυτότητας και απόκτηση διαπιστευτηρίων

- Η πλειοψηφία των συσκευών IoT απαιτούν σύνδεση σε απομακρυσμένο διακομιστή για να λειτουργούν σωστά. Μπορεί επίσης να χρειαστεί να συνδεθούν σε άλλες συσκευές Internet of Things. Οι συσκευές IoT πρέπει να το κάνουν μέσω ενός μη προστατευμένου δικτύου. Ο αμοιβαίος έλεγχος ταυτότητας ελαχιστοποιεί την πιθανότητα ένας κακόβουλος παράγοντας να θέτει σε κίνδυνο τις συνδέσεις του επαληθεύοντας ότι οι πληροφορίες που λαμβάνουν είναι ακριβείς και από αξιόπιστη πηγή.

- **Μοναδικά αναγνωριστικά υλικού - Unique Hardware Identifiers:** Σε κάθε συσκευή IoT μπορεί να δοθεί ένα μοναδικό αναγνωριστικό με βάση τα χαρακτηριστικά του υλικού της. Αυτό το αναγνωριστικό μπορεί να χρησιμοποιηθεί ως μέρος της διαδικασίας ελέγχου ταυτότητας, διασφαλίζοντας ότι μόνο εξουσιοδοτημένες συσκευές μπορούν να συνδεθούν στο δίκτυο (Kranz, 2016). Παράγοντες που επηρεάζουν την επιτυχή χρήση των συχνών αναγνωριστικών μιας χρήσης για το απόρρητο τοποθεσίας στο ασύρματο LAN είναι:

    1. ο τύπος περιβάλλοντος,
    2. η ανάλυση τοποθεσίας και
    3. η προηγούμενη γνώση του συστήματος ή του χρήστη από τον εισβολέα.

    - Πρώτον, εάν πρόκειται για ένα ανοιχτό περιβάλλον με μεγάλη διακύμανση χρηστών, όπως ένα κτίριο γραφείων με πολλούς υπαλλήλους ή σε δημόσιους χώρους όπως ένα αεροδρόμιο ή ένα εμπορικό κέντρο, είναι δύσκολο να εντοπιστούν οι αλλαγές στα αναγνωριστικά. Ωστόσο, εάν ο χρήστης βρίσκεται σε κλειστό περιβάλλον, όπως ένα εταιρικό δίκτυο όπου είναι καταχωρημένα όλα τα αναγνωριστικά διεπαφής των εξουσιοδοτημένων πελατών, οι αλλαγές στα αναγνωριστικά είναι ευκολότερο να εντοπιστούν.

    - Ο δεύτερος παράγοντας που πρέπει να ληφθεί υπόψη είναι η ανάλυση τοποθεσίας, η οποία είναι η ακρίβεια εντοπισμού ενός χρήστη. Ένα ενιαίο σημείο πρόσβασης - access point (AP) που συνδέεται με τον χρήστη θα

παρέχει μια κατά προσέγγιση εκτίμηση της τοποθεσίας του χρήστη. Από την άλλη πλευρά, πολλά AP μπορούν να εγκατασταθούν στην περιοχή, παρέχοντας πιο ακριβή ανίχνευση πληροφοριών τοποθεσίας (δηλαδή, επιτρέποντας τη συνεργασία μεταξύ των AP μέσω της προσέγγισης τριγωνισμού για τον προσδιορισμό της τοποθεσίας του χρήστη). Η λύση σε αυτό το πρόβλημα είναι ο έλεγχος της ισχύος του μεταδιδόμενου σήματος από τη συσκευή. Αυτό θα μειώσει τον αριθμό των AP που μπορούν να λάβουν τη μετάδοση. Τέλος, εάν ο εισβολέας έχει προηγούμενες γνώσεις για το περιβάλλον (π.χ. διάταξη κτιρίου, εργασία γραφείου, πρόγραμμα εργασίας των υπαλλήλων κ.λπ.), μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για την καλύτερη αναγνώριση του χρήστη (Hu, 2016).

Ακεραιότητα υλικού και λογισμικού:

- **Υπογραφή κώδικα - Code Signing:** Διασφαλίζει ότι το υλικό και το λογισμικό που εκτελούνται στη συσκευή IoT είναι νόμιμα και ότι δεν έχουν παραβιαστεί. Οι ψηφιακές υπογραφές[14] χρησιμοποιούνται για την επαλήθευση της γνησιότητας του κωδικού. Ένας εισβολέας μπορεί εύκολα να κρυφτεί ως νόμιμη πηγή εγκατάστασης κακόβουλου λογισμικού στον υπολογιστή του θύματος. Η υπογραφή κώδικα διασφαλίζει ότι αυτοί οι τύποι επιθέσεων δεν μπορούν να συμβούν, εφόσον οι χρήστες κατεβάζουν μόνο λογισμικό που θεωρείται ασφαλές από το λειτουργικό τους σύστημα. Σήμερα, όταν γίνεται λήψη λογισμικού σε υπολογιστή, το Λειτουργικό Σύστημα ελέγχει για το ψηφιακό πιστοποιητικό που δημιουργήθηκε μέσω της υπογραφής κώδικα, για να διασφαλίσει την ασφάλεια του λογισμικού που επιχειρείται να εγκατασταθεί. Εάν δεν βρεθεί ψηφιακό πιστοποιητικό, τότε ο χρήστης ειδοποιείται για αυτό το γεγονός και του ζητείται είτε να σταματήσει είτε να συνεχίσει την εγκατάσταση.

[14] https://www.encryptionconsulting.com/education-center/what-is-code-signing/ what is Code Signing? How does Code Signing work? (Ανάκτηση 10.9.2023).

Προστασία φυσικής παραβίασης:

- Συσκευασία αποδείξεως παραβίασης: Μπορούν να ληφθούν φυσικά μέτρα για να καταστεί εμφανές εάν μια συσκευή έχει παραβιαστεί φυσικά. Αυτό μπορεί να περιλαμβάνει σφραγίδες και περιβλήματα που είναι δύσκολο να ανοίξουν χωρίς να αφήνουν ορατά σημάδια παραβίασης. Οι διασφαλίσεις φυσικής ασφάλειας επηρεάζουν τον αρχιτεκτονικό σχεδιασμό, τις πολιτικές και τις διαδικασίες, ακόμη και τις προσεγγίσεις απόκτησης τεχνολογίας. Η έξοδος από το μοντέλο απειλής θα πρέπει να καθοδηγεί τη δημιουργία σχεδίου φυσικής ασφάλειας και θα πρέπει να λαμβάνει υπόψη εάν τα στοιχεία IoT τοποθετούνται σε εκτεθειμένες τοποθεσίες (Russell & Van Duren, 2016).

Πρωτόκολλα ασφαλούς επικοινωνίας:

- **TLS/SSL για ασφάλεια επιπέδου μεταφοράς:** Διασφαλίζει ότι τα δεδομένα που μεταδίδονται μεταξύ συσκευών IoT και διακομιστών είναι κρυπτογραφημένα και ασφαλή. Το SSL/TLS κρυπτογραφεί τις επικοινωνίες μεταξύ πελάτη και διακομιστή, κυρίως τα προγράμματα περιήγησης ιστού, ιστοσελίδες και εφαρμογές. Η κρυπτογράφηση SSL (Secure Sockets Layer) είναι πιο σύγχρονη και ασφαλής και αντικατέστησε τη κρυπτογράφηση TLS (Transport Layer Security) (Song, 2022).

- **VPN - Virtual Private Network - Εικονικό ιδιωτικό δίκτυο:** Η δημιουργία ασφαλών, κρυπτογραφημένων σηράγγων επικοινωνίας μπορεί να βελτιώσει την ασφάλεια των συσκευών IoT. Ένα VPN αναδρομολογεί την επισκεψιμότητα του χρήστη μέσω ενός απομακρυσμένου διακομιστή, κρυπτογραφώντας το στη διαδικασία (DeNardis, 2020). Συνήθως, όταν προσπαθεί ο χρήστης να αποκτήσει πρόσβαση σε έναν ιστότοπο, ο ISP (Παροχέας Υπηρεσιών Διαδικτύου) λαμβάνει το αίτημα και το ανακατευθύνει στον προορισμό. Αλλά όταν συνδέετε σε ένα VPN, ανακατευθύνει την κυκλοφορία στο Διαδίκτυο μέσω ενός απομακρυσμένου διακομιστή πριν το στείλει πίσω στον προορισμό (Kranz, 2016).

