ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ- ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ- ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΠΜΣ «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

ΖΗΤΗΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (INTERNET OF THINGS)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΗΣ ΙΩΑΝΝΙΔΟΥ ΚΑΛΛΙΟΠΗΣ (mli18004)

ΘΕΣΣΑΛΟΝΙΚΗ, ΙΟΥΛΙΟΣ 2020

ΖΗΤΗΜΑΤΑ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

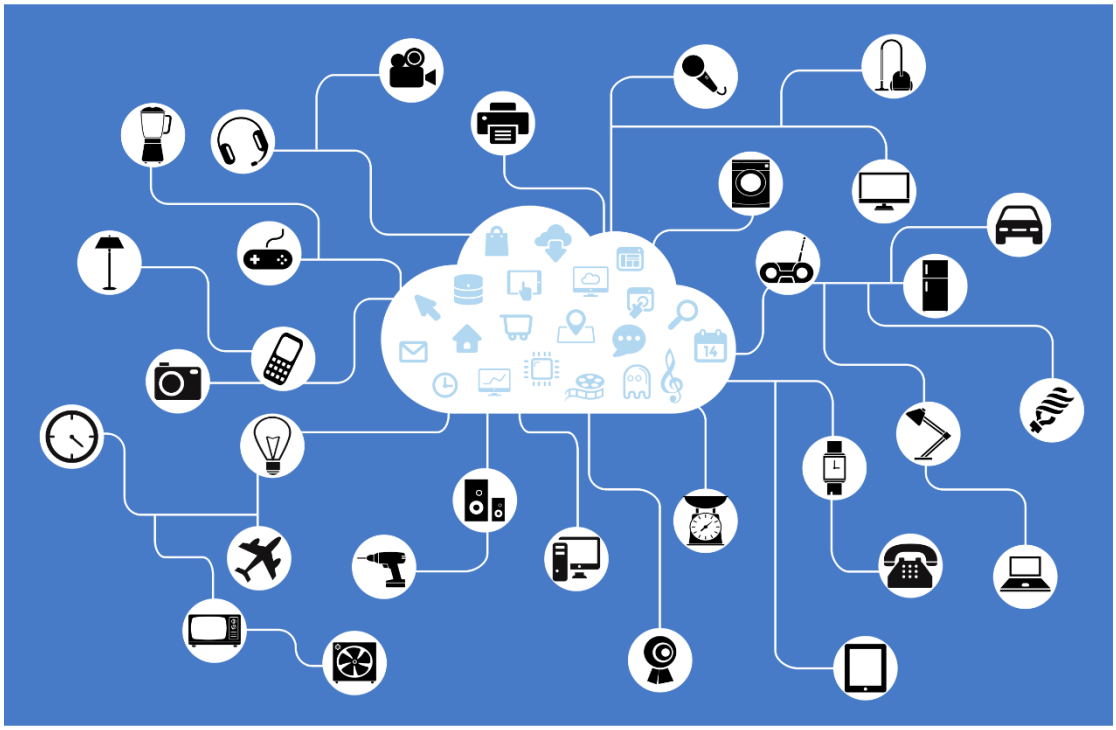
(INTERNET OF THINGS)

ΚΑΛΛΙΟΠΗ ΙΩΑΝΝΙΔΟΥ

ΠΡΟΠΤΥΧΙΑΚΕΣ ΣΠΟΥΔΕΣ

ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ Α.Π.Θ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΠΡΟΣ ΕΚΠΛΗΡΩΣΗ ΤΟΥ ΤΙΤΛΟΥ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»



ΕΠΙΒΛΕΠΩΝ: ΠΑΠΑΔΗΜΗΤΡΙΟΥ ΠΑΝΑΓΙΩΤΗΣ

Περιεχόμενα

Κατάλογος εικόνων

Κατάλογος πινάκων

Περίληψη

Η παρούσα εργασία πραγματεύεται ζητήματα ιδιωτικότητας στο διαδίκτυο των πραγμάτων (IoT: Internet of things). Αρχικά γίνεται αναφορά στον τρόπο με το οποίο συνδέεται το IoT με τις έξυπνες πόλεις (smart cities), την ηλεκτρονική υγεία (e-health) και το έξυπνο σπίτι (smart home).

Στη συνέχεια παρατίθενται τα ζητήματα ιδιωτικότητας που προκύπτουν στις έξυπνες πόλεις σε σχέση με την χρήση του IoT. Στο πλαίσιο αυτό γίνεται λόγος για εμπιστευτικότητα δεδομένων, διαχείριση εμπιστοσύνης και βασική διαχείριση προσωπικών δεδομένων. Επίσης μελετάται η ασφάλεια και το απόρρητο στο ιατρικό διαδίκτυο των πραγμάτων. Πιο αναλυτικά, γίνεται λόγος για απαιτήσεις ασφάλειας απορρήτου, για υφιστάμενες λύσεις και για κρυπτογράφηση δεδομένων.

Έπειτα αναλύονται ζητήματα ιδιωτικότητας που προκύπτουν στο έξυπνο σπίτι. Γίνεται αναφορά στους στόχους ασφάλειας στο έξυπνο σπίτι, στις επιθέσεις ασφάλειας και πραγματοποιείται αξιολόγηση των επιπτώσεων από τις επιθέσεις αυτές. Τέλος, παρατίθενται τα συμπεράσματα που εξήχθησαν από την παρούσα διπλωματική εργασία.

Abstract

This dissertation studies privacy aspects related to the Internet of Things (IoT). Initially, we discuss applications of IoT in smart cities, e-health, and smart homes. We particularly focus on the privacy issues that arise in smart cities in relation to the use of IoT. In this context, we investigate data confidentiality, trust management and basic personal data management. We also inspect aspects related to security and confidentiality, and in more particular, security requirements and existing solutions for data encryption. In addition, we study privacy aspects pertaining to smart home environments, with emphasis on attempts to gain unauthorized access to data and their potential impact on privacy. Finally, we highlight the conclusion drawn from this study.

1. Εισαγωγή

Το Διαδίκτυο των πραγμάτων (IoT) είναι ένα σύστημα αλληλένδετων υπολογιστικών συσκευών, μηχανικών και ψηφιακών μηχανών εφοδιασμένων με μοναδικά αναγνωριστικά στοιχεία (UID: unique identifiers) και τη δυνατότητα μεταφοράς δεδομένων μέσω δικτύου χωρίς να απαιτείται αλληλεπίδραση μεταξύ ανθρώπων[1].

Ο ορισμός του Διαδικτύου των πραγμάτων έχει εξελιχθεί λόγω της σύγκλισης πολλαπλών τεχνολογιών, αναλύσεων σε πραγματικό χρόνο, μηχανικής μάθησης , αισθητήρων εμπορευμάτων και ενσωματωμένων συστημάτων. Οι παραδοσιακοί τομείς των ενσωματωμένων συστημάτων, των ασύρματων δικτύων αισθητήρων, των συστημάτων ελέγχου και της αυτοματοποίησης (συμπεριλαμβανομένου του αυτοματισμού κατοικιών και των κτιρίων) συμβάλλουν στην καθιέρωση του Διαδικτύου. Στην αγορά των καταναλωτών, η τεχνολογία IoT είναι συνώνυμη με τα προϊόντα που αφορούν την έννοια του "έξυπνου σπιτιού", καλύπτοντας συσκευές (όπως φωτιστικά, θερμοστάτες , συστήματα ασφαλείας και κάμερες, και άλλες οικιακές συσκευές) που συνδέονται με το εν λόγω οικοσύστημα με συσκευές όπως τα smartphones και τα έξυπνα ηχεία .

Το Iot αποτελεί ένα πολυσύνθετο οικοσύστημα που επιτρέπει τη διασύνδεση συσκευών διαφορετικών κατασκευαστών, διανομέων ή παραγωγών λογισμικού. Αυτό δημιουργεί δυσκολίες στην απόδοση ευθυνών σε περιπτώσεις μη συμμόρφωσης με τη νομοθεσία ή σε περίπτωση υλικών ζημιών ή άλλων ζημιών που προκαλούνται σε τρίτους ή σε συστήματα λόγω ελαττωματικών προϊόντων ή λόγω της στρεβλής χρήσης των προϊόντων από τρίτους μέσω του διαδικτύου. Υπάρχει επίσης το ενδεχόμενο πολλοί από τους επαγγελματίες που συμμετέχουν στην παγκόσμια αλυσίδα αξίας του προϊόντος να μην διαθέτουν επαρκείς γνώσεις και εμπειρία σε θέματα ασφάλειας ή προστασίας δεδομένων όσον αφορά τις δικτυωμένες συσκευές. Για τον λόγο αυτόν απαιτείται μια νέα προσέγγιση όσον αφορά τις ευθύνες, με στόχο να διασφαλιστεί ότι τόσο οι καταναλωτές όσο και οι επιχειρήσεις που υιοθετούν εφαρμογές του Iot προστατεύονται σε περιπτώσεις που προϊόντα με

ενδεδειγμένες ρυθμίσεις μπορεί να αποδειχθούν ελαττωματικά ή μη ασφαλή λόγω συμβάντων ψηφιακής ασφάλειας ή λόγω μη εξουσιοδοτημένης αθέμιτης χρήσης (π.χ. από hackers).Το περιβάλλον αυτό πρέπει να δίνει τη δυνατότητα για πρόβλεψη, πρόληψη και προστασία από εκείνες τις αυτοματοποιημένες αποφάσεις που μπορεί παραβιάζουν τις ηθικές αξίες και τα παγκοσμίως αναγνωρισμένα ανθρώπινα δικαιώματα.

Οι καταναλωτές έχουν ενισχύσει την ικανότητά τους να ασκούν έλεγχο επί των προσωπικών τους δεδομένων και των ιδιωτικών τους προτιμήσεων βάσει του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ).Ο χρήστης μιας συσκευής πρέπει να ελέγχει τον τρόπο με τον οποίο γίνεται χρήση των δεδομένων που παράγει και το ποιος έχει τη δυνατότητα πρόσβασης σε αυτά, λαμβανομένου υπόψη ότι η ποικιλία των δεδομένων, καθώς και η συγκέντρωση και η σύνδεσή τους με άλλα δεδομένα, συνεπάγονται σοβαρό κίνδυνο για την ιδιωτικότητα στο οικοσύστημα του Iot.

Οι νομικές εγγυήσεις θα πρέπει να διασφαλίζουν την απόλυτη δυνατότητα των χρηστών να ασκούν τα δικαιώματα της ιδιωτικότητάς τους και της προστασίας των δεδομένων τους προσωπικού χαρακτήρα χωρίς περιορισμό, ώστε να αποφεύγονται ενδεχόμενες επιβλαβείς συνέπειες όπως οι διακρίσεις, οι επιθετικές πωλήσεις, η συρρίκνωση της ιδιωτικής σφαίρας ή οι παραβιάσεις της ασφάλειας. Από την άλλη πλευρά, οι καταναλωτές θα πρέπει να έχουν ενημέρωση σχετικά με την οικονομική αξία των δεδομένων τους και να διατηρούν το δικαίωμα να τα κοινοποιούν.

1.1. Στόχοι και συνεισφορά

Η παρούσα διπλωματική εργασία έχει ως στόχο να ερευνήσει ζητήματα ιδιωτικότητας στο IoT και πιο συγκεκριμένα ζητήματα που αφορούν την ιδιωτικότητα στις έξυπνες πόλεις, στο έξυπνο σπίτι και στο ιατρικό απόρρητο των ατόμων.

Στο πλαίσιο αυτό μελετήθηκε η σύγχρονη βιβλιογραφία που καλύπτει τα παραπάνω θεματικά πεδία. Οι μηχανές διαδικτυακής αναζήτησης που χρησιμοποιήθηκαν ήταν το Science direct και το google scholar.

Υπάρχουν πολλές σοβαρές ανησυχίες σχετικά με τους κινδύνους στην ανάπτυξη του Ίντερνετ, ιδίως στους τομείς της προστασίας της ιδιωτικής ζωής και της ασφάλειας, και κατά συνέπεια έχουν αρχίσει οι βιομηχανικές και κυβερνητικές ενέργειες για την αντιμετώπιση αυτών των ανησυχιών.

Μέσα από την ενδελεχή βιβλιογραφική ανασκόπηση τις σύγχρονης βιβλιογραφίας παρουσιάζονται ανάγλυφα τα ζητήματα της ιδιωτικότητας στο διαδίκτυο των πραγμάτων στους τομείς του έξυπνου σπιτιού, της έξυπνης πόλης και της έξυπνης υγείας. Επιπλέον, αναλύονται και οι υφιστάμενες προσπάθειες για την αντιμετώπιση των παραπάνω ζητημάτων.

1.2. Διάρθρωση της διπλωματικής

Στην εισαγωγή της εργασίας αναλύονται κάποιες βασικές έννοιες σχετικά με την ιδιωτικότητα στο διαδίκτυο των πραγμάτων. Στο δεύτερο κεφάλαιο γίνεται αναφορά στο διαδίκτυο των πραγμάτων και τις έξυπνες πόλεις. Πραγματοποιείται ιστορική αναδρομή, παρουσιάζονται εφαρμογές καταναλωτών και εφαρμογές έξυπνων πόλεων, αναλύονται οι τεχνολογίες διαδικτύου των πραγμάτων που χρησιμοποιούνται στις έξυπνες πόλεις και αναλύεται η αρχιτεκτονική του IoT. Έπειτα μελετάται το IoT ως μία τεχνολογία

εξουσιοδότησης για την έξυπνη πόλη και παρατίθενται εφαρμογές IoT για έξυπνες πόλεις. Πιο συγκεκριμένα γίνεται αναφορά σε διατήρηση κτιρίων, περιβαλλοντική παρακολούθηση, διαχείριση αποβλήτων, έξυπνος χώρος στάθμευσης, έξυπνη υγεία, συστήματα πλοήγησης, έξυπνο δίκτυο και αυτόνομη οδήγηση.

Στο τρίτο κεφάλαιο θίγονται ζητήματα ιδιωτικότητας στις έξυπνες πόλεις όπως εμπιστευτικότητα δεδομένων, ακεραιότητα και έλεγχος ταυτότητας.

Στο τέταρτο κεφάλαιο αναλύεται η ασφάλεια και το απόρρητο στο ιατρικό διαδίκτυο των πραγμάτων. Πιο αναλυτικά, γίνεται αναφορά στην απαίτηση ασφάλειας και απορρήτου, στην ακεραιότητα και ευχρηστία δεδομένων, στο απόρρητο πληροφοριών των ασθενών και μελετώνται οι υφιστάμενες λύσεις. Σε αυτές συμπεριλαμβάνονται η κρυπτογράφηση δεδομένων, ο έλεγχος πρόσβασης, ο αξιόπιστος έλεγχος τρίτων και η ανωνυμοποίηση δεδομένων. Γίνεται λόγος για την χρήση φορητών συσκευών και παρουσιάζονται συγκριτικά αποτελέσματα και ανάλυση. Μελετώνται επίσης και οι μελλοντικές προκλήσεις ασφάλειας και απορρήτου στο MIOT. Ως εκ τούτου γίνεται αναφορά στο μη ασφαλές δίκτυο, στα ελαφριά πρωτόκολλα για συσκευές και στην κοινή χρήση δεδομένων.

Στο πέμπτο κεφάλαιο, μελετώνται τα ζητήματα ιδιωτικότητας στο έξυπνο σπίτι. Γίνεται επισκόπηση του έξυπνου οικιακού συστήματος, των στόχων ασφάλειας στο σπίτι, την επίθεση ασφάλειας και την αξιολόγηση επιπτώσεων. Έπειτα παρουσιάζονται υφιστάμενες μελέτες για έξυπνη οικιακή ασφάλεια και παρατίθενται τα συμπεράσματα της εργασίας.