Η εφαρμογή αυτών των μέτρων ασφαλείας που βασίζονται σε υλικό βοηθά στη δημιουργία μιας ισχυρής βάσης ασφάλειας για συσκευές IoT, προστατεύοντάς τις από ένα ευρύ φάσμα απειλών. Είναι σημαντικό να σημειωθεί ότι η ασφάλεια θα πρέπει να λαμβάνεται υπόψη σε όλο τον κύκλο ζωής μιας συσκευής IoT, από τη σχεδίαση και την κατασκευή έως την ανάπτυξη και τον παροπλισμό. Επιπλέον, η ενημέρωση σχετικά με τα πιο πρόσφατα πρότυπα ασφαλείας και τις βέλτιστες πρακτικές είναι ζωτικής σημασίας καθώς εξελίσσεται το περιβάλλον του IoT.

Ένα παράδειγμα κυβερνοεπίθεσης σε υλικό IoT αλλά και σε οποιοδήποτε ψηφιακό υλικό είναι η επίθεση πλευρικού καναλιού - A side-channel attack[15] (SCA). Η επίθεση πλευρικού καναλιού είναι μια εκμετάλλευση ασφαλείας που επιχειρεί να εξάγει μυστικά από ένα τσιπ ή ένα σύστημα. Αυτό μπορεί να επιτευχθεί με τη μέτρηση ή την ανάλυση διαφόρων φυσικών παραμέτρων. Στα παραδείγματα περιλαμβάνονται το ρεύμα τροφοδοσίας, ο χρόνος εκτέλεσης και η ηλεκτρομαγνητική εκπομπή. Αυτές οι επιθέσεις αποτελούν σοβαρή απειλή για λειτουργικές μονάδες που ενσωματώνουν κρυπτογραφικά συστήματα.

Η επίθεση αυτή δεν στοχεύει απευθείας ένα πρόγραμμα ή τον κώδικά του. Αντίθετα, επιχειρεί να συγκεντρώσει πληροφορίες ή να επηρεάσει την εκτέλεση του προγράμματος ενός συστήματος μετρώντας ή εκμεταλλευόμενος έμμεσες επιδράσεις του συστήματος ή του υλικού του. Με απλά λόγια, μια επίθεση πλευρικού καναλιού σπάει την κρυπτογραφία εκμεταλλευόμενη πληροφορίες που διέρρευσαν ακούσια από ένα σύστημα. Ένα τέτοιο παράδειγμα είναι η επίθεση phreaking van Eck , η οποία είναι επίσης γνωστή ως Transient Electromagnetic Pulse Emanation Standard[16] (TEMPEST). Αυτή η επίθεση παρακολουθεί την ακτινοβολία ηλεκτρομαγνητικού πεδίου (EMF) που εκπέμπεται από μια οθόνη υπολογιστή για την προβολή πληροφοριών πριν κρυπτογραφηθούν.

[15] https://www.rambus.com/blogs/side-channel-attacks/ Side-channel attacks explained: everything you need to know, (Ανάκτηση 5.10.2023)

[16] Η προδιαγραφή TEMPEST (που ορίστηκε από την Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ) αναφέρεται στην ευαισθησία των συσκευών υπολογιστών και τηλεπικοινωνιών σε κλοπή δεδομένων. Ορισμένος ηλεκτρονικός εξοπλισμός εκπέμπει ηλεκτρομαγνητική ακτινοβολία ή διακυβευτικές εκπομπές (CE) με τρόπο που μπορεί να χρησιμοποιηθεί για την ανακατασκευή κατανοητών δεδομένων. (Ανάκτηση 5.10.2023 από https://www.astrodynetdi.com/blog/tempest-emi-filters)

4.4 Δοκιμές και αξιολόγηση υλικού IoT

Η δοκιμή και η αξιολόγηση του υλικού IoT (Internet of Things) είναι ζωτικής σημασίας για τη διασφάλιση της αξιοπιστίας, της ασφάλειας και της απόδοσης των συσκευών. Τα κυριότερα βήματα για τη δοκιμή και την αξιολόγηση υλικού IoT είναι:

1. Λειτουργική δοκιμή:

- **Δοκιμή συνδεσιμότητας:** Έλεγχος για το αν η συσκευή μπορεί να συνδεθεί στο προβλεπόμενο δίκτυο (Wi-Fi, κινητό, Bluetooth, κ.λπ.). – έλεγχος της ικανότητας της συσκευής να δημιουργεί και να διατηρεί συνδέσεις.
- **Επικοινωνία δεδομένων:** Έλεγχος εάν η συσκευή μπορεί να στείλει και να λάβει δεδομένα με ακρίβεια. Έλεγχος για την ακεραιότητα των δεδομένων και την αντιμετώπιση σφαλμάτων κατά την επικοινωνία.
- **Δοκιμή αισθητήρα και ενεργοποιητή:** Έλεγχος ότι οι αισθητήρες συλλέγουν δεδομένα με ακρίβεια. Δοκιμή στους ενεργοποιητές για επαλήθευση ότι ανταποκρίνονται σωστά στις εντολές.
- **Διαχείριση ενέργειας:** Έλεγχος στην κατανάλωση ενέργειας σε διαφορετικές λειτουργίες (ενεργός, αναμονή). – Επαλήθευση για τη σωστή λειτουργία κάτω από διαφορετικά σενάρια ισχύος (Russell & Van Duren, 2016; Khaled, 2019).

2. Δοκιμή απόδοσης:

- **Δοκιμή επεκτασιμότητας:** Αξιολόγηση της απόδοσης του συστήματος όταν αυξάνεται ο αριθμός των συνδεδεμένων συσκευών. Έλεγχος για το πόσο καλά διαχειρίζεται το σύστημα και οι συσκευές μεγάλο όγκο δεδομένων.
- **Δοκιμή λανθάνοντος χρόνου:** Μέτρηση του χρόνου που απαιτείται για να μεταφερθούν τα δεδομένα από τη συσκευή στον διακομιστή και πίσω. Έλεγχος ότι η καθυστέρηση είναι εντός αποδεκτών ορίων (Khaled, 2019).
- **Έλεγχος διέλευσης:** Αξιολόγηση της ποσότητας δεδομένων που μπορεί να χειριστεί η συσκευή σε ένα δεδομένο χρονικό πλαίσιο. Δοκιμή για πιθανά σημεία συμφόρησης στη μεταφορά δεδομένων.

3. Δοκιμή ασφαλείας:

- **Έλεγχος ταυτότητας και εξουσιοδότηση:** Δοκιμή στους μηχανισμούς ελέγχου ταυτότητας της συσκευής. Επιβεβαίωση ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση και να ελέγχουν τη συσκευή (Hu, 2016).
- **Κρυπτογράφηση δεδομένων:** Επαλήθευση ότι τα δεδομένα που μεταδίδονται μεταξύ της συσκευής και του διακομιστή είναι κρυπτογραφημένα. – Έλεγχος για τρωτά σημεία στους αλγόριθμους κρυπτογράφησης.
- **Ασφάλεια υλικού και λογισμικού:** Ενημέρωση τακτικά και δοκιμή του υλικού και του λογισμικού για αναβαθμίσεις και επιδιορθώσεις των τρωτών σημείων ασφαλείας (Patel, & Nishant, 2019).

4. Δοκιμή διαλειτουργικότητας:

- Έλεγχος ότι η συσκευή μπορεί να λειτουργεί απρόσκοπτα με άλλες συσκευές και πλατφόρμες IoT. Δοκιμή συμβατότητας με διάφορα πρωτόκολλα και πρότυπα επικοινωνίας.

5. Δοκιμή αξιοπιστίας και ανθεκτικής λειτουργίας:

- Έλεγχος στην αξιοπιστία της συσκευής υπό διαφορετικές περιβαλλοντικές συνθήκες. Δοκιμές ακραίων καταστάσεων για αξιολόγηση στην απόδοση της συσκευής υπό ακραίες συνθήκες (Chantzis, et al, 2021).

6. Δοκιμή χρηστικότητας:

- Αξιολόγηση της διεπαφής χρήστη και τη συνολική εμπειρία χρήστη. Έλεγχος στις διαδικασίες ρύθμισης, διαμόρφωσης και αντιμετώπισης προβλημάτων συσκευής.

7. Τεκμηρίωση και υποστήριξη:

- Έλεγχος και τεκμηρίωση για ακρίβεια και πληρότητα (Cheruvu, et al, 2020)

8. Δοκιμή κύκλου ζωής:

- Δοκιμή στη συσκευή κατά τη διάρκεια του αναμενόμενου κύκλου ζωής της για τον εντοπισμό από πιθανά προβλήματα με μακροχρόνια χρήση. Πρέπει να

λαμβάνεται υπ' υπόψιν, παράγοντες όπως η υποβάθμιση των εξαρτημάτων, η φθορά και η απαξίωση του λογισμικού.

Η διεξοδική δοκιμή και αξιολόγηση σε κάθε στάδιο του κύκλου ζωής ανάπτυξης υλικού IoT είναι απαραίτητες για την παροχή ενός αξιόπιστου και ασφαλούς προϊόντος. Οι συνεχείς δοκιμές, ειδικά στον ταχέως εξελισσόμενο τομέα του IoT, συμβάλλουν στη διασφάλιση ότι οι συσκευές πληρούν τα βιομηχανικά πρότυπα και τις ρυθμιστικές απαιτήσεις.

Καμία ενέργεια από μόνη της δεν μπορεί να αντιμετωπίσει επαρκώς τα προβλήματα απορρήτου, ασφάλειας και διαλειτουργικότητας που αναδύονται στα κυβερνοφυσικά συστήματα. Οι παγκόσμιες συζητήσεις γύρω από τη «θέσπιση κανόνων» μπορούν να επικεντρωθούν πολύ αποκλειστικά στην κυβερνητική δράση και να κάνουν αδικαιολόγητες υποθέσεις σχετικά με το πόσο αξιόπιστες είναι οι κυβερνήσεις να συμμορφώνονται με τους κανόνες. Η ρύθμιση από μόνη της δεν επαρκεί για την αντιμετώπιση της ασφάλειας και της ιδιωτικής ζωής, επειδή η νομοθεσία τόσο συχνά ακολουθεί τις τεχνολογικές αλλαγές και λόγω φραγμών τεχνολογικής πολυπλοκότητας που μπορούν να εμποδίσουν τη διαμόρφωση ουσιαστικής πολιτικής (DeNardis, 2020).

Οι συνέπειες των αστοχιών ασφάλειας του IoT μπορεί να προκαλέσουν άμεση απώλεια ζωής. Τα χρονοδιαγράμματα σχεδιασμού, ανάπτυξης, υλοποίησης, λειτουργίας και απόσυρσης μετρώνται συχνά σε δεκαετίες. Ο χρόνος απόκρισης μπορεί επίσης να παραταθεί λόγω σύνθεσης, περιβάλλοντος και περιβάλλοντος. Για παράδειγμα, ο συνδεδεμένος εξοπλισμός σε μια μονάδα παραγωγής ηλεκτρικής ενέργειας αναμένεται συχνά να ζει για περισσότερα από 20 χρόνια χωρίς αντικατάσταση. Όμως, οι επιθέσεις εναντίον ενός Ουκρανού προμηθευτή ενέργειας προκάλεσαν διακοπές λίγα δευτερόλεπτα αφότου οι αντίπαλοι ανέλαβαν δράση εντός της υποδομής του βιομηχανικού ελέγχου (Chantzis, et al, 2021).

Οι συσκευές IoT λειτουργούν συχνά σε συγκεκριμένα πλαίσια και περιβάλλοντα, όπως σπίτια, όπου ελέγχονται από άτομα χωρίς τη γνώση ή τους πόρους που απαιτούνται για την ασφαλή ανάπτυξη, λειτουργία και συντήρηση του συστήματος. Συνήθως μειώνουν το κόστος εξαρτημάτων στο ελάχιστο, μεταθέτοντας την ασφάλεια σε μεταγενέστερη

χρονική περίοδο. Επίσης, πολλές από αυτές τις συσκευές απευθύνονται σε πελάτες που έχουν σαν πρώτο κριτήριο τις τιμές με αποτέλεσμα την επιλογή μη εγκεκριμένων και ενδεδειγμένων συσκευών για την ασφαλή ανάπτυξη της υποδομής. Για παράδειγμα, δεν πρέπει να αναμένεται από τον οδηγό ενός σύγχρονου διασυνδεδεμένου αυτοκινήτου να εγκαταστήσει προϊόντα ασφαλείας μετά την αγορά για προστασία από ιούς. Ούτε πρέπει να αναμένεται από αυτούς να έχουν την τεχνογνωσία ή την ικανότητα να ανταποκρίνονται αρκετά γρήγορα κατά τη διάρκεια ενός συμβάντος ασφαλείας. Αλλά αυτό θα πρέπει να αποτελεί προτεραιότητα από μια επιχείρηση, όταν μάλιστα οι ενέργειες και οι λειτουργίες της έχουν επιπτώσεις στο κοινωνικό σύνολο και στο περιβάλλον (Chantzis, et al, 2021).

ΚΕΦΑΛΑΙΟ 5. Αναδυόμενες τάσεις στην ασφάλεια υλικού για το IoT

5.1 Εισαγωγή

Το Διαδίκτυο των Πραγμάτων έχει σημειώσει εκθετική ανάπτυξη τα τελευταία χρόνια, με τον πολλαπλασιασμό των συνδεδεμένων συσκευών. Ωστόσο, αυτή η αύξηση της συνδεσιμότητας έχει προκαλέσει επίσης πρωτοφανείς προκλήσεις ασφάλειας. Καθώς το τοπίο των απειλών εξελίσσεται, το ίδιο συμβαίνει και με την ανάγκη για ισχυρές λύσεις ασφάλειας υλικού για συσκευές IoT (Chantzis, et al, 2021). Αρκετές αναδυόμενες τάσεις διαμορφώνουν το μέλλον της ασφάλειας υλικού στον χώρο του IoT. Με την κλιμακούμενη πολυπλοκότητα των απειλών στον κυβερνοχώρο, η κρυπτογράφηση που βασίζεται σε υλικό αποκτά πρώτη προτεραιότητα. Οι συσκευές IoT ενσωματώνουν αποκλειστικούς επιταχυντές κρυπτογράφησης για να χειρίζονται αποτελεσματικά τις εργασίες κρυπτογράφησης, μειώνοντας την επιβάρυνση του κύριου επεξεργαστή της συσκευής. Αυτό όχι μόνο ενισχύει την ασφάλεια αλλά και ελαχιστοποιεί τον αντίκτυπο στην απόδοση της συσκευής (Song, 2022).

5.2 Ασφάλεια υλικού IoT και τεχνητή νοημοσύνη

Η εξαγωγή πληροφοριών από τον τεράστιο όγκο δεδομένων που συλλέγονται από διάφορα περιβάλλοντα IoT είναι μια πραγματική πρόκληση. Προβλέπεται ότι η αντιμετώπιση ενός τόσο τεράστιου όγκου δεδομένων (ακόμη και ένα δείγμα τους) με παραδοσιακές μεθόδους είναι υπερβολικά χρονοβόρα διαδικασία εκτός από τα σενάρια ασφάλειας που προκύπτουν (Song, 2022).

Η τεχνητή νοημοσύνη (AI) είναι ζωτικής σημασίας για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των συσκευών IoT και των δεδομένων που χειρίζονται. Βασικά ζητήματα όσον αφορά τη σύγκλιση της ασφάλειας υλικού IoT και της τεχνητής νοημοσύνης αναλύονται παρακάτω:

Έλεγχος ταυτότητας συσκευής και έλεγχος πρόσβασης:

- **Ενσωμάτωση AI:** Η τεχνητή νοημοσύνη μπορεί να βελτιώσει τον έλεγχο ταυτότητας ενσωματώνοντας ανάλυση συμπεριφοράς και ανίχνευση ανωμαλιών. Οι αλγόριθμοι τεχνητής νοημοσύνης μπορούν να μάθουν την τυπική συμπεριφορά των συσκευών και να εντοπίσουν αποκλίσεις που μπορεί να υποδηλώνουν απειλή για την ασφάλεια (Song, 2022).

Κρυπτογράφηση δεδομένων:

- **Ενσωμάτωση AI:** Η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για τη βελτιστοποίηση των διαδικασιών κρυπτογράφησης, όπως με τη δυναμική προσαρμογή των επιπέδων κρυπτογράφησης με βάση το αντιληπτό επίπεδο απειλής ή με τον εντοπισμό μοτίβων που μπορεί να υποδεικνύουν την ανάγκη για αυξημένη κρυπτογράφηση.