2. Διαδίκτυο των Πραγμάτων και Έξυπνες Πόλεις

Η έξυπνη πόλη έχει καταστεί ένας όρος ομπρέλα για πολλές τεχνολογίες, με στόχο τη βελτίωση της αποτελεσματικότητας των μελλοντικών πόλεων και την ποιότητα ζωής των κατοίκων τους, όχι μόνο με την εισαγωγή νέων εφαρμογών αλλά και με την αξιοποίηση των υφιστάμενων διαδικασιών. Έχει γίνει μόδα ο όρος έξυπνη πόλη και υπάρχουν πολιτικές προσπάθειες που αποσκοπούν στην ενθάρρυνση της ανάπτυξης έξυπνων πόλεων [1]. Υπάρχουν ορισμένοι τυπικοί ορισμοί του για την έξυπνη πόλη: Οι Caragliu et al. ορίζουν μια πόλη ως έξυπνη όταν οι επενδύσεις σε ανθρώπινο και κοινωνικό κεφάλαιο και οι παραδοσιακές (μεταφορικές) υποδομές και η σύγχρονη υποδομή επικοινωνίας (ΤΠΕ) συμβάλλουν στη βιώσιμη οικονομική ανάπτυξη και στην υψηλή ποιότητα ζωής, με σοφή διαχείριση των φυσικών πόρων μέσω συμμετοχικής διακυβέρνησης [2].

Ενώ άλλοι υποστηρίζουν ότι δεν μπορεί να υπάρξει ένας απόλυτος ορισμός, καθώς ο όρος έξυπνη πόλη δεν περιγράφει μια στατική έννοια αλλά μάλλον μια διαδικασία προς πιο ζωντανές και ανθεκτικές πόλεις [3], φαίνεται να υπάρχει συμφωνία ότι ορισμένες νέες τεχνολογίες και εφαρμογές ισοδυναμούν με τη δημιουργία πιο έξυπνων πόλεων [4]. Ο αριθμός των εφαρμογών έξυπνων πόλεων είναι μεγάλος, από υπηρεσίες έξυπνων καρτών για εύκολη επαλήθευση ταυτότητας και πληρωμή εν κινήσει, για έξυπνη διαχείριση πόρων νερού ή ηλεκτρικής ενέργειας, για εφαρμογές έξυπνης κινητικότητας που βελτιώνουν την κυκλοφοριακή αποτελεσματικότητα και μειώνουν τις εκπομπές CO_2. Η αποτελεσματικότητα αυτών των εφαρμογών και άλλων εφαρμογών έξυπνης πόλης εξαρτάται σε μεγάλο βαθμό από τη συλλογή δεδομένων, τη διασυνδεσιμότητα και την ευρύτατη διάδοση. Δυστυχώς, αυτός είναι και ο λόγος για τον οποίο οι έξυπνες πόλεις αποτελούν σοβαρή απειλή για την ιδιωτική ζωή των πολιτών: Η συλλογή και η συσχέτιση μεγάλων ποσοτήτων δεδομένων επιτρέπει τη δημιουργία λεπτομερών προφίλ που καλύπτουν κάθε πτυχή της ζωής.

Για παράδειγμα, μια υπηρεσία έξυπνων καρτών μπορεί να αποκαλύψει συμπεριφορές αγορών, ένα έξυπνο κτίριο μπορεί να αποκαλύψει ποιες

συσκευές χρησιμοποιούνται και μια έξυπνη εφαρμογή κινητικότητας μπορεί να διαρρεύσει ίχνη εντοπισμού των χρηστών της. Επιπλέον, η υπερκάλυψη ευαίσθητων δεδομένων χρήστη αποτελεί επιχειρηματική περίπτωση [5] και αποτελεί ήδη πρόβλημα στις εφαρμογές smartphone [6]. Το υψηλό επίπεδο διασυνδεσιμότητας προσθέτει περαιτέρω το πρόβλημα των προσωπικών δεδομένων. Ο συνδυασμός πολλαπλών πηγών δεδομένων από διαφορετικούς κατόχους δεδομένων, συσκευές και εφαρμογές μπορεί να βελτιώσει την ποιότητα και τη διαθεσιμότητα των υπηρεσιών, αλλά αυξάνει επίσης τον κίνδυνο διαρροών ευαίσθητων δεδομένων και παραβιάσεων της ιδιωτικής ζωής μέσω συσχέτισης.

Η διαπερατότητα των εφαρμογών και των αισθητήρων δεν αφήνει στον πολίτη άλλη επιλογή παρά να γίνει ψηφιακό μέρος των μελλοντικών πόλεων. Σε αντίθεση με τα κοινωνικά δίκτυα όπου οι χρήστες αποκαλύπτουν οικειοθελώς προσωπικές πληροφορίες, πολλές εφαρμογές έξυπνης πόλης δεν απαιτούν ούτε επιτρέπουν στον χρήστη να ελέγχει ποια δεδομένα συλλέγονται ή μεταδίδονται. Αυτή η απώλεια της κυριαρχίας των δεδομένων είναι μια ανησυχητική εξέλιξη επειδή η αποχώρηση από την έξυπνη πόλη είναι ανέφικτη για πολλούς. Η προστασία της ιδιωτικής ζωής δεν φαίνεται να αποτελεί αναπόσπαστο μέρος της τρέχουσας ανάπτυξης έξυπνων πόλεων. Ορισμένες βαθμολογίες συγκρίνουν τις πόλεις από την άποψη της έξυπνης συμπεριφοράς [7] αναθέτοντας βαθμολογίες σε δεκάδες δείκτες. Στις τρεις βαθμολογίες, μόνο ένας δείκτης αναφέρεται στην προστασία της ιδιωτικής ζωής, ιδιαίτερα στην παρουσία μιας πολιτικής απορρήτου. Η ακαδημαϊκή βιβλιογραφία σχετικά με την προστασία της ιδιωτικής ζωής σε έξυπνες πόλεις είναι ακόμη σπάνια και πολλές εκθέσεις που απευθύνονται στους δημιουργούς των έξυπνων πόλεων δεν αναφέρουν ούτε καν τη λέξη ιδιωτικότητα. Για παράδειγμα, μια μελέτη περίπτωσης σχετικά με τις κορυφαίες έξυπνες πόλεις δεν καλύπτει την προστασία της ιδιωτικής ζωής [10] και παρόλο που μια πρόσφατη έκθεση σχετικά με τις έξυπνες πόλεις στο Ηνωμένο Βασίλειο αναφέρει το απόρρητο, δεν το αναγνωρίζει ως γενική πρόκληση ή πρόβλημα [11].

Οι αναγνώστες αυτών των αναφορών - που απευθύνονται σε ηγέτες των πόλεων, πωλητές, παρόχους υπηρεσιών και επενδυτές - θα μπορούσαν να οδηγήσουν στο συμπέρασμα ότι δεν υπάρχουν προβλήματα προστασίας της

ιδιωτικής ζωής σε έξυπνες πόλεις. Πολλές μελέτες έχουν εντοπίσει ότι η αποδοχή από τους χρήστες είναι μία από τις σημαντικότερες απαιτήσεις για την επιτυχή εισαγωγή και λειτουργία νέων τεχνολογιών έξυπνων πόλεων [12].

2.1. Ιστορική Αναδρομή

Η βασική ιδέα ενός δικτύου έξυπνων συσκευών συζητήθηκε ήδη από το 1982, με μια τροποποιημένη μηχανή αυτόματης πώλησης Coca-Cola στο πανεπιστήμιο Carnegie Mellon να γίνει η πρώτη συσκευή που συνδέεται με το Διαδίκτυο [5], ικανή να αναφέρει την απογραφή της και αν τα νεοσύστατα ποτά είναι κρύο ή όχι. Το βιβλίο Mark Weiser του 1991 για την πανταχού παρούσα πληροφορική , "ο υπολογιστής του 21ου αιώνα", καθώς και ακαδημαϊκοί χώροι όπως οι UbiComp και PerCom, παρήγαγαν το σύγχρονο όραμα της IoT. [7] [8] Το 1994, ο Reza Raji περιέγραψε την έννοια στο IEEE Spectrum ως "[μετακίνηση] μικρών πακέτων δεδομένων σε ένα μεγάλο σύνολο κόμβων, έτσι ώστε να ενσωματωθούν και να αυτοματοποιηθούν όλα από οικιακές συσκευές σε ολόκληρα εργοστάσια". [9] Μεταξύ του 1993 και του 1997, πολλές εταιρείες που προτείνονται λύσεις, όπως η Microsoft 's Εργασία σε ή Novell' s NEST . Το πεδίο κέρδισε δυναμική όταν ο Bill Joy οραματίστηκε η επικοινωνία μεταξύ συσκευής ως μέρος του πλαισίου του "Six Webs", που παρουσιάστηκε στο Παγκόσμιο Οικονομικό Φόρουμ στο Νταβός το 1999. [10]

Ο όρος "Διαδίκτυο των πραγμάτων" ήταν πιθανότατα επινοημένος από τον Kevin Ashton της Procter & Gamble , αργότερα το Auto-ID Center του MIT , το 1999 [11], αν και προτιμά τη φράση "Διαδίκτυο για τα πράγματα". [12] Στο σημείο αυτό, θεωρούσε την αναγνώριση ραδιοσυχνοτήτων (RFID) ως απαραίτητη για το Διαδίκτυο των πραγμάτων, [13] η οποία θα επέτρεπε στους υπολογιστές να διαχειρίζονται όλα τα μεμονωμένα πράγματα. [14] [15] [16]

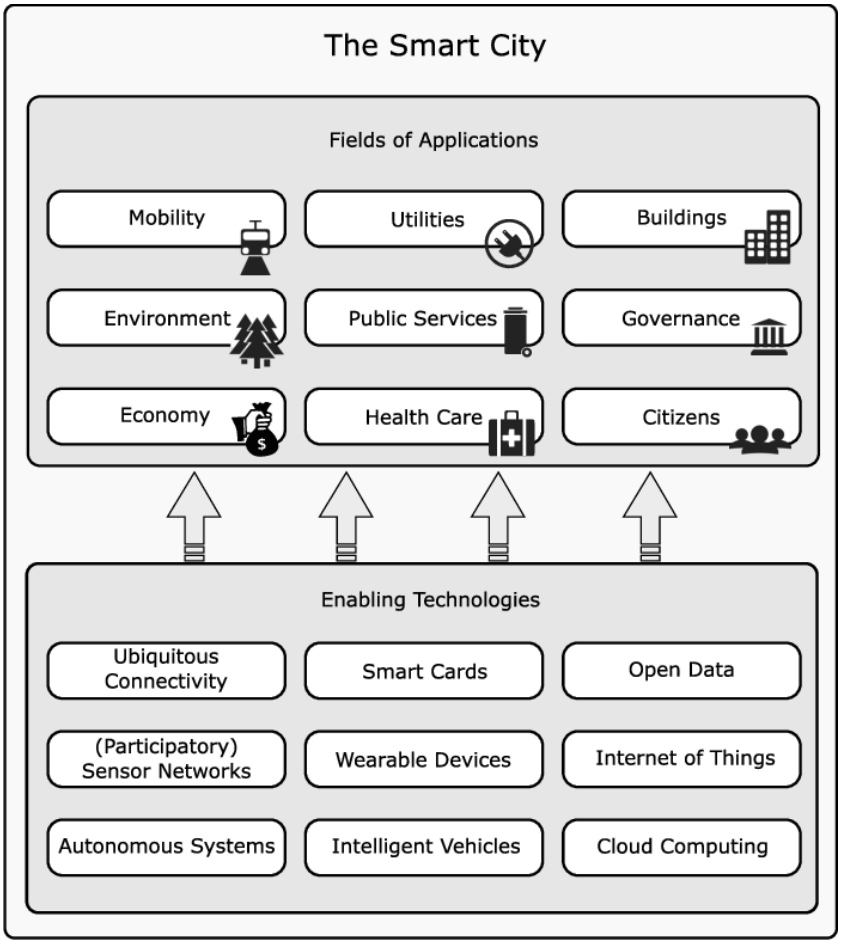
Ο καθορισμός του Διαδικτύου των πραγμάτων ως απλά το χρονικό σημείο που περισσότερα αντικείμενα συνδέονταν με το Διαδίκτυο από τους ανθρώπους, έγινε από την Cisco Systems που έκρινε ότι το IoT "γεννήθηκε" μεταξύ του 2008 και του 2009, από 0,08 το 2003 σε 1,84 το 2010. [17]

2.2. Εφαρμογές καταναλωτών

Ένα αυξανόμενο τμήμα των συσκευών IoT δημιουργούνται για χρήση από τους καταναλωτές, συμπεριλαμβανομένων των συνδεδεμένων οχημάτων, του αυτοματισμού στο σπίτι , της φορητής τεχνολογίας , της συνδεδεμένης υγείας και των συσκευών με δυνατότητες απομακρυσμένης παρακολούθησης. [25]

2.2.1. Εφαρμογές έξυπνων πόλεων

Οι πρωταρχικοί στόχοι των έξυπνων πόλεων είναι η βελτίωση της ποιότητας ζωής των πολιτών και η δημιουργία οικονομικής ανάπτυξης. Αυτοί οι δύο στόχοι μπορούν να επιτευχθούν με την αύξηση της αποτελεσματικότητας και της βιωσιμότητας, επιτρέποντας στους πολίτες να συμμετέχουν και βελτιώνοντας τη λήψη αποφάσεων μέσω της αυξημένης διαθεσιμότητας πληροφοριών. Για το σκοπό αυτό, έχουν προταθεί ή έχουν ήδη αναπτυχθεί πολλές εφαρμογές έξυπνων πόλεων σε εννέα βασικούς τομείς: Κινητικότητα, Βοηθητικά μέσα, Κτίρια, Περιβάλλον, Δημόσιες Υπηρεσίες, Διακυβέρνηση, Οικονομία, Υγεία και Πολίτες (βλέπε το πάνω μισό της εικόνας 1).



Εικόνα 1. Εφαρμογές έξυπνων πόλεων και τεχνολογίες ευρείας εφαρμογής

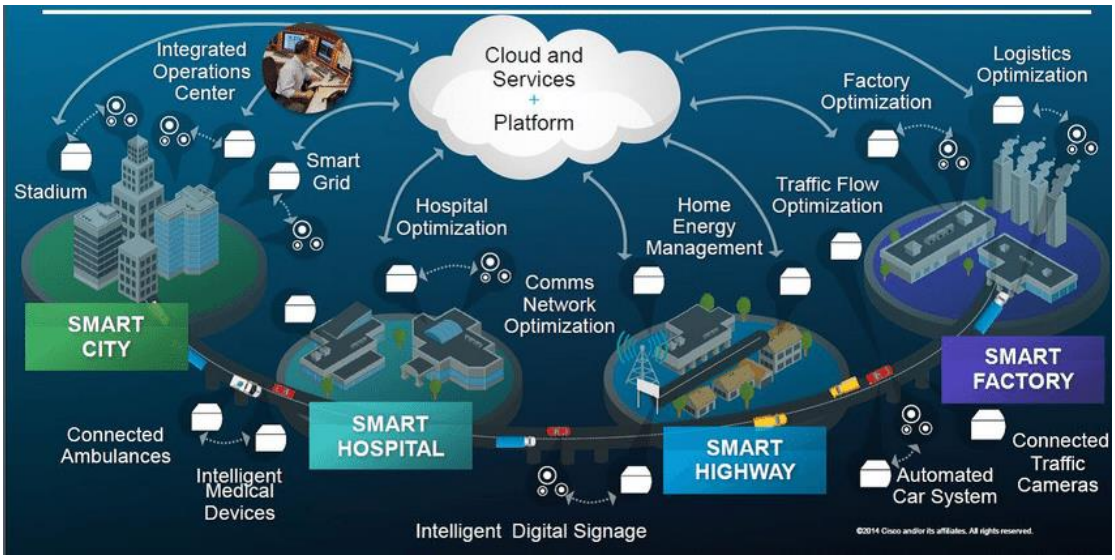
Αυτές οι εννέα περιοχές δεν είναι σε καμία περίπτωση απομονωμένες μεταξύ τους. Αντίθετα, οι υπηρεσίες σε διαφορετικές περιοχές μπορούν να αλληλεπιδρούν και συχνά αναπτύσσονται σε συνδυασμό. Για παράδειγμα, τα έξυπνα κτίρια συχνά συνδυάζονται με λύσεις έξυπνης χρησιμότητας για να διευκολύνουν τη διαχείριση της ζήτησης ηλεκτρικής ενέργειας από το δίκτυο [12], [15].