Ανίχνευση ανωμαλιών και νοημοσύνη απειλών:

- **Ασφάλεια IoT:** Ο εντοπισμός μη φυσιολογικής συμπεριφοράς ή πιθανών απειλών για την ασφάλεια σε πραγματικό χρόνο είναι κρίσιμος. Αυτό περιλαμβάνει την παρακολούθηση της συμπεριφοράς της συσκευής και της κυκλοφορίας δικτύου για ασυνήθιστα μοτίβα. Οι αλγόριθμοι τεχνητής νοημοσύνης, ιδιαίτερα τα μοντέλα μηχανικής μάθησης (ML), μπορούν να αναλύσουν μεγάλα σύνολα δεδομένων για να εντοπίσουν ανωμαλίες και πιθανές απειλές ασφαλείας πιο αποτελεσματικά από τα παραδοσιακά συστήματα που βασίζονται σε κανόνες. Τα μοντέλα ML μπορούν να προσαρμόζονται και να βελτιώνονται με την πάροδο του χρόνου καθώς μαθαίνουν από νέα δεδομένα (Cheruvu, et al, 2020)

Ανάλυση συμπεριφοράς και προγνωστική συντήρηση:

- Η κατανόηση της κανονικής συμπεριφοράς της συσκευής είναι ζωτικής σημασίας για τον εντοπισμό μη φυσιολογικών μοτίβων που μπορεί να

υποδηλώνουν παραβίαση ασφάλειας. Η τεχνητή νοημοσύνη μπορεί να αναλύσει ιστορικά δεδομένα για να προβλέψει πιθανά ζητήματα ασφάλειας ή αστοχίες συσκευών. Τα μοντέλα πρόβλεψης συντήρησης μπορούν να βοηθήσουν στην αποφυγή τρωτών σημείων ασφαλείας εντοπίζοντας και αντιμετωπίζοντας πιθανά ζητήματα προτού καταστούν κρίσιμα (Patel, & Nishant, 2019).

5.3 Ασφάλεια υλικού IoT και λύσεις με την τεχνολογία Blockchain

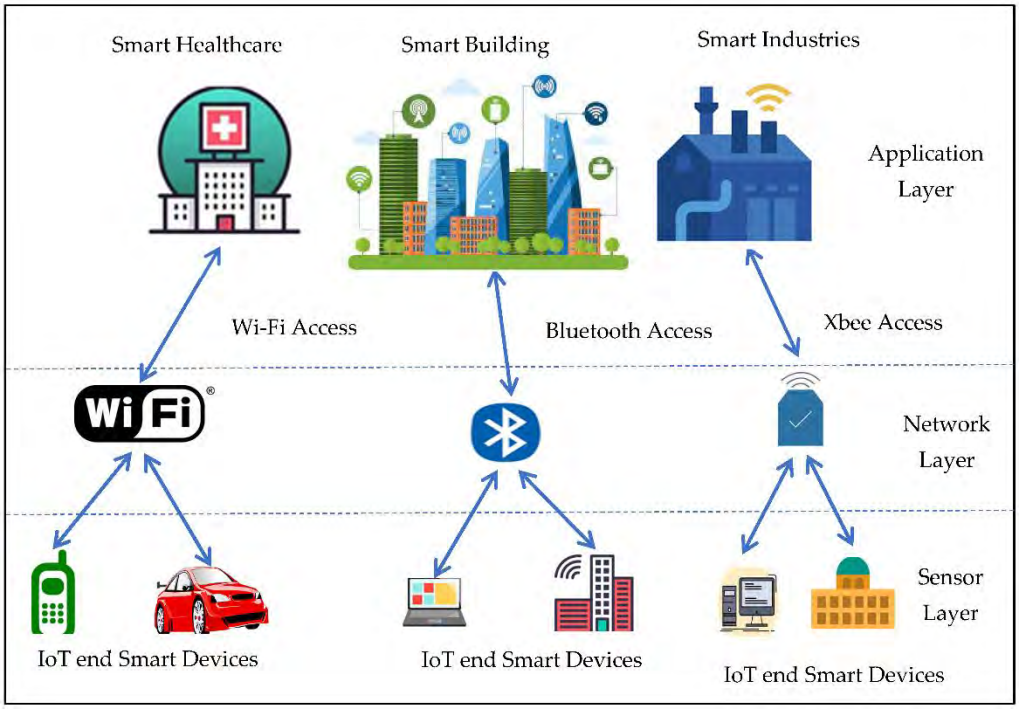
Η τεχνολογία Blockchain έχει αναδειχθεί ως μια από τις πιο μεταμορφωτικές και καινοτόμες τεχνολογίες του 21ου αιώνα. Αρχικά είχε σχεδιαστεί ως η υποκείμενη τεχνολογία για τα κρυπτονομίσματα όπως το Bitcoin, αλλά τώρα έχει εξελιχθεί πολύ πέρα από τον αρχικό του σκοπό. Σήμερα, το blockchain αναδιαμορφώνει διάφορους κλάδους σε παγκόσμιο επίπεδο (Lipovyanov, 2019).

Στον πυρήνα του, το blockchain είναι μια τεχνολογία κατανεμημένης λογιστικής που καταγράφει και επαληθεύει τις συναλλαγές με ασφαλή, διαφανή και αμετάβλητο τρόπο. Σε αντίθεση με τα παραδοσιακά κεντρικά συστήματα, όπου μια μεμονωμένη οντότητα, όπως μια τράπεζα ή μια κυβέρνηση, διατηρεί τον έλεγχο, ένα δίκτυο blockchain λειτουργεί σε ένα αποκεντρωμένο δίκτυο υπολογιστών. Αυτοί οι υπολογιστές, γνωστοί ως κόμβοι, συνεργάζονται για την επικύρωση και την καταγραφή συναλλαγών, δημιουργώντας μια αλυσίδα μπλοκ που περιέχει ένα ιστορικό όλων των συναλλαγών στο δίκτυο (Treiblmaier Beck, 2019).

Βασικές αρχές της τεχνολογίας Blockchain

- Αποκέντρωση: Το Blockchain λειτουργεί σε ένα αποκεντρωμένο δίκτυο, εξαλείφοντας την ανάγκη για μια κεντρική αρχή. Αυτή η αποκέντρωση ενισχύει την ασφάλεια, μειώνει τον κίνδυνο απάτης και αυξάνει τη διαφάνεια.
- Διαφάνεια: Όλες οι συναλλαγές σε ένα blockchain είναι ορατές σε όλους τους συμμετέχοντες στο δίκτυο. Αυτή η διαφάνεια βοηθά στην πρόληψη της απάτης και διασφαλίζει ότι όλα τα μέρη έχουν πρόσβαση στις ίδιες πληροφορίες.

- Αμετάβλητο: Από τη στιγμή που μια συναλλαγή καταγράφεται σε μια αλυσίδα μπλοκ, είναι σχεδόν αδύνατο να τροποποιηθεί ή να διαγραφεί. Αυτή η αμετάβλητη διασφαλίζει την ακεραιότητα των δεδομένων και προσθέτει ένα επιπλέον επίπεδο ασφάλειας (Treiblmaier Beck, 2019).
- Ασφάλεια: Το Blockchain χρησιμοποιεί κρυπτογραφικές τεχνικές για την ασφάλεια των συναλλαγών και τον έλεγχο της πρόσβασης στα δεδομένα. Αυτό το καθιστά εξαιρετικά ανθεκτικό στο hacking και την απάτη.



Σχεδιάγραμμα 4. Ασφάλεια υλικού IoT και λύσεις με την τεχνολογία Blockchain

Το IoT δεν αντιμετωπίζει μόνο ζητήματα ασφάλειας όπως η ασφάλεια λογισμικού και υλικού και προστασίας δικτύου, αλλά και νέους κινδύνους ασφαλείας όπως εισβολή, μη εξουσιοδοτημένη πρόσβαση, υποκλοπή, απώλεια δεδομένων κ.λπ. Αποτελεί σοβαρή απειλή για την ασφάλεια και το απόρρητο των χρηστών. Ο έλεγχος πρόσβασης είναι μια τεχνολογία που διαχειρίζεται την επαλήθευση ταυτότητας και την εξουσιοδότηση πρόσβασης, ανάκτησης και λειτουργίας πόρων, έτσι ώστε οι πόροι να μπορούν να χρησιμοποιούνται εντός νόμιμου εύρους ή να υπόκεινται σε περιορισμούς χρήσης. Είναι ένα σημαντικό μέτρο για τη διατήρηση της ασφάλειας του δικτύου και

της ασφάλειας δεδομένων. Τα παραδοσιακά μοντέλα ελέγχου πρόσβασης βασίζονται σε κεντρικές οντότητες αποφάσεων εξουσιοδότησης, οι οποίες λαμβάνουν αποφάσεις ελέγχου πρόσβασης με βάση τις πολιτικές ελέγχου πρόσβασης και άλλες πληροφορίες χαρακτηριστικών (Jiang, et al, 2023)

Το Blockchain, ως αποκεντρωμένη και κατανεμημένη τεχνολογία, προσφέρει πιθανές λύσεις. Με την ικανότητα του blockchain να παρέχει αποκεντρωμένη αξιόπιστη αποθήκευση (Patel, & Nishant, 2019), οι πολιτικές ελέγχου πρόσβασης και τα αρχεία σε ένα κατανεμημένο σύστημα μπορούν να αποθηκευτούν με ασφάλεια στο blockchain χωρίς παραβίαση, και το σύστημα είναι επίσης εξοπλισμένο με ισχυρή δυνατότητα ελέγχου. Επιπλέον, η εμφάνιση έξυπνων συμβολαίων διευρύνει την ικανότητα του blockchain για διάφορες αποκεντρωμένες εφαρμογές. Έτσι, το blockchain μπορεί να λειτουργήσει ως μια ασφαλής και αξιόπιστη αποκεντρωμένη πλατφόρμα, παρέχοντας ισχυρή ιχνηλασιμότητα και επαληθευσιμότητα για τον έλεγχο πρόσβασης στο IoT (Jiang, et al, 2023)

Τεχνολογικά, το blockchain επιλύει τα προβλήματα ασφαλείας που δημιουργούνται από κεντρικά μοντέλα που βασίζονται στην εμπιστοσύνη, εγγυάται την ασφαλή μεταφορά αξίας με βάση αλγόριθμους κρυπτογραφίας, διασφαλίζει την ιχνηλασιμότητα και τη μη παραβίαση δεδομένων που βασίζονται σε αλυσίδες κατακερματισμού και μηχανισμούς χρονικής σήμανσης, εγγυάται τη συνέπεια μπλοκ δεδομένων μεταξύ κόμβων που βασίζονται σε συναινετικούς αλγόριθμους και διασφαλίζει το προγραμματιζόμενο συμβόλαιο νοημοσύνης που βασίζεται σε αυτοματοποιημένους κώδικες σεναρίων και εικονικές μηχανές (Cheruvu, et al, 2020). Τα τελευταία χρόνια, η τεχνολογία blockchain έχει επεκταθεί από τον χρηματοοικονομικό τομέα στον τομέα του Internet of Things (Song, 2022).

5.4 Επιπτώσεις και κίνδυνοι από την ευρεία χρήση του IoT

Μία από τις κύριες ανησυχίες που σχετίζονται με τη διάδοση του IoT είναι ο αυξημένος κίνδυνος παραβίασης δεδομένων. Με ένα πλήθος διασυνδεδεμένων συσκευών που ανταλλάσσουν πληροφορίες, αυξάνεται η πιθανότητα μη εξουσιοδοτημένης

πρόσβασης και κακής χρήσης ευαίσθητων δεδομένων. Από προσωπικές πληροφορίες σε έξυπνες οικιακές συσκευές έως κρίσιμα δεδομένα σε βιομηχανικούς αισθητήρες, η ασφάλεια των δικτύων IoT πρέπει να είναι ισχυρή για να αποτρέπει κακόβουλους παράγοντες από την εκμετάλλευση ευπαθειών. (Hu, 2016).

Το απόρρητο, όπως και κάθε άλλη πιθανή απαίτηση ή ευπάθεια σε ένα δεδομένο σύστημα ή υπηρεσία IoT, είναι κάτι που πρέπει να εκτιμηθεί και όχι να υποτεθεί. Η τεράστια ποσότητα δεδομένων που υπάρχει στο σύνολο του διαδικτύου των πραγμάτων, σε όλα τα στοιχεία και τις υπηρεσίες του, ανεξάρτητα από τη διαφορά ιδιοκτησίας και διαχείρισης του, τη φυσική και λογική αποθήκευση, σημαίνει ότι δεν υπάρχει αμφιβολία ότι το IOT, είναι δυνητικά μια τεράστια και μαζική πηγή δεδομένων, πολλές φορές και προσωπικών δεδομένων. (Macaulay, 2017).

Καθώς ο αριθμός των συσκευών IoT συνεχίζει να αυξάνεται, το ίδιο συμβαίνει και με την επιφάνεια πιθανών επιθέσεων για τους εγκληματίες του κυβερνοχώρου. Πολλές συσκευές IoT έχουν περιορισμένη επεξεργαστική ισχύ και μνήμη, γεγονός που τις καθιστά επιρρεπείς σε επιθέσεις που αξιοποιούν τις εγγενείς αδυναμίες τους. Μια παραβιασμένη συσκευή σε ένα δίκτυο θα μπορούσε να οδηγήσει σε φαινόμενο ντόμινο, επηρεάζοντας ολόκληρο το σύστημα και δυνητικά προκαλώντας εκτεταμένες διακοπές. Η αξιοπιστία των κρίσιμων υποδομών, όπως τα δίκτυα ηλεκτρικής ενέργειας και τα συστήματα μεταφορών, εξαρτάται όλο και περισσότερο από τις τεχνολογίες IoT. Ενώ το IoT ενισχύει την αποτελεσματικότητα και τις δυνατότητες παρακολούθησης, εισάγει επίσης ένα νέο επίπεδο ευπάθειας. Μια στοχευμένη επίθεση σε υποδομές με δυνατότητα IoT θα μπορούσε να έχει σοβαρές συνέπειες, διαταράσσοντας βασικές υπηρεσίες και θέτοντας κινδύνους για τη δημόσια ασφάλεια.

Η έλλειψη τυποποιημένων πρωτοκόλλων και μέτρων ασφαλείας σε διάφορες συσκευές IoT αποτελεί σημαντική πρόκληση. Καθώς διαφορετικοί κατασκευαστές αναπτύσσουν συσκευές με διαφορετικά χαρακτηριστικά ασφαλείας, η ενσωμάτωσή τους σε ένα συνεκτικό και ασφαλές δίκτυο γίνεται πολύπλοκη. Η τυποποίηση είναι ζωτικής σημασίας για τη διασφάλιση ότι όλες οι συσκευές IoT συμμορφώνονται με ένα σύνολο πρωτοκόλλων ασφαλείας, μειώνοντας τον συνολικό κίνδυνο τρωτών σημείων (Russell & Van Duren, 2016).

Ο τεράστιος όγκος δεδομένων που παράγονται από συσκευές IoT μπορεί να είναι συντριπτικός. Καθώς περισσότερες συσκευές έρχονται στο διαδίκτυο, η πρόκληση δεν έγκειται μόνο στη διαχείριση και ανάλυση αυτού του τεράστιου όγκου δεδομένων, αλλά και στη διασφάλιση της συνάφειας και της ακρίβειάς τους. Η αναποτελεσματική διαχείριση δεδομένων θα μπορούσε να οδηγήσει στη λήψη αποφάσεων με βάση λανθασμένες ή ξεπερασμένες πληροφορίες, με δυνητικά αρνητικά αποτελέσματα (Aufner, 2020).

Ο περιβαλλοντικός αντίκτυπος του IoT είναι μια πτυχή που συχνά παραβλέπεται. Η κατασκευή, η χρήση και η απόρριψη συσκευών IoT συμβάλλουν στα ηλεκτρονικά απόβλητα και στην υποβάθμιση του περιβάλλοντος. Ο γρήγορος ρυθμός των τεχνολογικών εξελίξεων οδηγεί σε συντόμευση του κύκλου ζωής των συσκευών IoT, καθώς νεότερα, πιο προηγμένα μοντέλα εισέρχονται στην αγορά, οι παλαιότερες συσκευές καθίστανται απαρχαιωμένες, συμβάλλοντας στη συγκέντρωση ηλεκτρονικών αποβλήτων που διαχειρίζονται εξαιρετικά δύσκολα. Η διασφάλιση υπεύθυνων και βιώσιμων πρακτικών στην παραγωγή και απόρριψη συσκευών IoT είναι ζωτικής σημασίας για τον μετριασμό του περιβαλλοντικού αποτυπώματος που σχετίζεται με την ευρεία χρήση τους.