2.3. Τεχνολογίες Διαδικτύου των πραγμάτων (IoT) για έξυπνες πόλεις

Καθώς οι πόλεις αναπτύσσονται και επεκτείνονται, έξυπνες και καινοτόμες λύσεις είναι ζωτικής σημασίας για τη βελτίωση της παραγωγικότητας, την αύξηση της επιχειρησιακής αποτελεσματικότητας και τη μείωση του κόστους διαχείρισης [1]. Οι πολίτες εξοπλίζουν σταδιακά τα σπίτια τους με συσκευές IoT όπως τηλεόραση και Internet box. Στον τομέα των ακινήτων, τα συνδεδεμένα αντικείμενα περιλαμβάνουν θερμοστάτες, έξυπνους συναγερμούς, έξυπνες κλειδαριές θυρών και άλλα συστήματα και συσκευές. Στη συνδιάσκεψη των Ηνωμένων Εθνών για την αλλαγή του κλίματος (Cop21) που πραγματοποιήθηκε στο Παρίσι το 2016, τα αντικείμενα που συνδέονται με τα αντικείμενα αντιμετωπίστηκαν εκτενώς και έδωσαν σε πολλές τοπικές κοινότητες την ευκαιρία να επανεξετάσουν τους περιβαλλοντικούς στόχους τους, προκειμένου να μειώσουν τις εκπομπές CO2 τους μέσω της χρήσης του IoT.

Οι τελευταίες μπορούν να διαδραματίσουν ζωτικό ρόλο στο πλαίσιο των έξυπνων πόλεων. Για παράδειγμα, τα ευφυή δοχεία αποβλήτων μπορούν να αποφέρουν πραγματικά οφέλη στους πολίτες. θα είναι σε θέση να υποδείξουν ότι σύντομα θα είναι πλήρεις και θα πρέπει να εκκενωθούν. Οι πολίτες μπορούν να ελέγξουν μέσω μιας έξυπνης εφαρμογής τηλεφώνου εάν τα δοχεία αποβλήτων στο δρόμο είναι γεμάτα ή όχι. Επίσης, μετά την αναγγελία των δοχείων απορριμμάτων, οι εταιρείες μπορούν να προσφέρουν λύσεις βελτιστοποίησης διαδρομών στις ομάδες υπεύθυνες για τη συλλογή απορριμμάτων. Οι χώροι μπορούν να εξοπλιστούν με αισθητήρες και να παρακολουθούν τις περιβαλλοντικές συνθήκες, οι ποδηλάτες ή οι αθλητές μπορούν να βρουν τα πιο "υγιή" ταξίδια και η πόλη μπορεί να ανταποκριθεί προσαρμόζοντας την κίνηση ή φυτεύοντας περισσότερα δέντρα σε ορισμένες περιοχές. Τα δεδομένα θα είναι προσιτά σε όλους τους πολίτες για να προωθήσουν τη δημιουργία εφαρμογών χρησιμοποιώντας πληροφορίες σε πραγματικό χρόνο για τους κατοίκους.

Οι πόλεις έχουν γίνει κόμβοι για την ανταλλαγή γνώσεων. Οι τεχνολογίες και οι λύσεις που απαιτούνται για τη δημιουργία έξυπνων πόλεων μόλις αρχίζουν να εμφανίζονται. Η εικόνα 2 περιγράφει ένα παράδειγμα μιας έξυπνης πόλης.



Εικόνα 2. Ανάπτυξη έξυπνων πόλεων

Η Gartner έχει αναφέρει [2] ότι η επένδυση στην IoT θα είναι ζωτικής σημασίας για την κατασκευή έξυπνων πόλεων και υπηρεσιών, καθώς η χρήση των δεδομένων θα αποφέρει τα περισσότερα έσοδα. Η ασφάλεια και η ασφάλεια των έξυπνων κατοικιών θα είναι η δεύτερη μεγαλύτερη αγορά όσον αφορά τα έσοδα από υπηρεσίες. Όσον αφορά τις υπηρεσίες που σχετίζονται με την υγεία και την ευημερία, θα πρέπει να αντιπροσωπεύουν μια αγορά ύψους 38 δισεκατομμυρίων δολαρίων το 2020 [2]. Μια πρακτική λύση πρέπει να βρει τις ανταλλαγές μεταξύ της αποτελεσματικότητας και των ιδιωτικών κινδύνων.

Ένας εξελιγμένος επιτιθέμενος θα μπορούσε, για παράδειγμα, να πάρει τον έλεγχο των διαφόρων ευφυών συσκευών όπως οι κάμερες φωτισμού, τα φανάρια, τα συνδεδεμένα αυτοκίνητα και πολλές άλλες έξυπνες συσκευές στις πόλεις. Με περισσότερα από 50 δισεκατομμύρια συσκευές συνδεδεμένες έως το 2020, οι δήμοι θα ανησυχούν πολύ για την ασφάλεια των ευφυών πόλεων [2] [3]. Ωστόσο, οι λύσεις για την αντιμετώπιση των ανησυχιών σχετικά με την ασφάλεια, την ασφάλεια και την προστασία της ιδιωτικής ζωής των έξυπνων πόλεων που βασίζονται σε ποικίλα ευφυή αντικείμενα δεν εμπίπτουν μόνο στην

τεχνολογία, αλλά και σε άλλους τομείς, όπως η κοινωνιολογία, η νομική διαχείριση και η πολιτική.

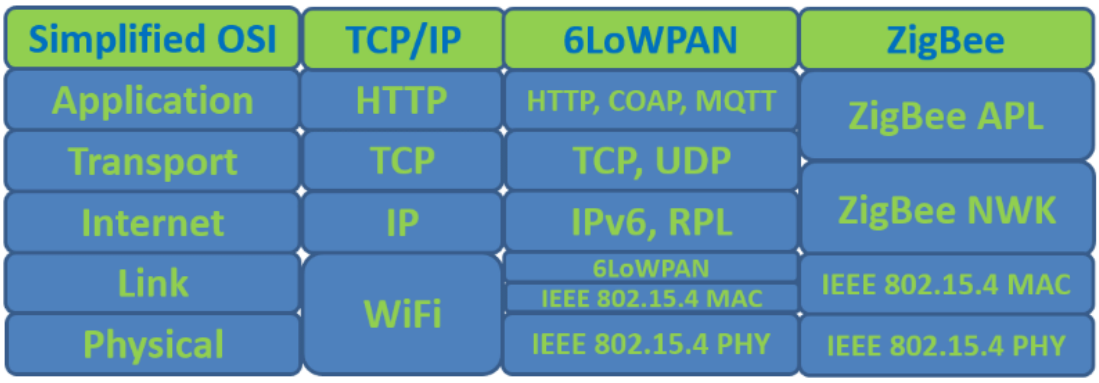
2.3.1. Διαδίκτυο των πραγμάτων και έξυπνη πόλη

Στην πρόσφατη βιβλιογραφία, αρκετοί συγγραφείς έχουν δώσει ορισμούς για τον όρο Διαδίκτυο των πραγμάτων [4] [5] [6]. Το Διαδίκτυο μπορεί να οριστεί ως "Αντικείμενα που έχουν ταυτότητες και εικονικές προσωπικότητες σε έξυπνους χώρους χρησιμοποιώντας έξυπνες διεπαφές για σύνδεση και επικοινωνία εντός κοινωνικού και ιατρικού περιβάλλοντος και χρηστών" [7]. Σήμερα πραγματοποιούνται τεράστιες επενδύσεις στην περιοχή του IoT για την υποστήριξη της παροχής υπηρεσιών ευρείας κλίμακας. Διάφορες πτυχές της κοινωνικής και οικονομικής ζωής εξετάζονται επί του παρόντος για την IoT. Η εμπιστοσύνη στο IoT συνεπάγεται ότι οι επενδυτές δεν διστάζουν να δεσμευτούν οικονομικά σε αυτό. 100 εκατομμύρια ευρώ επενδύθηκαν από μεγάλες εταιρείες όπως η Telefónica, η SK Telecom, η NTT Docomo Ventures, η Elliott Management Corporation και οι βιομηχανικές ομάδες GDF SUEZ, η Air Liquide για έρευνα και ανάπτυξη του Διαδικτύου.

Η ανάπτυξη του IoT απαιτεί πρότυπα επικοινωνίας που λειτουργούν άψογα μεταξύ των διαφόρων αντικειμένων. Αρκετοί διεθνείς οργανισμοί συμμετέχουν στην τυποποίηση αυτών των επικοινωνιών. Μεταξύ αυτών συγκαταλέγονται η Διεθνής Ένωση Τηλεπικοινωνιών (ITU), το Ινστιτούτο Ηλεκτρολόγων Μηχανικών και Ηλεκτρονικών Μηχανικών (IEEE), η Task Force Μηχανικών Διαδικτύου (IETF), το Παγκόσμιο Πρότυπο1 (GS1), ο Οργανισμός Προώθησης Δομημένων Πληροφοριακών Προτύπων (OASIS) Βιομηχανική Διαδικτυακή Κοινοπραξία (IIC), και πολλά άλλα. Παρουσιάζουμε εν συντομία μερικά από αυτά τα πρότυπα και τις πρωτοβουλίες του Διαδικτύου στον Πίνακα 1. Για παράδειγμα, η Διεθνής Πρωτοβουλία Ίντερνετ των Πράξεων (IoT-GSI) υποστηριζόμενη από την ITU έκανε δύο συστάσεις: το ITU-T Y.2060 [8] επισκόπηση της έννοιας της IoT και ITU-T Y.2061 [8], η οποία περιγράφει τις συνθήκες για τη διεπαφή μηχανής προσανατολισμένη προς εφαρμογές.

Διάφορα πρότυπα προτάθηκαν από τα IEEE και IETF σε διαφορετικά επίπεδα για τα δίκτυα αισθητήρων που βασίζονται στο πρωτόκολλο Internet (IP).

Για παράδειγμα, στο επίπεδο σύνδεσης, το πρότυπο IEEE 802.15.4 είναι πιο κατάλληλο από το Ethernet σε βιομηχανικά περιβάλλοντα. Σε επίπεδο δικτύου, το πρότυπο IPv6 πάνω σε ασύρματα δίκτυα προσωπικών χώρων χαμηλής κατανάλωσης (6LoWPAN) μπορεί να προσαρμόσει το πρωτόκολλο IPv6 για ασύρματες επικοινωνίες [9]. Το 2011, το IETF δημοσίευσε το πρότυπο πρωτόκολλο δρομολόγησης IPv6 (RPL) για δίκτυα χαμηλής κατανάλωσης ενέργειας. Το IETF ξεκίνησε επίσης μια ομάδα εργασίας για την τυποποίηση ενός πρωτοκόλλου προσανατολισμένου στρώματος εφαρμογών για συνδεδεμένα αντικείμενα. Το πρωτόκολλο αναφοράς ονομάζεται πρωτόκολλο περιορισμένης εφαρμογής (CoAP). Το CoAP (δείτε το RFC 7252 του Ιουνίου 2014) παρέχει μεθόδους και εντολές (όπως HTTP Get) για την αναζήτηση ενός αντικειμένου και την αλλαγή της κατάστασής του. Το CoAP βασίζεται στο UDP και μπορεί προαιρετικά να χρησιμοποιεί Datagram Transport Layer Security (DTLS) για την παροχή ασφάλειας επικοινωνίας. Τα λειτουργικά συστήματα [10] που χρησιμοποιούνται σε IoT περιλαμβάνουν: TinyOS, Contiki OS, MantisOS, Nano-RK, Android, Brillo (Google), Windows 10 IoT Core, LiteOS (Huawei). Επιπλέον, έχουν αναπτυχθεί αρκετές πλατφόρμες [10] για το IoT: Arrayent, πλαίσιο Καλιφόρνιας CoAP Java, Erbium, πλαίσιο CoAP για το Contiki και στοίβα δικτύωσης XMesh. Στο επίπεδο εφαρμογής, αναπτύχθηκε ένας μεγάλος αριθμός εφαρμογών [10]: Iobridge Thingspeak, Nimbits, Evrythng, Open.Sen.se, NanoService, exosite One, η HP υποτίθεται, Isidorey, SensorCloud, Manybots κ.ο.κ. Η εικόνα 3 συγκρίνει τη στοίβα επικοινωνίας 6lowPAN με άλλες δημοφιλείς στοίβες επικοινωνίας.

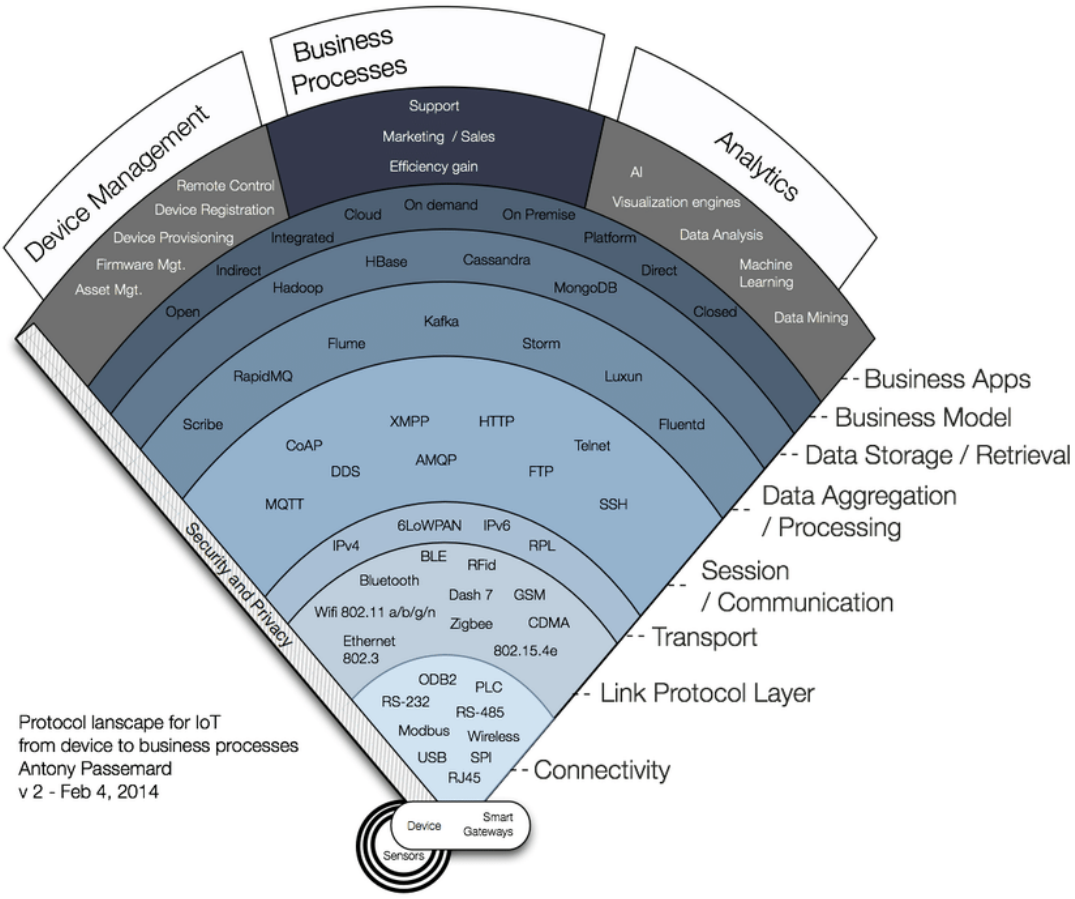


Εικόνα 3. Σύγκριση της στοίβας του 6LowPAN με άλλες στοίβες [11]

Η πρωτοβουλία του Global Standard 1 (GS1) του Global Electronic Code Code (Global Product Code) καθορίζει ένα μοναδικό μεμονωμένο αναγνωριστικό για τον προσδιορισμό ενός ηλεκτρονικού προϊόντος και τη γενική αρχιτεκτονική δικτύου EPC που ορίζει την οργάνωση συστημάτων πληροφοριών σχεδιασμένων για την ανταλλαγή πληροφοριών σε ένα δίκτυο EPC [12] [13]. Ένα από τα κύρια συστατικά του είναι η υπηρεσία ονομασίας αντικειμένου (ONS), η οποία βασίζεται στο σύστημα ονομάτων τομέα (DNS). Στην πραγματικότητα, το 1970 προέκυψε το πρότυπο της ευρωπαϊκής αρίθμησης αντικειμένων (EAN) για τον προσδιορισμό του προϊόντος. Ωστόσο, αυτός ο γραμμικός κώδικας EAN χρησιμοποιείται στην πραγματικότητα για την αναγνώριση μιας κατηγορίας προϊόντων, όχι για μεμονωμένες περιπτώσεις εντός αυτής της κατηγορίας. Επιπλέον, στο διαδίκτυο, απαιτείται μια μοναδική διεύθυνση IP για κάθε σύνδεση. Αυτός είναι ο λόγος για τον οποίο το EPC προτάθηκε από το GS1 ως νέο πρότυπο. Εν τω μεταξύ, η OASIS εξέδωσε διάφορες συστάσεις σχετικά με τις τεχνολογίες δικτύου στις τεχνολογίες επικοινωνίας και τεχνολογίας ανταλλαγής μηνυμάτων, όπως η τηλεμετρία μεταφοράς μηνυμάτων (MQTT), το πρωτόκολλο Advanced Message Queuing Protocol (AMQP) και η υπηρεσία διανομής δεδομένων για συστήματα πραγματικού χρόνου (DDS).