Σύμφωνα με την Παγκόσμια Παρακολούθηση Ηλεκτρονικών Αποβλήτων 2017 το The Global E-waste Monitor - 2017, μια έκθεση που δημοσιεύτηκε από το Πανεπιστήμιο των Ηνωμένων Εθνών, τη Διεθνή Ένωση Τηλεπικοινωνιών και τη Διεθνή Ένωση Στερεών Αποβλήτων το 2016 δημιουργήθηκαν 49,3 εκατομμύρια τόνοι ηλεκτρονικών αποβλήτων. Αυτό είναι το ισοδύναμο βάρους σχεδόν 25 εκατομμυρίων επιβατικών αυτοκινήτων. (Balde et al., 2017)

Πολλές συσκευές IoT απαιτούν συνεχή σύνδεση στο διαδίκτυο και καταναλώνουν ενέργεια ακόμη και σε κατάσταση αναμονής. Ο αθροιστικός αντίκτυπος της ευρείας υιοθέτησης του IoT στην κατανάλωση ενέργειας προκαλεί ανησυχία, ειδικά σε μια εποχή όπου η βιωσιμότητα αποτελεί παγκόσμια προτεραιότητα.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το Διαδίκτυο των Πραγμάτων (IoT) έχει εξελιχθεί γρήγορα, ενσωματώνοντας χιλιάδες τύπους διαφορετικών συσκευών, από απλούς αισθητήρες ενημέρωσης μέχρι πολύπλοκες συσκευές ελέγχου κρίσιμων υποδομών και ενεργειών στην καθημερινή ζωή. Η εξέλιξη αυτή έχει μεταμορφώσει τις ανθρώπινες δραστηριότητες δημιουργώντας μια άνευ προηγουμένου συνδεσιμότητα με τα πάντα σε σημείο που να έχει προταθεί ο ορισμός διαδίκτυο των πάντων - internet of everything. Ωστόσο, αυτή η αύξηση της συνδεσιμότητας προκαλεί μια εύλογη ανησυχία, την ευπάθεια των συσκευών IoT σε απειλές ασφαλείας.

Ο κύριος τομέας της ασφάλειας του IoT βρίσκεται στην υποδομή του υλικού. Σε αντίθεση με τα παραδοσιακά συστήματα υπολογιστών, οι συσκευές IoT λειτουργούν συχνά σε περιβάλλοντα περιορισμένα σε πόρους, όπου η υπολογιστική ισχύς και η μνήμη περιορίζονται λόγω των φυσικών αδυναμιών και μεγεθών αλλά και λόγου κόστους. Ένας αισθητήρας θερμοκρασίας που μπορεί να ελέγχει την έναρξη του κλιματιστικού σε ένα έξυπνο σπίτι, η του φούρνου μαγειρέματος, αλλά ακόμη και μια σειρά μηχανών σε ένα εργοστάσιο, είναι μια απλή συσκευή, φθηνή σε κόστος και μικρή σε μέγεθος. Από την άλλη πλευρά είναι όμως συνδεμένη στο διαδίκτυο και αυτόματα αποτελεί «πόρτα» εισόδου για πρόσβαση στο σύνθετο περιβάλλον του δικτύου και των κεντρικών συστημάτων.

Αυτός ο περιορισμός των συσκευών IoT απαιτεί επανεκτίμηση των παραδοσιακών παραδειγμάτων ασφάλειας, καθώς οι περιορισμοί των πόρων μπορούν να εμποδίσουν την ανάπτυξη ισχυρών μέτρων ασφαλείας. Για το λόγο αυτό οι μηχανισμοί ασφαλείας υλικού πρέπει να σχεδιαστούν ώστε να λειτουργούν αποτελεσματικά εντός αυτών των περιορισμών, δίνοντας έμφαση στην ανάγκη για ελαφρούς κρυπτογραφικούς αλγόριθμους και ενεργειακά αποδοτικά πρωτόκολλα ασφαλείας.

Ένας άλλος σημαντικός τομέας είναι η κατανόηση της απειλής, η οποία είναι ζωτικής σημασίας για την ενίσχυση των συσκευών IoT. Οι ευπάθειες του υλικού μπορούν να εκδηλωθούν με διάφορες μορφές, από παραδοσιακές επιθέσεις πλευρικού καναλιού μέχρι πιο εξελιγμένες απειλές, όπως Trojans υλικού και επιθέσεις εφοδιαστικής

αλυσίδας. Η διασυνδεδεμένη φύση του IoT επιδεινώνει αυτούς τους κινδύνους, καθώς ένας συμβιβασμός σε μία συσκευή μπορεί δυνητικά να περάσει σε ένα ολόκληρο δίκτυο. Ο μετριασμός αυτών των απειλών απαιτεί μια ολιστική προσέγγιση, που συνδυάζει άμυνες σε επίπεδο υλικού με μέτρα ασφαλείας σε επίπεδο λογισμικού και δικτύου.

Η συνεχής παρακολούθηση του υλικού και οι ενημερώσεις του λογισμικού είναι επιτακτική ανάγκη για την αντιμετώπιση των αναδυόμενων απειλών. Η ανάπτυξη τεχνικών κρυπτογράφησης, προσαρμοσμένες στους περιορισμούς των συσκευών που αναφέρθηκαν, εγγυάται την μεγαλύτερη δυνατή ασφάλεια. Αν και τα κρυπτογραφικά πρωτόκολλα είναι το θεμέλιο της ασφάλειας δεδομένων στις συσκευές IoT, διασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα των δεδομένων που μεταδίδονται και υποβάλλονται σε επεξεργασία από συσκευές IoT, οι περιορισμοί που εντοπίζονται στις συσκευές IoT εμφανίζονται και στην κρυπτογράφηση. Το IoT απαιτεί κρυπτογραφικούς αλγόριθμους, οι οποίοι προσαρμοσμένοι στα περιορισμένα περιβάλλοντα που δουλεύουν οι συσκευές IoT, πρέπει να επιτυγχάνουν μια ισορροπία μεταξύ ασφάλειας και αποδοτικότητας πόρων.

Ο ανθρώπινος παράγοντας παραμένει μια σημαντική μεταβλητή στην εξίσωση ασφάλειας. Οι χρήστες, είτε ιδιώτες, είτε επιχειρήσεις, είτε δημόσιοι οργανισμοί, πρέπει να γνωρίζουν τις επιπτώσεις στην ασφάλεια που σχετίζονται με τις συσκευές IoT. Οι κατασκευαστές, με τη σειρά τους, θα πρέπει να δώσουν προτεραιότητα στις φιλικές προς τον χρήστη διεπαφές που διευκολύνουν την ασφαλή διαχείριση συσκευών, ελαχιστοποιώντας την πιθανότητα εσφαλμένων διαμορφώσεων που θα μπορούσαν να δημιουργήσουν ευπάθειες και δυνατότητα επιθέσεων.

Η υιοθέτηση αναδυόμενων τεχνολογιών, όπως η τεχνητή νοημοσύνη και η τεχνολογία Blockchain έχουν τη δυνατότητα να ενισχύσουν τις δυνατότητες ανίχνευσης ανωμαλιών και μετριασμού των απειλών. Το νέο όμως αυτό περιβάλλον, ειδικά με την υιοθέτηση όλο και πιο προηγμένων τεχνικών ελέγχουν από την τεχνητή νοημοσύνη, αυξάνει επίσης τους κινδύνους αλλά και την ανησυχία για την ασφάλεια των συσκευών IoT. Μέχρι πρόσφατα μια συσκευή IoT μπορούσε να λειτουργεί αυτόνομα, να ολοκλήρωνε επαναλαμβανόμενες, κουραστικές ή επικίνδυνες εργασίες για τον

άνθρωπο, δημιουργώντας κυρίως ηθικά ζητήματα σε επίπεδο απώλειας θέσεων εργασίας, ή στην πρόκληση ατυχημάτων από την μη σωστή λειτουργία της.

Το τελευταίο διάστημα με την ολοένα αυξανόμενη χρήση προγραμμάτων τεχνητής νοημοσύνης και δυνατότητας μηχανικής εκμάθησης από τις συσκευές, έχουν δημιουργηθεί σενάρια όπου συσκευές IoT θα μπορούν να αποφασίζουν για κάποιες ενέργειες, χωρίς την επέμβαση ανθρώπου, στηριζόμενες στη δική τους κρίση με βάση τη τεχνητή νοημοσύνη τους.