Το 2014 ξεκίνησε μια νέα Κοινοπραξία Βιομηχανικού Διαδικτύου (ICC), προκειμένου να συντονιστούν και να καθιερωθούν οι προτεραιότητες και οι τεχνολογίες που επιτρέπουν το βιομηχανικό Διαδίκτυο. Υπάρχουν χιλιάδες ιδρυτικά και συνεισφέροντα μέλη του ICC και περιλαμβάνουν: Bosh, Intel, IBM,

Schneider, Huawei, Cisco και πολλούς άλλους. Υπάρχουν επί του παρόντος 19 ομάδες εργασίας και ομάδες που εργάζονται σε διάφορους τομείς: Επιχειρηματική Στρατηγική και Λύση Κύκλου Ζωής, Νομική, Διασύνδεση, Ασφάλεια, Τεχνολογικές Δοκιμές, Μάρκετινγκ και Σύνθεση κ.ο.κ. Η εικόνα 4 συνοψίζει ορισμένα πρωτόκολλα και πρότυπα του IoT και ο Πίνακας 2 περιγράφει λεπτομερώς τα χρησιμοποιούμενα ακρωνύμια.



Εικόνα 4. Πρωτόκολλο Ίντερνετ των πραγμάτων [14]

Μια έξυπνη πόλη ορίζεται ως μια πόλη που συνδέει τις φυσικές υποδομές, τις υποδομές ΤΠΕ, τις κοινωνικές υποδομές και τις επιχειρηματικές υποδομές για την αξιοποίηση της συλλογικής νοημοσύνης της πόλης [15]. Μια πόλη μπορεί να είναι έξυπνη μέσω μιας μεγάλης ανάπτυξης του IoT (ειδικά μέσω της επικοινωνίας μηχανή με μηχανή και από άνθρωπο σε μηχανή). Τα ασύρματα δίκτυα αισθητήρων (WSNs), ο βραχίονας ενεργοποίησης αισθητήρα του IoT, ενσωματώνονται άψογα στην αστική υποδομή σχηματίζοντας γύρω της ένα

«ψηφιακό δέρμα». Οι πληροφορίες που δημιουργούνται είναι κοινές σε διάφορες πλατφόρμες και εφαρμογές για την ανάπτυξη μιας κοινής επιχειρησιακής εικόνας (COP) της πόλης [16].

2.4. Αρχιτεκτονική IoT

Οι τεχνολογίες IoT αναμένεται να είναι μέρος δικτύων μεγάλης κλίμακας, με τον αριθμό των συσκευών να ανέρχεται σε χιλιάδες και τις περιοχές να εκτείνονται σε αρκετά χιλιόμετρα. Στο υπόλοιπο κεφάλαιο αυτό, εστιάζουμε κυρίως στην τεχνολογία LoRa Ultra-Narrow Band (UNB) που αναπτύχθηκε από την Semtech και τη SigFox.

Πίνακας 1. Κύρια επικοινωνιακά πρότυπα στο Διαδίκτυο

	802.11a	802.11b	802.11g	802.11n	802.11 ac	802.11 ad	802.15.1	802.15.3	802.15.4	802.15.6	NFC
Network Type	WLAN	WLAN	WLAN	WLAN	WLAN	WLAN	WPAN	WPAN	WPAN	WBAN	Point-to-Point
Date	1999	1999	2003	2009	2014	2012	2002/2005	2003	2007	2011	2011
Network Size	30	30	30	30			7	245	65535	250	-
Bit Rate	54 Mbps	11Mbps	54 Mbps	248 Mbps	3.2 Gbps	≥ 7Gbps	3 Mbps	55 Mbps	250 Kbps	10 Mbps	424 Kbps
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5/60GHz	2.4 GHz	2.4 GHz	868-915 MHz 2.4 GHz	402-405 MHz	13.56 Mhz
Range	120 m	140 m	140 m	50 m indoor 250 m outdoor	30 m	5 m	100 m	100 m	75 m	2-5 m	0.2 m
Modulation	BPSK, QPSK 16-QAM 64-QAM OFDM	DBPSK DQPSK CCK DSSS	DBPSK DQPSK 16-QAM 64-QAM OFDM	OFDM	OFDM	QAM-256	8DPSK DQPSK PIDQPSK GFSK AFM	QPSK DQPSK 16-QAM 32-QAM 64-QAM	ASK DSSS PSSS		Manchester and Modified Miller
Application	WiFi	WiFi	WiFi	WiFi			Bluetooth		ZigBee		

Πίνακας 2. Πίνακας ακρωνύμιων

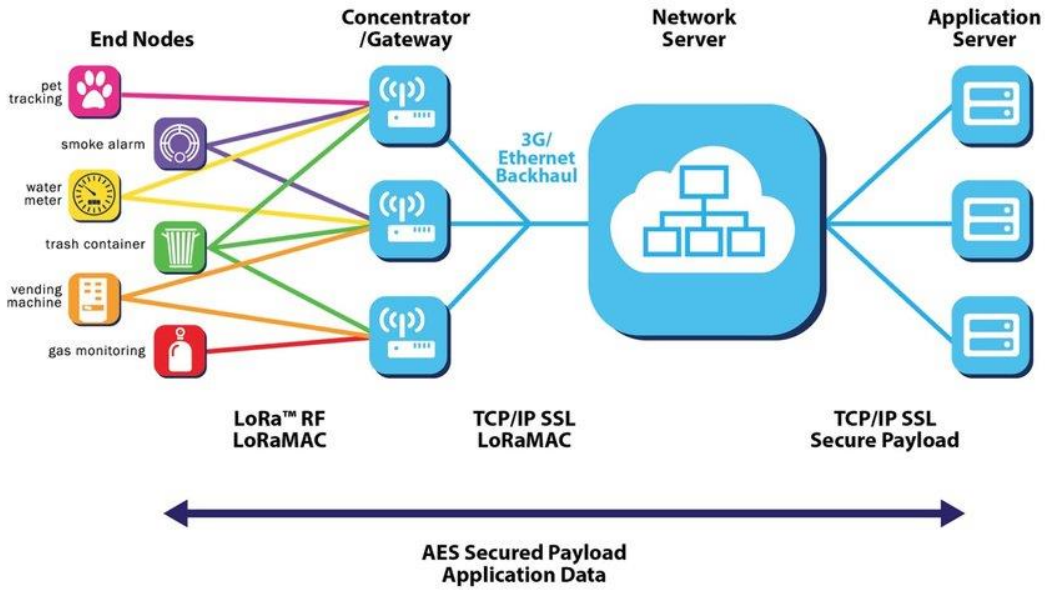
Acronym	Description	Acronym	Description
HBase	Hadoop Database	RapidMQ	Rapid Message Queuing
MQTT	Message Queuing Telemetry Transport	DDS	Data Distribution Service
XMPP	Extensible Messaging and Presence Protocol	AMQP	Advanced Message Queuing Protocol
HTTP	HyperText Transfer Protocol	FTP	File Transfer Protocol
Telnet	Telecommunication Network	SSH	Secure SHell
IPv4	Internet Protocol Version 4	IPv6	Internet Protocol version 6
6LowPan	IPv6 over Low power Wireless Personal Area Networks	RPL	IPv6 Routing Protocol for Low-Power and Lossy Networks
BLE	Bluetooth Low Energy	RFID	radio frequency identification
GSM	Global System for Mobile Communications	CDMA	Code division multiple access
OBD2	On-board diagnostics 2	PLC	Power-line communication
RS-232	Recommended Standard 232	Modbus	Modicon Communication Bus
USB	Universal Serial Bus	SPI	Serial Peripheral Interface
AES	Advanced Encryption Standard	SSL	Secure Sockets Layer

2.4.1. LoRa

Η LoRa είναι μια ασύρματη τεχνολογία που έχει σχεδιαστεί για να παρέχει χαμηλή ισχύ σε δίκτυα ευρείας περιοχής (LPWAN) που απαιτούνται για τις υπηρεσίες Internet of Things [17]. Η τεχνολογία προσφέρει ένα συνδυασμό μεγάλης εμβέλειας, χαμηλής κατανάλωσης ενέργειας και ασφαλούς μετάδοσης δεδομένων. Το πρότυπο LoRa έχει αναπτυχθεί για συσκευές τύπου IoT σε περιφερειακά ή παγκόσμια δίκτυα. Αυτή η τεχνολογία παρέχει απρόσκοπτη διαλειτουργικότητα μεταξύ των συσκευών χωρίς να απαιτούνται πολύπλοκες εγκαταστάσεις. Οι υπηρεσίες που στοχεύουν περιλαμβάνουν την παρακολούθηση της ενεργειακής κατανάλωσης στο σπίτι, τα συστήματα συναγερμού, την απομακρυσμένη παρακολούθηση της υγείας, τη μεταφορά, την προστασία του περιβάλλοντος κ.ο.κ.

Αυτή η προδιαγραφή καθορίζει το πρωτόκολλο επικοινωνίας και την αρχιτεκτονική συστήματος για το υποκείμενο δίκτυο. Υποστηρίζει συχνότητες στις ζώνες ISM 433, 868 ή 915 MHz, ανάλογα με την περιοχή στην οποία

αναπτύσσεται. Στην Ευρώπη, χρησιμοποιεί είτε το Gaussian Frequency Shift Keying (GFSK) είτε το ιδιόκτητο σύστημα διαμόρφωσης LoRa, το οποίο λειτουργεί με μια έκδοση του Chirp Spread Spectrum χρησιμοποιώντας εύρος ζώνης διαύλου 125 KHz [18]. Η αρχιτεκτονική LoRa περιγράφεται στην εικόνα 5.



Εικόνα 5. Αρχιτεκτονική LoRa [20]

Η ιεραρχική τοπολογία βασισμένη σε άστρα χρησιμοποιείται από τα δίκτυα LoRa. Οι συσκευές IoT σε τέτοια δίκτυα μπορούν να είναι διακομιστές, τελικά σημεία ή πύλες.

Οι ρυθμοί δεδομένων μπορούν να κυμανθούν, στην Ευρώπη, από 0,3 Kbps έως και 50 Kbps όταν χρησιμοποιείται η συσσωμάτωση καναλιών. Στη Βόρειο Αμερική, ο ελάχιστος ρυθμός δεδομένων είναι 0,9 Kbps λόγω των απαιτήσεων της FCC (Federal Communications Commission). Το ωφέλιμο φορτίο για αυτήν την τεχνολογία μπορεί να κυμαίνεται από 2 έως 255 bytes [19]. Αυτό το πρότυπο είναι βελτιστοποιημένο για αισθητήρες χαμηλού κόστους και μπαταρίας. Οι συσκευές είναι ασύγχρονες και επικοινωνούν μόνο όταν έχουν δεδομένα έτοιμα να αποσταλούν εάν η εκδήλωση είναι προγραμματισμένη ή προγραμματισμένη. Η κατανάλωση ρεύματος είναι ανάλογη με τις συσκευές

που ξοδεύονται κατά τη διάρκεια της λειτουργίας ακρόασης. Το LoRa κερδίζει σημαντική προσοχή στα δίκτυα IoT που αναπτύσσονται από τους φορείς εκμετάλλευσης ασύρματων δικτύων. Μπορεί να αναπτυχθεί με ελάχιστες επενδύσεις υποδομής και λειτουργικά έξοδα. Όταν απαιτείται αυξημένη χωρητικότητα δικτύου, μπορούν να προστεθούν και άλλες πύλες. Εκτιμάται ότι το κόστος εγκατάστασης αυτής της τεχνολογίας σε μη αδειοδοτημένες ζώνες χρειάζεται πολύ λιγότερα κεφάλαια από ό, τι ακόμη και μια αναβάθμιση λογισμικού 3G [19].

Οι μεγάλοι φορείς εκμετάλλευσης τηλεπικοινωνιών (π.χ. Swisscom, NKE Electronics και άλλοι) αναπτύσσουν αυτήν την τεχνολογία σε εθνικά δίκτυα λόγω των πλεονεκτημάτων τους έναντι των ανταγωνιστικών τεχνολογιών. Αυτά τα οφέλη περιλαμβάνουν αμφίδρομες επικοινωνίες, κινητικότητα για παρακολούθηση περιουσιακών στοιχείων, ασφάλεια και ακριβή εντοπισμό [20].

2.4.2. SigFox

Η SigFox δημιούργησε ένα σύστημα επικοινωνιών ultra-narrowband IoT που σχεδιάστηκε για να υποστηρίξει τις εφαρμογές IoT σε μεγάλες αποστάσεις, π.χ. πάνω από 20 km μεταξύ μιας συσκευής πελάτη και ενός σταθμού βάσης . Η SigFox χρησιμοποιεί φάσμα απαλλαγμένο από άδειες εκμετάλλευσης για το προϊόν της, δηλαδή τη ζώνη των 868 MHz στην Ευρώπη και τη ζώνη 915 MHz στις ΗΠΑ, για τη μετάδοση δεδομένων από ένα στενό φάσμα προς και από τα συνδεδεμένα αντικείμενα. Η λειτουργία εξαιρετικά στενής λωρίδας επιτυγχάνεται χρησιμοποιώντας κανάλια εύρους ζώνης κάτω από 1 KHz που μεταδίδουν δεδομένα ωφέλιμου φορτίου 12 bits uplink και 8 bits downlink με ένα overhead πρωτόκολλο 26 byte [19].

Ένα από τα πλεονεκτήματα των συσκευών SigFox είναι η αποδοτικότητα των πόρων τους. Η ζήτηση ισχύος είναι αμελητέα επειδή οι συσκευές είναι "ενεργοποιημένες" μόνο όταν μεταδίδουν. αυτό σημαίνει ότι η ζήτηση ισχύος είναι ένα κλάσμα της ζήτησης για μια συσκευή που λειτουργεί σε κυψελοειδή

δίκτυα. Η τεχνολογία SigFox επιτρέπει την ανάπτυξη πολύ αποτελεσματικών επικοινωνιών χαμηλής απόδοσης, περιορίζοντας τον αριθμό των κεραιών (σταθμοί βάσης). Για το ίδιο επίπεδο κάλυψης, η SigFox απαιτεί περίπου 1.000 φορές λιγότερες κεραίες και σταθμούς βάσης, σε σύγκριση με ορισμένα κυψελοειδή δίκτυα *. Αυτή η τεχνολογία προσφέρει πρόσβαση σε μια διεπαφή διαχείρισης υπηρεσιών, η οποία μπορεί να ενεργοποιήσει τον έλεγχο βασικών παραμέτρων επικοινωνίας, όπως ρυθμίσεις μπαταρίας και θερμοκρασίας, ποιότητα σήματος, όγκο ανταλλαγμένων δεδομένων και άλλα.