Είναι χαρακτηριστικό ότι ένα αυτόνομα όχημα στις ΗΠΑ είναι υπεύθυνο για το πρώτο θάνατο ανθρώπου από αυτόνομα οχήματα, καθώς οι αισθητήρες αποφυγής σύγκρουσης παρέβλεψαν ένα στοιχείο. Μπροστά στο αυτοκίνητο υπήρχε ένα φορτηγό, με άσπρη καρότσα, στοιχείο που ποτέ δεν ενσωματώθηκε στο πρόγραμμα αναγνώρισης του αισθητήρα. Ο αισθητήρας «είδε» απλά ένα άσπρο «φόντο» που δεν θεώρησε απειλή και δεν ενεργοποίησε το σύστημα φρένων, με αποτέλεσμα να συγκρουστεί το αυτοκίνητο και να επέλθει ο θανάσιμος τραυματισμός του οδηγού, που προφανώς αν είχε αυτός τον έλεγχο του αυτοκινήτου θα το είχε αποφύγει. Το παράδειγμα μπορεί να φαίνεται απλοϊκό, αλλά δείχνει ταυτόχρονα την πολυπλοκότητα του νέου διασυνδεμένου κόσμου που θα στηρίζεται ολοένα και περισσότερο στη τεχνητή νοημοσύνη και στα αυτόνομα συστήματα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Albino, V., Berardi, U., & Dangelico, R. M. (2015), Smart cities: Definitions, dimensions, performance, and initiatives, *Journal of Urban Technology, 22:1, pp.3-21.*
- Alaali, A., & Elmedany, W. (2022). Hardware Trojan and Countermeasures for Internet of Things. *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*
- Anuradha, J. & Tripathy, B.K, (2018). *Internet of things. IoT, technologies, applications, challenges and solutions.* U.S.A.: CRC Press, Taylor & Francis.
- Anuradha, J. & Tripathy, B.K, (2018). *Internet of things. IoT, technologies, applications, challenges and solutions.* U.S.A.: CRC Press, Taylor & Francis.
- Ashton, K. (2009). That «Internet of Things» Thing. RFiD Journal. https://www.rfidjournal.com/that-internet-of-things-thing
- Aufner, P. (2020). The IoT security gap: a look down into the valley between threat models and their implementation. *International Journal of Information Security 19, 3–14 (2020).*
- Augusto, J. (2021). *Handbook of Smart Cities.* UK: Springer (2021).
- Bart, C., He, F., Tucci, V., & Christopher, L. (2022). How the Internet of Things reshapes the organization of innovation and entrepreneurship. *Technovation 118(2022)102644.*
- Balde, C. P., Forti, V., Gray, V., Kuehr, R., & Stegmann, P. (2017). *The Global E-waste Monitor 2017 Quantities, Flows, and Resources.* Germany, United Nations University, IAS - SCYCLE.
- Beg, M., Yusri, I., Jamlos, M., Azmi, W., Badrulhisam, N., & Awad, O. (2022). Potential and Limitation of Internet of Things (IOT) Application in the Automotive Industry: An Overview. *International journal of automotive and mechanical engineering. VOL. 19, ISSUE 3, 9939 – 9949*
- Beranger, J., & Rizoulieres, R. (2021). *The Digital Revolution in Health. Innovating and Acting for Sustaining Transformations in the Health System.*

USA: Wiley & Sons, Inc.

- Biswas, A., & Wang, C. (2023). Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain. *Sensors 2023, 23(4).*
- Bolic M., Simplot-Ryl D., & Stojmenovic I. (2010). *RFID Systems. Research Trends and Challenges.* U.K.: John Wiley & Sons.
- Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial Internet of things (IIoT). An analysis framework. *Computers in Industry Volume 101, October 2018, Pages 1-12*
- Carvalho, M. (2023). *Building Smart Home Automation Solutions with Home Assistant. Configure, integrate, and manage hardware and software systems.* U.K.: Packt Publishing.
- Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2019). Toward the automation of threat modeling and risk assessment in IoT systems. Internet of Things,
- Chantzis, F., Stais, I., Calderon, P., Deirmentzoglou, E., Woods, B. (2021). *Practical IoT Hacking. The Definitive Guide to Attacking the Internet of Things.* USA: No Starch Press.
- Chen, M., & Chen, S. (2016). *RFID Technologies for Internet of Things.* Switzerland: Springer International Publishing AG.
- Cheruvu, S., Kumar, A., Smith, N., & Wheele, D. (2020). *Demystifying Internet of Things Security Successful IoT Device/Edge and Platform Security Deployment.* USA: Open Access
- Cisco, (2014). *The Internet of Things Reference Model.* USA: Cisco Systems Inc.
- DeNardis, L. (2020). *The Internet in Everything. Freedom and Security in a World with No off Switch.* USA: Yale University Press.
- Ghosh, R., Basu, D., Banerjiee, A., Ghosh, U. (2022). *Intelligent IoT for Automotive Industry 4.0: Challenges, Opportunities, and Future Trends.* Chapter on Intelligent Internet of Things for Healthcare and Industry. Internet of Things. Switzerland: Springer Nature.

- Halegoua, G. (2020). *Smart Cities.* USA: The MIT Press
- Hemanth, J. (2019). *Telemedicine Technologies. Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare.* USA: Academic Press.
- Hu, F. (2016). *Security and Privacy in Internet of Things (IoTs). Models, Algorithms, and Implementations.* U.S.A.: CRC Press, Taylor & Francis Group
- Jiang, W., Li, E., Zhou, W., Yang, Y. & Luo, T. (2023). IoT Access Control Model Based on Blockchain and Trusted Execution Environment. *Processes 2023, 11(3), 723*
- Khaled, M. (2019). *The Era of Internet of Things. Towards a Smart World.* Switzerland: Springer.
- Kranz, M. (2016). *Building the Internet of Things. Implement New Business Models, Disrupt Competitors. Transform Your Industry*. U.S.A.: John Wiley & Sons
- Kranz, M. (2016). *Building the Internet of Things. Implement New Business Models, Disrupt Competitors. Transform Your Industry*. U.S.A.: John Wiley & Sons
- Kraus, S., Schiavone, F., Pluzhnikova, A., & Invernizzi, C. (2021). Digital transformation in healthcare: analyzing the current state-of-research. *Journal of Business Research (123) (2021), pp. 557-567*
- Kyriakidis, M., Happee, R., & De Winter, JC. (2015). Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. *Transportation Research Part F: Traffic Psychology and Behaviour Volume 32, July 2015, Pages 127-140*
- Li, S., & Xu, L. (2017). *Securing the Internet of Things.* U.S.A.: Syngress
- Lipovyanov, P. (2019). Blockchain for Business. UK: Packt Publishing.
- Mahmood, Z. (2019). *The Internet of Things in the Industrial Sector. Security and Device Connectivity, Smart Environments, and Industry 4.0.* Switzerland: Springer Nature AG

- Mesko, B. (2018). Health IT and digital health: the future of health technology is diverse. *Journal of Clinical and Translational Research 2018; 3(Suppl. 3):431e4.*
- Misra, S., Mukherjee, A., & Roy, A. (2021). *Introduction to IoT.* U.K.: Cambridge University Press.
- Mocnej, J., Pekar, A., Seah, W., & Zolotova, I. (2018). Network Traffic Characteristics of the IoT Application Use Cases. *New Zealand: School of Engineering and Computer Science, Victoria University of Wellington, 2018.*
- Mohanta, B., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things Volume 11, September 2020, 100227.*
- Mukherjee, A., Roy, C., & Misra, S. (2021). *Introduction to Industrial Internet of Things and Industry 4. 0.* USA: CRC Press
- Nayyar, A., & Kumar, A. (2020). *A Roadmap to Industry 4.0. Smart Production, Sharp Business and Sustainable Development.* Switzerland: Springer International Publishing.
- Nilanjan, D., Hassanien, A., Bhatt, C., Ashour, A., & Satapathy, S., (2018). *Internet of Things and Big Data Analytics toward Next-Generation Intelligence.* Switzerland: Springer.
- Pani, S., Patra, P., Ferrari, G., Kraleva, R., & Wang, X. (2022). *The Internet of Medical Things. Enabling technologies and emerging applications.* USA: The Institution of Engineering and Technology.
- Parsons, E., Panaousis, E., Loukas, G., & Sakellari, G. (2023). A Survey on Cyber Risk Management for the Internet of Things. Journals Applied Sciences Volume 13 Issue 15.
- Patel, C. & Nishant, D. (2019). *Internet of Things Security. Challenges, Advances, and Analytics.* USA: CRC Press.
- Patel, C. & Nishant, D. (2019). *Internet of Things Security. Challenges, Advances, and Analytics.* USA: CRC Press.