Τα δίκτυα που βασίζονται στην τεχνολογία SigFox έχουν ήδη συνδέσει χιλιάδες συσκευές σε διάφορες διεθνείς πόλεις. Επί του παρόντος λειτουργούν σε 14 χώρες και καλύπτουν έκταση άνω των 1,2 εκατομμυρίων τετραγωνικών χιλιομέτρων και φθάνουν τα 223 εκατομμύρια άτομα. Σε γενικές γραμμές, το IoT μπορεί να χωριστεί σε τρία επίπεδα: το επίπεδο αντίληψης, το στρώμα δικτύου και το στρώμα εφαρμογής. Το στρώμα αντίληψης χρησιμοποιείται κυρίως για τη συλλογή, τη διάκριση και την αναγνώριση των πληροφοριών αντικειμένων στον φυσικό κόσμο [5]. Αυτό το στρώμα περιλαμβάνει ετικέτες RFID, φωτογραφικές μηχανές, GPS, αισθητήρες, σαρωτές λέιζερ και ούτω καθεξής. Το επίπεδο δικτύου χρησιμοποιείται για την προώθηση πακέτων μέσω αξιόπιστου μέσου επικοινωνίας. Το επίπεδο εφαρμογής επεξεργάζεται τα δεδομένα, συγκεντρώνει διάφορες πηγές και το εμφανίζει. Ο Πίνακας 3 συγκρίνει τις διαφορετικές τεχνολογίες WAN χαμηλής ισχύος που χρησιμοποιούνται στα σενάρια περίπτωσης χρήσης διαδικτύου.

Πίνακας 3. Σύγκριση τεχνολογιών WAN χαμηλής ισχύος [21]

Standard	SIGFOX	LoRaWAN	LTE-M	IEEE P802.11ah (low power WiFi)	Dash7 Alliance Pro-tocol 1.0	Ingenu RPMA	nWave
Frequency Band	868 MHz/902 MHz ISM	868 MHz/902 MHz ISM	Cellular	License-exempt bands below 1 GHz, excluding the TV White Spaces	433, 868, 915 MHz	2.4 GHz ISM	Sub-GHz ISM
Range	30-50km (rural), 3-10km (urban), 1000km LoS	2-5k (urban), 15k (rural)	2.5-5km	Up to 1Km (outdoor)	0.5 km	>500 km LoS	10km (urban), 20-30km (rural)

2.5. IoT ως μια τεχνολογία εξουσιοδότησης για την έξυπνη πόλη

Η φιλοσοφία του IoT αξιοποιεί διάφορες πανταχού παρούσες υπηρεσίες για να διευκολύνει την ανάπτυξη του Smart City σε όλο τον κόσμο. Το IoT εισάγει νέες ευκαιρίες όπως η δυνατότητα παρακολούθησης και διαχείρισης συσκευών εξ αποστάσεως, η ανάλυση και η ανάληψη ενεργειών με βάση τις πληροφορίες που λαμβάνονται από διάφορες ροές δεδομένων κίνησης σε πραγματικό χρόνο. Ως αποτέλεσμα, τα προϊόντα IoT αλλάζουν πόλεις ενισχύοντας τις υποδομές, δημιουργώντας αποτελεσματικότερες και αποδοτικότερες δημοτικές υπηρεσίες, βελτιώνοντας τις υπηρεσίες μεταφορών μειώνοντας την κυκλοφοριακή συμφόρηση και βελτιώνοντας την ασφάλεια των πολιτών. Για να αξιοποιηθούν πλήρως οι δυνατότητες του Διαδικτύου, οι αρχιτέκτονες και οι πάροχοι έξυπνων πόλεων αναγνωρίζουν ότι οι πόλεις δεν πρέπει να προσφέρουν ξεχωριστό χαρακτηριστικό γνώρισμα για έξυπνες πόλεις, αλλά να παράγουν κλιμακούμενες και ασφαλείς λύσεις IoT που περιλαμβάνουν αποτελεσματικά συστήματα IoT. 4.1 IoT για έξυπνες πόλεις: απαιτήσεις και

αληθινά παραδείγματα Μια αποτελεσματική έξυπνη λύση πόλης πρέπει να σχεδιάζει και να ενσωματώνει πλατφόρμες IoT που πληρούν τις απαιτήσεις της σημερινής IoT και επιτρέπει τη διαχείριση εκατομμυρίων συνδεδεμένων συσκευών, συστημάτων και ανθρώπων. Συγκεκριμένα, μια πλατφόρμα IoT πρέπει να προκαλεί:

• Μείωση του κόστους και του κινδύνου που απαιτείται για τη δημιουργία και την ανάπτυξη υπηρεσιών IoT.

• Σύνδεση σε πολλά ετερογενή συστήματα σε μια πόλη.

• Μείωση του χρόνου που απαιτείται για την υλοποίηση και την ανάπτυξη υπηρεσιών IoT που αποτελούν μέρος των έξυπνων πρωτοβουλιών της πόλης.

• Εξασφάλιση ασφαλούς και κλιμακούμενης πρόσβαση σε υπηρεσίες και διάνοιξη νέων ευκαιριών για την πόλη.

• Δημιουργία αξίας (π.χ. καλύτερες υπηρεσίες) από έξυπνα συνδεδεμένα δεδομένα και συσκευές.

Πολλά αντικείμενα με διάφορες δυνατότητες (π.χ. θερμοκρασία, φωτισμός, υγρασία, πίεση) έχουν εμφανιστεί σήμερα και πολλά από αυτά μας επιτρέπουν να αντιλαμβανόμαστε παρά να αντιδρούμε απλά. Πράγματι, υπάρχουν πολλοί τομείς (υγεία, κατασκευή, μεταφορές και άλλοι) όπου αναπτύσσονται συνδεδεμένα αντικείμενα. Σύμφωνα με την IDC [22], η αγορά της κινεζικής διαδικτύου αναμένεται να φθάσει τα 361 δισεκατομμύρια δολάρια μέχρι το 2020, με αύξηση κατά 13,3% κατά την επόμενη πενταετία. Οι γνωστές κινεζικές επιχειρήσεις όπως η Alibaba, η Baidu, η Huawei, η Lenovo και η Xiaomi πραγματοποιούν μεγάλες επενδύσεις στον τομέα της διαδικτυακής πύλης. Επιπλέον, στην πόλη Zhonggnauchun, που ονομάζεται επίσης "κινεζική Silicon Valley", που βρίσκεται στα βορειοανατολικά του Πεκίνου, έχει προσελκύσει επίσης επιχειρηματίες του πολέμου από όλο τον κόσμο. Το 2015, ο Λευκός Οίκος ξεκίνησε την πρωτοβουλία Smart City, η οποία στοχεύει στη διευκόλυνση της τεχνολογικής συνεργασίας μεταξύ πόλεων, ομοσπονδιακών φορέων, πανεπιστημίων και ιδιωτικού τομέα.

Στις ΗΠΑ, η Kansas City υπέγραψε συμφωνία με την Sprint και τη Cisco για τη δημιουργία της μεγαλύτερης έξυπνης πόλης στη Βόρεια Αμερική με σκοπό τη βελτίωση των δημοτικών υπηρεσιών. Μέσω ενός ευρυζωνικού δικτύου αισθητήρων και Wi-Fi, το έργο (αξίας άνω των 15 εκατομμυρίων δολαρίων) θα παρέχει διαφορετικούς τύπους πληροφοριών στους πολίτες, συλλέγοντας δεδομένα σχετικά με τη συμπεριφορά τους στην πόλη. Η Fujisawa, μια πόλη που βρίσκεται στο νότιο Τόκιο, είναι υπό κατασκευή από την Panasonic και 3000 άτομα αναμένεται να είναι εκεί μέχρι το 2018. Η Songdo στη Νότια Κορέα χτίζεται από την Gale, μια ισχυρή αμερικανική ομάδα ακινήτων. Ο Σόνγκντο ελπίζει να καλωσορίσει περίπου 300.000 εργαζόμενους και 65.000 κατοίκους μέχρι το 2020. Τα ΗΑΕ εξετάζουν επίσης το μέλλον πέρα από την εποχή μετά το πετρέλαιο και είχαν οδηγήσει σε επενδύσεις αξίας 18 δισεκατομμυρίων δολαρίων για την κατασκευή του Masdar,) από ανανεώσιμες πηγές ενέργειας. Στο Masdar, για παράδειγμα, τα λύματα χρησιμοποιούνται για την άρδευση των χώρων πρασίνου.

Το έργο Malmo Green Digital City στη Σουηδία αποσκοπεί στο να καταστήσει το Μάλμο μια πόλη ουδέτερη σε άνθρακα μέχρι το 2020. Το έργο στοχεύει επίσης να κάνει την πόλη να λειτουργεί αποκλειστικά με ανανεώσιμες πηγές ενέργειας έως το 2030. Οι αξιωματούχοι του Μάλμο προβλέπουν ότι το έργο αυτό πόλης θα μπορεί να φιλοξενήσει 10.000 άτομα περιμένουν επιπλέον 20.000 για να εργαστούν ή να σπουδάσουν εκεί. Στο Fujisawa, το φως του δρόμου φωτίζεται μόνο όταν οι αισθητήρες ανιχνεύουν την παρουσία ενός ατόμου. Η ανακύκλωση αποτελεί επίσης ένα σημαντικό μέλημα. Στο Songdo, τα όμβρια ύδατα συλλέγονται, φιλτράρονται και χρησιμοποιούνται για την άρδευση πάρκων. Στη Γαλλία, το Υπουργείο Μεταφορών ξεκίνησε (το 2016) ένα έργο που ονομάζεται scoop @ F για την ανάπτυξη υποδομής για έξυπνα οχήματα. Στο έργο αυτό, θα δοκιμαστούν 3.000 ευφυή οχήματα σε 6 τοποθεσίες, όπως το Ile-de-France, στον περιφερειακό δρόμο του Μπορντό και στο τμήμα Isère.

Ο προϋπολογισμός του scoop @ F υπολογίζεται σε 20 εκατομμύρια ευρώ που χρηματοδοτούνται μεταξύ του κράτους, των κοινοτήτων, της βιομηχανίας και της ΕΕ. Στο έργο αυτό, προσαρμοσμένα οχήματα που κινούνται από άτομα και επαγγελματίες, θα συνδέονται με την έξυπνη διαδρομή και διασυνδέονται μέσω

τεχνολογιών WiFi, 4G ή 5G για να μοιράζονται πληροφορίες μεταξύ τους σχετικά με την κυκλοφορία, το ατύχημα, την παρουσία συντριμμιών ή ένα ζώο στο δρόμο. Επομένως, ένα συνδεδεμένο αυτοκίνητο είναι μια λύση που βελτιώνει τις συνθήκες οδήγησης συλλέγοντας και διαδίδοντας πληροφορίες κυκλοφορίας σε πραγματικό χρόνο και συνθήκες κυκλοφορίας μεταξύ των οχημάτων που θα βελτιώσουν την ασφάλεια κυκλοφορίας [23] [24]

Συνοψίζοντας, οι έξυπνες πόλεις συνδέονται με πόλεις που χρησιμοποιούν τεχνολογίες τηλεπικοινωνιών και συστήματα πληροφοριών για τη βελτίωση της ζωής των πολιτών. πιστεύουμε ότι μια έξυπνη πόλη μπορεί να γίνει έξυπνη, επιτυγχάνοντας δύο κύριους στόχους:

• Παροχή προηγμένης αστικής υποδομής με δυνατότητα συλλογής και επεξεργασίας δεδομένων με χρήση αναδυόμενων τεχνολογιών όπως έξυπνο δίκτυο, έξυπνοι μετρητές, έξυπνα κτίρια, συνδεδεμένα αντικείμενα και μεγάλα δεδομένα για την πρόβλεψη οποιωνδήποτε ανωμαλιών.

• Επιτρέποντας στους χρήστες να αλληλεπιδρούν με το περιβάλλον μέσω έξυπνων εφαρμογών, προκειμένου να μειωθούν οι εκπομπές CO2. Η μείωση των επιπέδων ρύπανσης θα βελτιώσει το περιβάλλον και τελικά την ποιότητα ζωής (π.χ. βελτίωση της υγείας, ασφαλέστερη, ταχύτερη, φθηνότερη μετακίνηση) των πολιτών.

2.6. Εφαρμογές IoT για έξυπνες πόλεις

Είναι ενδιαφέρον να εξεταστεί η εφαρμογή του παραδείγματος του IoT σε αστικό περιβάλλον. Πράγματι, πολλές εθνικές κυβερνήσεις διερευνούν σήμερα και σχεδιάζουν πώς να υιοθετήσουν λύσεις ΤΠΕ στην διαχείριση δημόσιων υπηρεσιών, προκειμένου να υλοποιήσουν την έννοια της Smart City [25].

2.6.1. Διατήρηση των κτιρίων

Για να διατηρήσουμε σωστά τα ιστορικά κτίρια μιας πόλης, πρέπει: (1) να παρακολουθούμε συνεχώς τις πραγματικές συνθήκες κάθε κτιρίου και (2) να προσδιορίσουμε τις περιοχές που πλήττονται περισσότερο από διάφορους εξωτερικούς παράγοντες [26]. Η πόλη περιέχει πολλές δομές, οι οποίες έχουν διαφορετικά μεγέθη και διαφορετικές ηλικίες. Είναι διαφορετική από μια πόλη στην άλλη, αλλά, γενικά, οι περισσότερες δομές είναι πολύ παλιές (όπως κτίρια, φράγματα ή γέφυρες [26]). Για να εκτιμηθούν οι συνθήκες ενός κτιρίου, τα παθητικά WSNs μπορούν να ενσωματωθούν μέσα σε μια δομή από σκυρόδεμα και να αποσταλούν περιοδικά ένα ραδιοσήμα με κατάλληλο εύρος και χαρακτηριστικό φάσης για να ενημερωθεί για την κατάσταση της δομής [16].

2.6.2. Περιβαλλοντική παρακολούθηση

Οι WSN επεξεργάζονται, αναλύουν και διαδίδουν πληροφορίες που συλλέγονται από πολλαπλά περιβάλλοντα [2]. Οι διάφορες παράμετροι που μετριούνται από αισθητήρες [8] είναι:

• Επίπεδο νερού για λίμνες, ρεύματα, αποχετεύσεις.

• Συγκέντρωση αερίων στον αέρα για πόλεις, εργαστήρια και καταθέσεις.

• Υγρασία εδάφους και άλλα χαρακτηριστικά.

• κλίση για στατικές δομές (π.χ. γέφυρες, φράγματα).

• Αλλαγές θέσης (π.χ., για κατολισθήσεις).

• Συνθήκες φωτισμού είτε ως μέρος συνδυασμένης ανίχνευσης είτε ως αυτόνομο (π.χ. για την ανίχνευση εισβολών σε σκοτεινά μέρη).

• Υπέρυθρη ακτινοβολία για θερμότητα (φωτιά) ή ανίχνευση ζώων.