- Powell, A. (2021). *Undoing Optimization. Civic Action in Smart Cities.* USA: Yale University Press.
- Russell, B., & Van Duren, D. (2016). *Practical internet of things security.* UK: Published by Packt Publishing Ltd.
- Salih, K., Rashid, T., Radovanovic, D., & Bacanin, N. (2022). A Comprehensive Survey on the Internet of Things with the Industrial Marketplace. Journals Sensors Volume 22 Issue 3.
- Sharma, S., Nalin, D., Jayakody, K., Chatzinotas, S., & Anpalagan, A. (2021). *Communication Technologies for Networked Smart Cities.* UK: Institution of Engineering and Technology.
- Shostack, A. (2014). *Threat modeling designing for security.* USA: J. Wiley & Sons.
- Sidhu, S., Mohd, B., & Hayajneh, T. (2019). Hardware Security in IoT Devices with Emphasis on Hardware Trojans. Journal of Sensor and Actuator Networks 2019, 8(3), 42.
- Song, H. (2022). *Internet of Everything. Key Technologies, Practical Applications and Security of IoT.* Singapore: World Scientific Publishing.
- Soroceanu, T., Buchmann, N., & Margraf, M. (2023). On Multiple Encryption for Public-Key Cryptography. *Cryptography 2023, 7(4), 49;*
- Stergiou, C., Koidou, M., & Psannis, K. (2023). IoT-Based Big Data Secure Transmission and Management over Cloud System: A Healthcare Digital Twin Scenario. *Journals Applied Sciences Volume 13 Issue 16.*
- Treiblmaier, H., & Beck, R. (2019). *Business Transformation through Blockchain. Switzerland*: Palgrave Macmillan (2019)
- Wang, J., Lim, M., Wang, C., & Tseng, M. (2021). The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering Volume 155, May 2021, 107174.*
- Παρασκευάς, Μ., Ασημακόπουλος, Γ., & Τριανταφύλλου, Β. (2015). *Κοινωνία της Πληροφορίας.* Αθήνα: Σύνδεσμος Ελληνικών ακαδημαϊκών βιβλιοθηκών.

ΔΙΑΔΙΚΤΥΟ

- Η αναγνώριση ραδιοσυχνοτήτων - Radio Frequency Identification (RFID) είναι μια τεχνολογία που χρησιμοποιεί ραδιοκύματα για την παθητική αναγνώριση ενός αντικειμένου με ετικέτα. Χρησιμοποιείται σε πολλές εμπορικές και βιομηχανικές εφαρμογές, από την παρακολούθηση αντικειμένων κατά μήκος μιας αλυσίδας εφοδιασμού έως την παρακολούθηση των αντικειμένων σε οποιαδήποτε ανθρώπινη δραστηριότητα. https://www.investopedia.com/terms/r/radio-frequency-identification-rfid.asp (Ανάκτηση 25.7.2023).
- https://www.riot-os.org/ RIOT OS, (Ανάκτηση 25.7.2023).
- https://www.statista.com/outlook/tmo/internet-of-things/worldwide Internet of Things - Worldwide. (Ανάκτηση 26.7.2023).
- https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ Number of connected Internet of Things (IoT) devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030, (Ανάκτηση 26.7.2023).
- Το Industry 4.0 φέρνει επανάσταση στον τρόπο με τον οποίο οι εταιρείες κατασκευάζουν, βελτιώνουν και διανέμουν τα προϊόντα τους. Οι κατασκευαστές ενσωματώνουν νέες τεχνολογίες, συμπεριλαμβανομένου του Διαδικτύου των πραγμάτων (IoT), του υπολογιστικού νέφους και της ανάλυσης, καθώς και της τεχνητής νοημοσύνης και της μηχανικής μάθησης στις εγκαταστάσεις παραγωγής τους και σε όλες τις δραστηριότητές τους. https://www.ibm.com/topics/industry-4-0 (Ανάκτηση 26.7.2023).
- https://www.forbes.com/sites/forbestechcouncil/2019/05/02/the-iot-yesterdays-predictions-vs-todays-reality/?sh=4d0eed11512b The IoT: Yesterday's Predictions Vs. Today's Reality, (Ανάκτηση 29.7.2023).
- https://www.marketsandmarkets.com/Market-Reports/iot-smart-cities-market-215714954.html IoT in Smart Cities, (Ανάκτηση 10.8.2023).
- Ο σύνθετος ετήσιος ρυθμός ανάπτυξης (CAGR) είναι ο ρυθμός απόδοσης (RoR) που θα απαιτούνταν για να αυξηθεί μια επένδυση από το αρχικό της υπόλοιπο στο τελικό υπόλοιπό της, υποθέτοντας ότι τα κέρδη επανεπενδύθηκαν στο τέλος κάθε περιόδου της διάρκειας ζωής της επένδυσης. (Ανάκτηση 10.8.2023, από https://www.investopedia.com/terms/c/cagr.asp)
- https://www.globenewswire.com/news-release/2023/07/17/2705500/0/en/Smart-Home-Market-Size-to-Surpass-USD-338-28-billion-by-2030-exhibiting-a-CAGR-of-20-1.html Smart Home Market Size, (Ανάκτηση 14.8.2023).
- https://www.fortunebusinessinsights.com/internet-of-things-iot-in-healthcare-

market-102188 Internet of things (IoT) in Healthcare Market Size, (Ανάκτηση 17.8.2023).

- Το ZigBee είναι μια ασύρματη τεχνολογία βασισμένη σε πρότυπα που αναπτύχθηκε για να επιτρέπει χαμηλού κόστους, χαμηλής κατανάλωσης ασύρματα δίκτυα μηχανής-προς-μηχανή (M2M) και internet of things (IoT). (Ανάκτηση 20.8.2023 από https://www.techtarget.com/iotagenda/definition/ZigBee)
- LoRaWAN είναι ένα «πρωτόκολλο δικτύωσης χαμηλής ισχύος, ευρείας περιοχής (LPWA) που έχει σχεδιαστεί για να συνδέει ασύρματα «πράγματα» που λειτουργούν με μπαταρία στο Διαδίκτυο σε περιφερειακά, εθνικά ή παγκόσμια δίκτυα καλύπτοντας βασικές απαιτήσεις του IoT, όπως δι-υπηρεσίες κατευθυντικής επικοινωνίας, ασφάλειας από άκρο σε άκρο, κινητικότητας και εντοπισμού. (Ανάκτηση 20.8.2023 από https://docs.aws.amazon.com/iot/latest/developerguide/connect-iot-lorawan-what-is-lorawan.html)
- backdoor (computing). Η επίθεση με κερκόπορτα είναι ένας τρόπος πρόσβασης σε ένα σύστημα υπολογιστή ή σε κρυπτογραφημένα δεδομένα που παρακάμπτουν τους συνήθεις μηχανισμούς ασφαλείας του συστήματος. Ένας προγραμματιστής μπορεί να δημιουργήσει μια κερκόπορτα ώστε να είναι δυνατή η πρόσβαση σε μια εφαρμογή, λειτουργικό σύστημα (OS) ή δεδομένα για αντιμετώπιση προβλημάτων ή άλλους σκοπούς. Οι επιτιθέμενοι χρησιμοποιούν backdoors που εγκαθιστούν οι προγραμματιστές λογισμικού και εγκαθιστούν επίσης οι ίδιοι backdoors ως μέρος μιας εκμετάλλευσης υπολογιστή. (Ανάκτηση 30.8.2023 από https://www.techtarget.com/searchsecurity/definition/back-door)
- https://www.encryptionconsulting.com/education-center/what-is-code-signing/ what is Code Signing? How does Code Signing work? (Ανάκτηση 10.9.2023).
- https://www.rambus.com/blogs/side-channel-attacks/ Side-channel attacks explained: everything you need to know, (Ανάκτηση 5.10.2023)
- Η προδιαγραφή TEMPEST (που ορίστηκε από την Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ) αναφέρεται στην ευαισθησία των συσκευών υπολογιστών και τηλεπικοινωνιών σε κλοπή δεδομένων. Ορισμένος ηλεκτρονικός εξοπλισμός εκπέμπει ηλεκτρομαγνητική ακτινοβολία ή διακυβευτικές εκπομπές (CE) με τρόπο που μπορεί να χρησιμοποιηθεί για την ανακατασκευή κατανοητών δεδομένων. (Ανάκτηση 5.10.2023 από https://www.astrodynetdi.com/blog/tempest-emi-filters)