2.6.3. Διαχείριση των αποβλήτων

Η διαχείριση των αποβλήτων γίνεται όλο και μεγαλύτερο πρόβλημα στην αστική ζωή. Σχετίζεται με πολλές πτυχές, συμπεριλαμβανομένων των κοινωνικοοικονομικών και περιβαλλοντικών. Ένα σημαντικό χαρακτηριστικό στη διαχείριση των αποβλήτων είναι η περιβαλλοντική βιωσιμότητα [9]. Ένα σημαντικό πλεονέκτημα των παγκόσμιων υποδομών IoT είναι ότι μας παρέχουν τη δυνατότητα συλλογής δεδομένων και περαιτέρω βοήθειας για τη βελτίωση της αποτελεσματικής διαχείρισης για διάφορα θέματα. Σήμερα, το φορτηγό απορριμμάτων πρέπει να παραλάβει όλα τα κουτιά σκουπιδιών ακόμη και όταν είναι άδεια [20]. Χρησιμοποιώντας συσκευές IoT μέσα στο δοχείο απορριμμάτων, αυτές οι συσκευές θα συνδεθούν με τον υπολογιστικό διακομιστή χρησιμοποιώντας μία από τις τεχνολογίες LPWAN. Ο υπολογιστικός διακομιστής μπορεί να συλλέξει τις πληροφορίες και να βελτιστοποιήσει το δρόμο για τη συλλογή απορριμμάτων από τα φορτηγά απορριμμάτων.

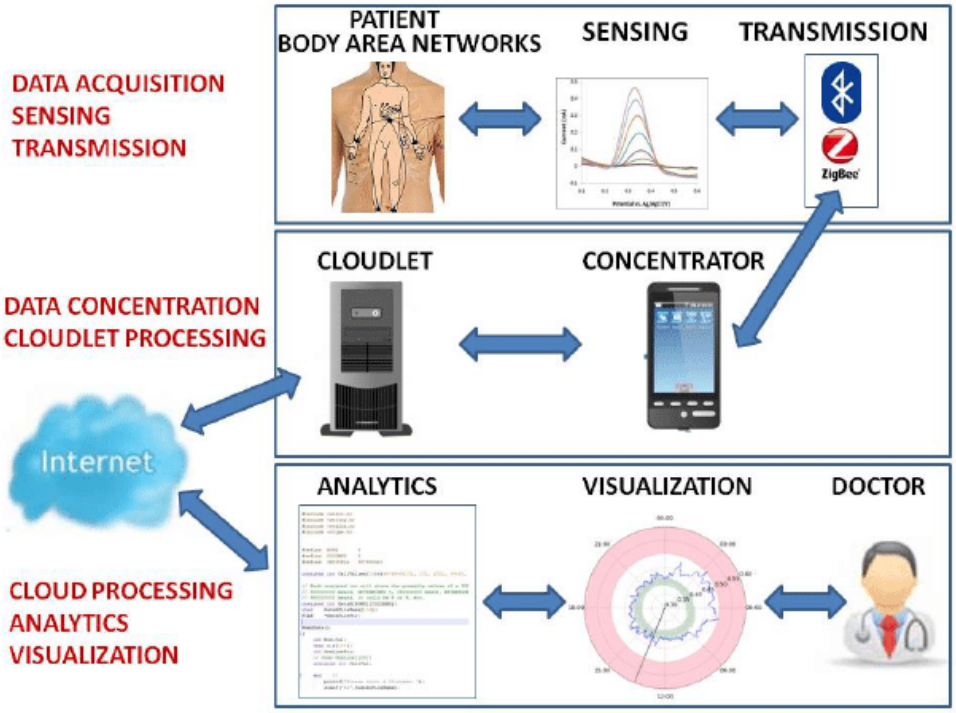
2.6.4. Έξυπνος χώρος στάθμευσης

Σε αυτή τη περίπτωση χρήσης υπάρχει ασύρματος αισθητήρας (ή συνδεδεμένο αντικείμενο) σε κάθε σημείο στάθμευσης. Εάν ένα πάρκο αυτοκινήτων ή εάν ένα παρκαρισμένο όχημα εγκαταλείψει ένα σημείο στάθμευσης, ο αισθητήρας στο σημείο στάθμευσης στέλνει μια ειδοποίηση σε ένα διακομιστή διαχείρισης. Με τη συλλογή πληροφοριών σχετικά με την κατοχή του χώρου στάθμευσης, ο διακομιστής μπορεί να παρέχει πληροφορίες για κενές θέσεις στάθμευσης στους οδηγούς μέσω πλατφορμών απεικόνισης, όπως έξυπνα τηλέφωνα, διεπαφές ανθρώπινων μηχανών (HMI) ή διαφημιστικών πινακίδων οχημάτων. Οι πληροφορίες αυτές θα επιτρέψουν επίσης στο δημοτικό συμβούλιο να επιβάλει πρόστιμα σε περίπτωση παραβίασης στάθμευσης [16]. Η τεχνολογία αναγνώρισης ραδιοσυχνότητας (RFID) είναι αυτοματοποιημένη και μπορεί να είναι πολύ χρήσιμη για τα συστήματα αναγνώρισης οχημάτων. Τα οχήματα

αναγνωρίζονται και τα τέλη στάθμευσης παρτίδας συλλέγονται αυτόματα μέσω αυτού του συστήματος [11]. Όσον αφορά τις απαιτήσεις υλικού, με τη χρήση αναγνωστών RFID, μπορούν να επιτευχθούν φραγμοί, έλεγχος στάθμευσης παρτίδας και έλεγχο ελέγχου. Με αυτό τον τρόπο, σε αντίθεση με τις παραδοσιακές λειτουργίες στάθμευσης παρτίδας που ελέγχονται από το προσωπικό, μπορεί να αναπτυχθεί ένα μη επανδρωμένο, αυτοματοποιημένο σύστημα ελέγχου και αναγνώρισης οχημάτων όπως περιγράφεται στο [11]. Η ανάπτυξη των δικτύων ad hoc οχημάτων (VANETs) [22] μαζί με την πρόοδο και την ευρεία ανάπτυξη τεχνολογιών ασύρματων επικοινωνιών, οδηγεί πολλά μεγάλα εργοστάσια αυτοκινήτων και βιομηχανίες τηλεπικοινωνιών να προσαρμόζουν ολοένα και περισσότερο τα αυτοκίνητά τους με συσκευές επικοινωνίας μονάδας επί οχήματος (OBU). Αυτό επιτρέπει σε διαφορετικά αυτοκίνητα να επικοινωνούν μεταξύ τους καθώς και με την οδική υποδομή. Έτσι, οι εφαρμογές που παρέχουν πληροφορίες σχετικά με την κατοχή χώρου στάθμευσης ή οδηγών σε άδειους χώρους στάθμευσης καθίστανται δυνατές μέσω οδικών επικοινωνιών [13].

2.6.5. Έξυπνη υγεία

Ένα ασύρματο δίκτυο χώρου σώματος (WBAN: Wireless Body Area Network), το οποίο βασίζεται σε μια χαμηλού κόστους ασύρματη τεχνολογία δικτύου αισθητήρων, θα μπορούσε να ωφελήσει σημαντικά τα συστήματα παρακολούθησης ασθενών σε νοσοκομεία, οικιακά και εργασιακά περιβάλλοντα [24]. Οι μικροσκοπικοί αισθητήρες μπορούν να ενσωματωθούν μέσα στο σώμα ή να τοποθετηθούν στην επιφάνεια του σώματος. Οι αισθητήρες επικοινωνούν με ιατρικές συσκευές που χρησιμοποιούν διαφορετικές τεχνολογίες WPAN (ZigBee, 6LowPAN, CoAP, κλπ.). Οι αισθητήρες είναι επίσης σε θέση να μετρούν διάφορες πληροφορίες φυσιολογικών παραμέτρων (π.χ. ροή αίματος, αναπνευστικό ρυθμό, πίεση αίματος, PH αίματος, θερμοκρασία σώματος κλπ.), οι οποίες συλλέγονται και αναλύονται από απομακρυσμένους διακομιστές (βλ. εικόνα 6)



Εικόνα 6. Συστατικά ενός απομακρυσμένου συστήματος παρακολούθησης ασθενών που βασίζεται σε μια αρχιτεκτονική IoT-Cloud [25]

Η απαίτηση φθοράς θέτει φυσικούς περιορισμούς στο σχεδιασμό αυτών των αισθητήρων. Οι αισθητήρες πρέπει να είναι ελαφροί, μικρές και δεν πρέπει να παρεμποδίζουν τις κινήσεις και την κινητικότητα του ασθενούς. Επιπλέον, επειδή οι αισθητήρες πρέπει να λειτουργούν σε μικρές μπαταρίες που περιλαμβάνονται στη φορητή συσκευασία, πρέπει να είναι υψηλής ενεργειακής απόδοσης [15].

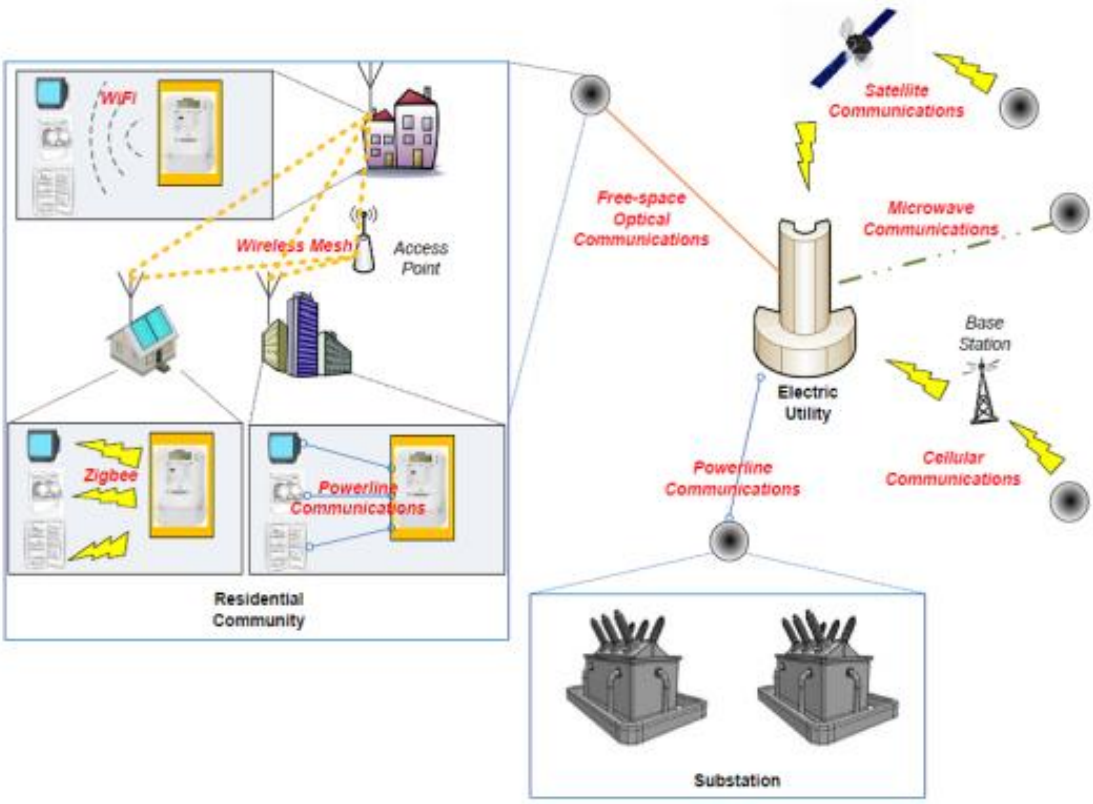
2.6.6. Σύστημα πλοήγησης αστικών λεωφορείων

Το UBN βασίζεται σε μια αρχιτεκτονική IoT που χρησιμοποιεί ένα σύνολο από κατανεμημένα συστατικά λογισμικού και υλικού που είναι στενά ενσωματωμένα στο σύστημα διαύλου. Το σύστημα UBN που αναπτύσσεται στη Μαδρίτη της

Ισπανίας αποτελείται από τρία βασικά στοιχεία: 1) το αστικό σύστημα αστικών λεωφορείων με δίκτυα με λεωφορεία εξοπλισμένα με WiFi, 2) την εφαρμογή πλοήγησης UBN για τους αναβάτες λεωφορείων και 3) -time πληροφορίες σχετικά με την πληρότητα από λεωφορεία που εκτελούν δρομολόγια σε διάφορες διαδρομές στη Μαδρίτη [16].

2.6.7. Έξυπνο δίκτυο

Το έξυπνο δίκτυο χρησιμοποιεί νέες τεχνολογίες, όπως έξυπνους και αυτόνομους ελεγκτές, προηγμένο λογισμικό διαχείρισης δεδομένων και αμφίδρομες επικοινωνίες μεταξύ των εταιρειών παροχής ενέργειας και των καταναλωτών, για τη δημιουργία ενός αυτοματοποιημένου και κατανεμημένου δικτύου προηγμένης παροχής ενέργειας [17]. Χρησιμοποιώντας την υποδομή για την ανίχνευση και τη μετάδοση πληροφοριών για το έξυπνο δίκτυο, η τεχνολογία IoT, όταν εφαρμοστεί στο δίκτυο ηλεκτρικής ενέργειας, θα διαδραματίσει σημαντικό ρόλο στην αποδοτική παραγωγή, διανομή, μεταφορά και κατανάλωση ενέργειας [18].



Εικόνα 7. Αρχιτεκτονική έξυπνου δικτύου [17]

2.6.8. Αυτόνομη οδήγηση

Σε μια έξυπνη πόλη, οι αυτόνομες τεχνολογίες οδήγησης θα είναι συνώνυμες με την εξοικονόμηση χρόνου για τον χρήστη. Αυτή η τεχνολογία θα βοηθήσει στην επιτάχυνση της ροής της κυκλοφορίας σε μια πόλη και θα εξοικονομήσει σχεδόν το 60% [19] χώρου στάθμευσης, σταθμεύοντας τα αυτοκίνητα πιο κοντά ο ένας στον άλλο. Σύμφωνα με την Nissan-Renault, τα αυτόνομα οχήματα θα κυκλοφορήσουν στην αγορά το 2020. Αυτά τα "αυτόματα αυτοκίνητα" κυκλοφορούν αυτόνομα σε περίπου 30 με 50 km / h ως το μοντέλο Renault Next Two-autonomous του γαλλικού κατασκευαστή [20]. Το 2017, η Volvo θα πειραματιστεί με εκατό αυτόνομα αυτοκίνητα που οδηγούν σε πραγματικές συνθήκες κυκλοφορίας στους δρόμους του Γκέτεμποργκ, του Λονδίνου και αρκετών κινεζικών πόλεων. Μέσω ενός συνδυασμού ραντάρ, φωτογραφικών μηχανών και αισθητήρων υπερήχων που βρίσκονται γύρω από το αυτοκίνητο, ένα αυτόνομο αυτοκίνητο μπορεί να ανιχνεύσει ανωμαλίες παντού και να

ενεργοποιήσει μια ειδοποίηση που ενεργοποιεί αυτόματα τα φρένα έκτακτης ανάγκης για την πρόληψη ατυχημάτων ή συγκρούσεων. Το Ευφυές Σύστημα Μεταφορών θα μπορούσε να μας επιτρέψει να υπολογίσουμε την καλύτερη διαδρομή σε πραγματικό χρόνο, συνδέοντας διαφορετικούς τρόπους μεταφοράς για να εξοικονομήσουμε χρόνο και να μειώσουμε τις εκπομπές άνθρακα.

2.7. IoT πλατφόρμες

Η σημαντική αύξηση της εξάπλωσης του Διαδικτύου οδήγησε στην εμφάνιση πλατφορμών Διασύνδεσης Διαδικτύου που υποστηρίζουν:

• Εύκολη ενσωμάτωση νέων συσκευών και υπηρεσιών.

• Επικοινωνία μεταξύ συσκευών (αντικείμενα και διακομιστές).

• Διαχείριση διαφόρων συσκευών και πρωτοκόλλων επικοινωνίας.

• Μετάδοση ροών δεδομένων και δημιουργία νέων εφαρμογών.

• Διαλειτουργικότητα μεταξύ στοιχείων, αντικειμένων, δεδομένων σύννεφου και εφαρμογών λογισμικού.

• Επεκτασιμότητα της υποδομής του Διαδικτύου.

Ανάλογα με το επίπεδο των παρεχόμενων υπηρεσιών, οι πλατφόρμες IoT μπορούν να χωριστούν σε:

1. Backends υποδομής-ως-υπηρεσιών: παρέχουν χώρο φιλοξενίας και επεξεργασίας για εφαρμογές και υπηρεσίες, π.χ. IBM Bluemix.

2. Πλατφόρμες συνδεσιμότητας M2M: εστιάζουν μόνο στη συνδεσιμότητα αντικειμένων IoT μέσω τηλεπικοινωνιακών δικτύων και πρωτοκόλλων, π.χ. Comarch και AirVantage

3. Ειδικές πλατφόρμες λογισμικού: πολλές εταιρείες πωλούν την ιδιόκτητη τεχνολογία τους, η οποία περιλαμβάνει το υλικό και το backend λογισμικού, π.χ. Google Nest

4. Επεκτάσεις λογισμικού για επιχειρήσεις: Ορισμένες εταιρείες λογισμικού και λειτουργικού συστήματος, όπως τα Windows και η Apple, επιτρέπουν όλο και περισσότερο την ενσωμάτωση συσκευών IoT, όπως smartphones, συνδεδεμένα ρολόγια και οικιακές συσκευές. Σύμφωνα με [3], τα κύρια χαρακτηριστικά που πρέπει να επιτύχει μια πλατφόρμα IoT είναι:

• Δικτύωση.

• Διαχείριση συσκευής.

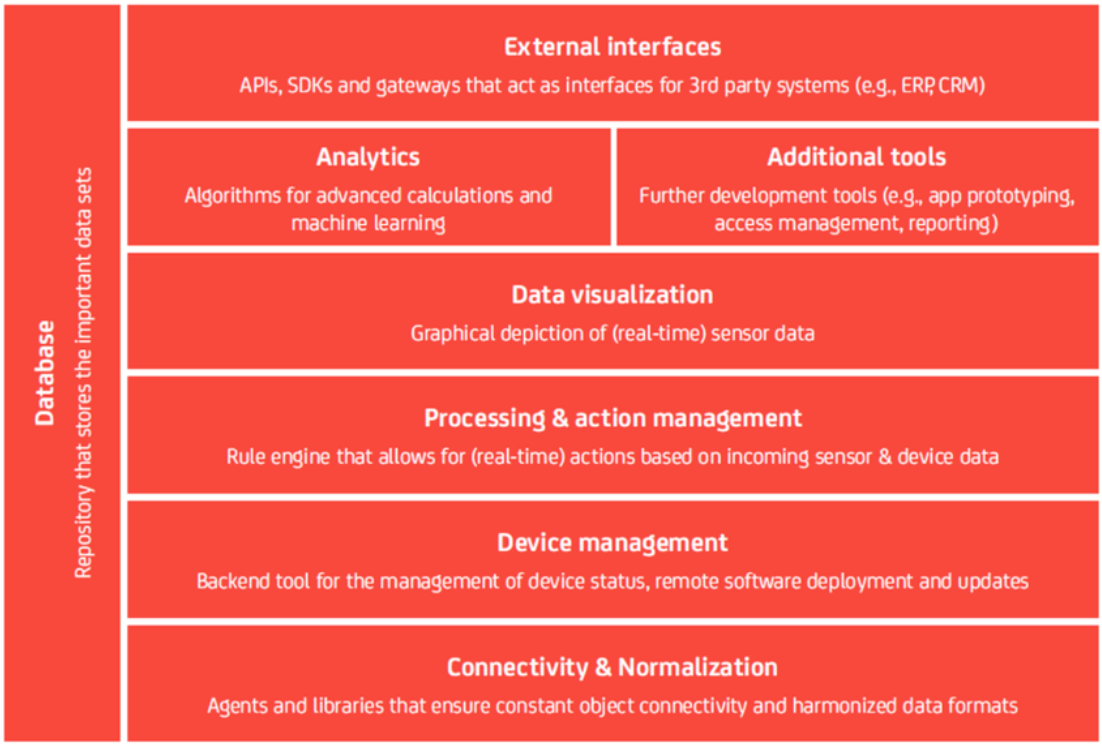
• Ασφάλεια.

• Πρωτόκολλα συλλογής δεδομένων.

• Analytics.

• Υποστήριξη για απεικονίσεις.

Με βάση αυτά τα χαρακτηριστικά, οι συγγραφείς στο [23] πρότειναν μια στοίβα για την αρχιτεκτονική πλατφόρμας IoT όπως φαίνεται στο Σχήμα 8.



Εικόνα 8. Κύρια στοιχεία μιας Πλατφόρμας Ενεργοποίησης Εφαρμογών IoT [23]

Όπως αναφέρθηκε προηγουμένως, ο αριθμός των πλατφορμών του Διαδικτύου αυξάνεται με ταχείς ρυθμούς. Σύμφωνα με [14], αυτή η αγορά θα φτάσει το 1 δισεκατομμύριο δολάρια το 2019.

3. Ζητήματα ιδιωτικότητας στις έξυπνες πόλεις

Η ασφάλεια του IoT αποτελεί σημαντική πρόκληση για τη βιωσιμότητα και την ανταγωνιστικότητα των εταιρειών και των διοικήσεων. Η Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ (FTC) επισήμανε σε μια έκθεση [6] ότι η προγραμματισμένη ανάπτυξη της τεχνολογίας IoT θα ανοίξει διάφορα θέματα ασφάλειας και απορρήτου για τους χρήστες IoT που πρέπει να αντιμετωπιστούν ή να επιλυθούν. Για πολλές από αυτές τις κρίσιμες εφαρμογές IoT, η χρήση εσφαλμένων ή κακόβουλων δεδομένων μπορεί να έχει σοβαρές συνέπειες. Οι συμβατικές λύσεις ασφαλείας όπως ο έλεγχος ταυτότητας, η εμπιστευτικότητα και η ακεραιότητα των δεδομένων είναι κρίσιμες για αντικείμενα, δίκτυα και εφαρμογές IoT. Εάν τα αντικείμενα IoT έχουν αρκετή ισχύ μνήμης και επεξεργασίας, ενδέχεται να ισχύουν τα υπάρχοντα πρωτόκολλα και αλγόριθμοι ασφαλείας, αλλά λόγω των περιορισμών πόρων των αντικειμένων IoT, αυτές οι υπάρχουσες λύσεις ασφαλείας είναι πολύ δαπανηρές για τα αντικείμενα στο IoT.

Τα ζητήματα ασφάλειας παραμένουν μεγάλα εμπόδια στην υιοθέτηση και ανάπτυξη του IoT παγκοσμίως. Με άλλα λόγια, οι χρήστες δεν θα υιοθετήσουν πλήρως το IoT εάν δεν υπάρχει εγγύηση ότι θα προστατεύσει το απόρρητό τους. Πράγματι, το IoT είναι πολύ ευάλωτο σε επιθέσεις για πολλούς λόγους: (1) συνήθως, τα αντικείμενα περνούν το μεγαλύτερο μέρος του χρόνου τους χωρίς επίβλεψη, γεγονός που καθιστά τις φυσικές επιθέσεις σε αυτά σχετικά εύκολες, (2) οι περισσότερες επικοινωνίες είναι ασύρματες. Κατά συνέπεια, τα ανταλλαγμένα μηνύματα ενδέχεται να υπόκεινται σε υποκλοπή, κακόβουλη δρομολόγηση, παραβίαση μηνυμάτων και άλλα ζητήματα ασφαλείας που μπορούν να επηρεάσουν την ασφάλεια ολόκληρου του IoT και (3) πολλαπλοί τύποι αντικειμένων, όπως οι ετικέτες RFID, έχουν περιορισμένους πόρους από άποψη ενέργειας και υπολογισμού. Τα συνδεδεμένα αντικείμενα έχουν τις δικές τους ευπάθειες που σχετίζονται με τις συγκεκριμένες δυνατότητές τους. Αυτές οι νέες ευπάθειες προκαλούνται λόγω των παρακάτω λόγων:

• Πολλοί διαφορετικοί τύποι λειτουργικών συστημάτων χρησιμοποιούνται από τα συνδεδεμένα αντικείμενα και δεν είναι πάντα γνωστοί. Ο κωδικός ενός

λειτουργικού συστήματος είναι συνήθως της τάξης των δεκάδων χιλιάδων ή εκατομμυρίων γραμμών κώδικα. Ως εκ τούτου, η πιθανότητα να έχουν ευπάθειες είναι υψηλή.

• Δεν υπάρχουν γνωστά πρότυπα ασφαλείας.

• Υπάρχουν πολλά ιδιόκτητα πρωτόκολλα.

• Οι αρχιτεκτονικές είναι πολύ ετερογενείς και η φυσική ασφάλεια συχνά διακυβεύεται.

• Η ενημέρωση ακεραιότητας λογισμικού συνδεδεμένων αντικειμένων δεν είναι εγγυημένη.

• Η ασφάλεια των αποθηκευμένων δεδομένων δεν είναι εγγυημένη.

• Οι περιορισμένοι πόροι ενός συνδεδεμένου αντικειμένου εμποδίζουν τη χρήση κλασικών κρυπτογραφικών συναρτήσεων και πρωτοκόλλων ασφαλείας.

Τα ζητήματα ασφάλειας δεδομένων μπορούν να συνοψιστούν σε εμπιστευτικότητα δεδομένων, γνησιότητα δεδομένων και ακεραιότητα δεδομένων. Οι κρυπτογραφικές τεχνικές είναι οι καλύτερες λύσεις για την υποστήριξη αυτών των αναγκών ασφαλείας [67].

3.1. Εμπιστευτικότητα δεδομένων, ακεραιότητα και έλεγχος ταυτότητας

Πολλά σενάρια εφαρμογών IoT απαιτούν υψηλή ασφάλεια δεδομένων, συμπεριλαμβανομένης της εμπιστευτικότητας των δεδομένων και της ακεραιότητας των δεδομένων. Αυτή η απαίτηση μπορεί να επιλυθεί με κρυπτογράφηση δεδομένων. Οι αλγόριθμοι κρυπτογράφησης δεδομένων χωρίζονται σε δύο κατηγορίες: (1) συμμετρικοί αλγόριθμοι κρυπτογράφησης και (2) αλγόριθμοι κρυπτογράφησης δημόσιου κλειδιού. Οι τελευταίοι καταναλώνουν περισσότερους πόρους που τους καθιστούν δύσκολο να εφαρμοστούν σε αντικείμενα με περιορισμένη ισχύ και ενεργειακούς πόρους. Αντίθετα, οι συμμετρικοί αλγόριθμοι είναι κατάλληλοι για τέτοιες συσκευές και χρησιμοποιούνται ευρέως σε αυτό το πλαίσιο [67]. Ωστόσο, υποφέρουν από αρκετά μειονεκτήματα: (1) τα συμμετρικά πρωτόκολλα ανταλλαγής κλειδιών τέτοιων κρυπτοσυστημάτων είναι πολύ περίπλοκα που περιορίζουν την επεκτασιμότητα της υποδομής [7] και (2) υποφέρουν από το πρόβλημα εμπιστευτικότητας των κοινών κλειδιών.

Πράγματι, όσο υψηλότερος είναι ο αριθμός των αντικειμένων, τόσο μεγαλύτερος είναι ο κίνδυνος ασφάλειας. Εάν ένα κλειδί παραβιάζεται, όλες οι επικοινωνίες συστήματος διακυβεύονται. Ως λύση, το σύστημα μπορεί να χωριστεί σε πολλές ομάδες και ένα διαφορετικό συμμετρικό κλειδί χρησιμοποιείται σε κάθε ομάδα. Ωστόσο, παραμένει ο κίνδυνος, καθώς εάν ένα κλειδί παραβιαστεί, οι επικοινωνίες με την ομάδα διακυβεύονται επίσης. Για την αντιμετώπιση αυτού του προβλήματος, οι ερευνητές έχουν εξετάσει αλγόριθμους κρυπτογράφησης δημόσιου κλειδιού. Σε αυτήν τη λύση, κάθε αντικείμενο διαθέτει ένα ζευγάρι δημόσιων και ιδιωτικών κλειδιών. Κάθε αντικείμενο διατηρεί το ιδιωτικό κλειδί του, ενώ ο σταθμός βάσης αποθηκεύει τα δημόσια κλειδιά όλων των αντικειμένων. Στην πραγματικότητα, οι κύριες προτάσεις [8] αλγορίθμων κρυπτογράφησης δημόσιου κλειδιού κατάλληλες για IoT [17] περιλαμβάνουν το Σχέδιο Rabin [71], το NtruEncrypt [72] και την Κρυπτογραφία Ελλειπτικής Καμπύλης (ECC) [73]. Το ECC προσφέρει καλή επεκτασιμότητα, χωρίς πολύπλοκο πρωτόκολλο διαχείρισης κλειδιών. Ωστόσο, η εφαρμογή αυτών των αλγορίθμων στο περιβάλλον IoT διερευνάται ακόμη.

Επιπλέον, δεν ισχύουν για όλους τους τύπους αντικειμένων, ιδίως ετικέτες RFID, όπου το πρόβλημα του προβλήματος των περιορισμένων πόρων παραμένει ένα δύσκολο ζήτημα. Επιπλέον, η λύση κρυπτογράφησης δημόσιου κλειδιού υποφέρει από ζητήματα εμπιστοσύνης. Πράγματι, ένας σταθμός βάσης που διαθέτει δημόσια κλειδιά δεν μπορεί να αποδείξει ότι τα αντικείμενα είναι πραγματικά αυτά που προσποιούνται.

3.2. Βασική διαχείριση

Η βασική διαχείριση είναι ένα άλλο σημαντικό ζήτημα στο IoT. Παίζει ζωτικό ρόλο στην εφαρμογή διαφόρων λύσεων ασφαλείας. Η διαχείριση κλειδιών περιλαμβάνει πολλά βήματα που περιλαμβάνουν δημιουργία κλειδιών, διανομή, αποθήκευση, ενημέρωση και καταστροφή. Ένα σημαντικό στοιχείο του κύκλου διαχείρισης κλειδιών είναι η διανομή κλειδιών που περιλαμβάνει ασφαλή μετάδοση και διανομή σε νόμιμους χρήστες (1) δημόσιων κλειδιών και κοινών μυστικών στην περίπτωση ασύμμετρης κρυπτογράφησης και (2) μυστικών κλειδιών στην περίπτωση συμμετρικής κρυπτογράφησης. Πολλά έργα έχουν προτείνει βασικά συστήματα διαχείρισης προσαρμοσμένα σε τεχνολογίες που αποτελούν το οικοσύστημα IoT, και πιο συγκεκριμένα για το WSN τα τελευταία χρόνια. Χρησιμοποιούν συμμετρική διαχείριση κλειδιών, δημόσια κλειδιά, συντομευμένα (ένα συντομευμένο πιστοποιητικό όπου ορισμένα πεδία έχουν αφαιρεθεί) ή έμμεσα πιστοποιητικά. Ωστόσο, αυτές οι λύσεις σχεδιάστηκαν κυρίως για WSN και δεν είναι κατάλληλες για όλους τους τύπους αντικειμένων. Κατά συνέπεια, ο σχεδιασμός ελαφρών συστημάτων διαχείρισης κλειδιών προσαρμοσμένων στο περιβάλλον IoT και τα σενάρια εφαρμογής του παραμένει βασικό ζήτημα που πρέπει να λυθεί στο μέλλον.

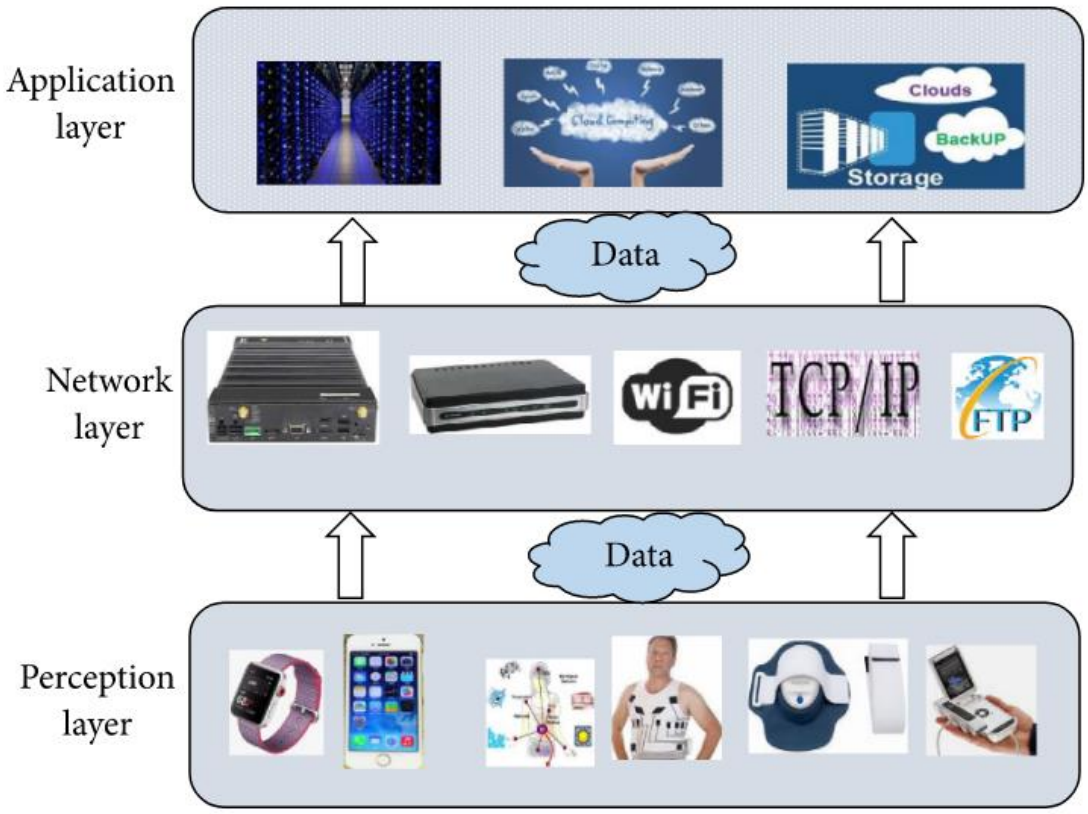
3.3. Διαχείριση εμπιστοσύνης

Πρέπει να αναπτύξουμε και να εφαρμόσουμε μηχανισμούς διαχείρισης εμπιστοσύνης στο IoT. Πράγματι, σε πολλά σενάρια, το δίκτυο βασίζεται στη συνεργασία όλων των κόμβων. Η ευπάθεια ενός μόνο κόμβου μπορεί να έχει σοβαρές συνέπειες σε ολόκληρο το δίκτυο. Πράγματι, εάν ένας εισβολέας καταφέρει να συμβιβάσει ή να προσθέσει ένα ή περισσότερα αντικείμενα στο δίκτυο, ο εισβολέας μπορεί να παρέχει ψεύτικες ή εσφαλμένες πληροφορίες, οι οποίες μπορούν στη συνέχεια να επηρεάσουν τη συνεργασία κόμβων, την επεξεργασία δεδομένων και το αποτέλεσμα που παρέχεται στον τελικό χρήστη. Έτσι, η αξιοπιστία κάθε κόμβου είναι το κλειδί για την εξασφάλιση ακριβούς και αξιόπιστης παροχής υπηρεσιών δικτύου. Τα τρέχοντα συστήματα διαχείρισης εμπιστοσύνης όπως αυτά που προτείνονται στο [74] [78] παρέχουν μόνο επαλήθευση της συνέπειας και της εγκυρότητας των δεδομένων, αλλά δεν μπορούν να εγγυηθούν τον έλεγχο ταυτότητας των αντικειμένων. Επιπλέον, αυτά τα προηγούμενα προτεινόμενα σχήματα δεν είναι πλήρως προσαρμόσιμα στο πλαίσιο IoT. Κατά συνέπεια, απαιτείται περισσότερη έρευνα για την ανάπτυξη ελαφρών τεχνικών και πρωτοκόλλων διαχείρισης εμπιστοσύνης που είναι ιδιαίτερα κατάλληλα για σενάρια IoT στο μέλλον.

4. Ασφάλεια και απόρρητο στο ιατρικό Διαδίκτυο των πραγμάτων

Το Medical Internet of Things είναι η ομάδα συσκευών που είναι συνδεδεμένες στο Διαδίκτυο, για την εκτέλεση των διαδικασιών και των υπηρεσιών που υποστηρίζουν την υγειονομική περίθαλψη. Το MIoT έχει αναδειχθεί ως μια νέα τεχνολογία για την ηλεκτρονική υγειονομική περίθαλψη που συλλέγει ζωτικές παραμέτρους του σώματος των ασθενών και παρακολουθεί τις παθολογικές τους λεπτομέρειες από μικρές φορητές συσκευές ή εμφυτεύσιμους αισθητήρες. Το MIoT έχει δείξει μεγάλες δυνατότητες στην παροχή καλύτερης εγγύησης για την υγεία των ανθρώπων και υποστηρίζει ένα ευρύ φάσμα εφαρμογών από εμφυτεύσιμα ιατρικά βοηθήματα έως ασύρματο δίκτυο περιοχής σώματος (WBAN). Γενικά, η δομή MIoT αποτελείται από τρία επίπεδα: το επίπεδο αντίληψης, το επίπεδο δικτύου και το επίπεδο εφαρμογής, όπως φαίνεται στο Σχήμα 9. Το κύριο καθήκον του επιπέδου αντίληψης είναι η συλλογή δεδομένων υγειονομικής περίθαλψης με μια ποικιλία συσκευών.

Το επίπεδο δικτύου, το οποίο αποτελείται από ενσύρματο και ασύρματο σύστημα και ενδιάμεσο λογισμικό, επεξεργάζεται και μεταδίδει την είσοδο που λαμβάνεται από το επίπεδο αντίληψης που υποστηρίζεται από τεχνολογικές πλατφόρμες. Τα καλά σχεδιασμένα πρωτόκολλα μεταφοράς όχι μόνο βελτιώνουν την απόδοση μετάδοσης και μειώνουν την κατανάλωση ενέργειας, αλλά διασφαλίζουν επίσης την ασφάλεια και την ιδιωτικότητα. Το επίπεδο εφαρμογής ενσωματώνει τους πόρους ιατρικής πληροφόρησης για να παρέχει εξατομικευμένες ιατρικές υπηρεσίες και να ικανοποιεί τις ανάγκες των τελικών χρηστών, σύμφωνα με την πραγματική κατάσταση του πληθυσμού-στόχου και τη ζήτηση υπηρεσίας.



Εικόνα 9. Δομή του Ιατρικού Διαδικτύου των πραγμάτων.

4.1. Απαίτηση ασφάλειας και απορρήτου

Παρόλο που η πλειονότητα των οργανισμών υγειονομικής περίθαλψης δεν ξοδεύει αρκετούς πόρους για την προστασία της ασφάλειας και της ιδιωτικής ζωής [14], δεν υπάρχει αμφιβολία ότι η ασφάλεια και η ιδιωτικότητα διαδραματίζουν βασικό ρόλο στο MIoT. Οι συσκευές MIoT παράγουν έναν ολοένα και μεγαλύτερο όγκο δεδομένων όλο και περισσότερο σε πραγματικό χρόνο, τα οποία είναι ιδιαίτερα ευαίσθητα. Αφενός, η καταστροφή της ασφάλειας του ιατρικού συστήματος ή του δικτύου θα μπορούσε να προκαλέσει καταστροφικές συνέπειες. Από την άλλη πλευρά, οι πληροφορίες απορρήτου του ασθενούς υπάρχουν σε όλα τα στάδια της συλλογής δεδομένων, της μετάδοσης δεδομένων, της αποθήκευσης στο cloud και της αναδημοσίευσης δεδομένων. Κατά την ανάπτυξη ιατρικών συστημάτων ασφάλειας και

απορρήτου στο Διαδίκτυο, πρέπει να ληφθούν υπόψη οι ακόλουθες τέσσερις απαιτήσεις.

4.1.1. Ακεραιότητα δεδομένων

Η ακεραιότητα των δεδομένων αναφέρεται στο γεγονός ότι όλες οι τιμές δεδομένων ικανοποιούν σημασιολογικά πρότυπα χωρίς παράνομη παραβίαση. Περιλαμβάνει δύο επίπεδα ακρίβειας και αξιοπιστίας. Η ακεραιότητα των δεδομένων μπορεί να χωριστεί σε τέσσερις κατηγορίες, δηλαδή, ακεραιότητα οντότητας, ακεραιότητα τομέα, ακεραιότητα αναφοράς και ακεραιότητα καθορισμένη από τον χρήστη, οι οποίες μπορούν να διατηρηθούν από ξένα κλειδιά, περιορισμούς, κανόνες και κανόνες. [47]

4.1.2. Ευχρηστία δεδομένων

Η χρηστικότητα των δεδομένων χρειάζεται για να διασφαλιστεί ότι τα δεδομένα ή τα συστήματα δεδομένων μπορούν να χρησιμοποιηθούν από εξουσιοδοτημένους χρήστες. Τα μεγάλα δεδομένα δεν προσφέρουν μόνο μεγάλα οφέλη, αλλά και κρίσιμες προκλήσεις, όπως βρώμικα δεδομένα και μη τυπικά δεδομένα. Επιπλέον, η καταστροφή δεδομένων ή η απώλεια δεδομένων που προκαλείται από μη εξουσιοδοτημένη πρόσβαση επίσης καταστρέφει περαιτέρω τη χρηστικότητα των δεδομένων. [48]

4.1.3. Έλεγχος δεδομένων

Ο έλεγχος της πρόσβασης στα ιατρικά δεδομένα είναι ένα αποτελεσματικό μέσο για την παρακολούθηση της χρήσης πόρων και ένα κοινό μέτρο για την εύρεση και παρακολούθηση ανώμαλων συμβάντων. Επιπλέον, οι πάροχοι υπηρεσιών cloud παίζουν συνήθως μη αξιόπιστους ρόλους, οι οποίοι απαιτούν λογικές

μεθόδους ελέγχου. Το περιεχόμενο ελέγχου περιλαμβάνει γενικά χρήστες, παρόχους υπηρεσιών cloud, αρχεία πρόσβασης και λειτουργίας. [47]

4.1.4. Απόρρητο πληροφοριών ασθενών

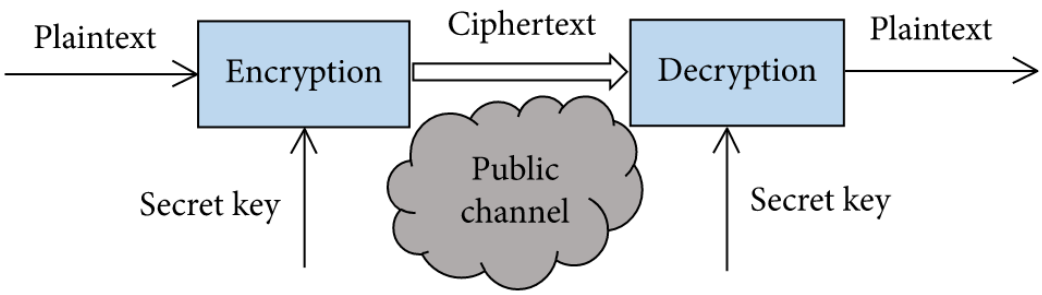
Οι πληροφορίες για τον ασθενή μπορούν να υποδιαιρεθούν σε δύο κατηγορίες: γενικές καταγραφές και ευαίσθητα δεδομένα. Τα ευαίσθητα δεδομένα, τα οποία μπορούν επίσης να ονομαστούν απόρρητα των ασθενών, περιλαμβάνουν διανοητική κατάσταση, σεξουαλικό προσανατολισμό, σεξουαλική λειτουργία, μολυσματικές ασθένειες, κατάσταση γονιμότητας, τοξικομανία, γενετικές πληροφορίες και πληροφορίες ταυτότητας. Πρέπει να διασφαλίσουμε ότι τα ευαίσθητα δεδομένα δεν θα διαρρεύσουν σε μη εξουσιοδοτημένους χρήστες, ή ακόμα και αν τα δεδομένα υποκλαπούν, οι πληροφορίες που εκφράζονται δεν μπορούν να γίνουν κατανοητές από μη εξουσιοδοτημένους χρήστες. [46]

4.2. Υφιστάμενες λύσεις

Δεδομένου ότι οι συσκευές MIoT δεν διαθέτουν επαρκή μνήμη, υπολογισμό και δυνατότητες επικοινωνίας, απαιτούν μια ισχυρή και επεκτάσιμη υπολογιστική υψηλής απόδοσης και υποδομή μαζικής αποθήκευσης για επεξεργασία σε πραγματικό χρόνο και αποθήκευση δεδομένων. Επί του παρόντος, τα περισσότερα ιδρύματα MIoT αποθηκεύουν τα συλλεγμένα ιατρικά δεδομένα και αναπτύσσουν τους διακομιστές εφαρμογών τους στο cloud. Οι συσκευές μπορούν να εκφορτώσουν τις εργασίες υγειονομικής περίθαλψης στο cloud ανάλογα. Οι υπηρεσίες cloud μέσω της ελαστικότητάς τους και της δυνατότητάς τους να έχουν πρόσβαση σε κοινόχρηστους πόρους και σε κοινές υποδομές με πανταχού παρόν και διάχυτο τρόπο διευκολύνουν μια πολλά υποσχόμενη λύση για την αποτελεσματική διαχείριση των διαδεδομένων δεδομένων περίθαλψης.

4.2.1. Κρυπτογράφηση δεδομένων

Η κρυπτογραφία είναι μια τεχνολογία ασφάλειας για την ανταλλαγή πληροφοριών και την επικοινωνία σύμφωνα με τους συμφωνημένους κανόνες [15]. Όπως φαίνεται στο Σχήμα 10, το απλό κείμενο, επίσης γνωστό ως το αρχικό μήνυμα, κρυπτογραφείται σε κρυπτότυπο από τον αλγόριθμο κρυπτογράφησης. Μέσω του δημόσιου καναλιού, το μήνυμα μεταδίδεται από τον αποστολέα στον παραλήπτη. Το μήνυμα στη συνέχεια αποκρυπτογραφείται σε απλό κείμενο.



Εικόνα 10. Κοινό μοντέλο κρυπτογράφησης και αποκρυπτογράφησης δεδομένων.

Η γενική κρυπτογράφηση δεδομένων μπορεί να εφαρμοστεί σε τρία επίπεδα επικοινωνίας: κρυπτογράφηση συνδέσμου, κρυπτογράφηση κόμβων και κρυπτογράφηση από άκρο σε άκρο. Για οποιονδήποτε ενδιάμεσο κόμβο σε κρυπτογράφηση συνδέσμου, το μήνυμα που λαμβάνεται από τον προηγούμενο σύνδεσμο θα αποκρυπτογραφηθεί σε απλό κείμενο και στη συνέχεια το απλό κείμενο θα κρυπτογραφηθεί σε κρυπτότυπο χρησιμοποιώντας το μυστικό κλειδί του επόμενου συνδέσμου. Ωστόσο, σε αντίθεση με την κρυπτογράφηση συνδέσμων, η κρυπτογράφηση κόμβων δεν επιτρέπει μηνύματα σε μορφή απλού κειμένου στον κόμβο δικτύου. Επομένως, η κρυπτογράφηση κόμβων μπορεί να παρέχει υψηλή ασφάλεια για δεδομένα δικτύου. Όταν χρησιμοποιείτε

κρυπτογράφηση από άκρο σε άκρο, το μήνυμα δεν αποκρυπτογραφείται έως ότου μεταδοθεί στον προορισμό. Επειδή τα μηνύματα είναι πάντα παρόντα ως κρυπτογράφημα καθόλη τη διάρκεια της μετάδοσης, δεν υπάρχει διαρροή πληροφοριών ακόμη και αν ένας κόμβος είναι κατεστραμμένος. [46]

Για τη διασφάλιση των επικοινωνιών ηλεκτρονικής υγείας, τα πρωτόκολλα βασικής διαχείρισης διαδραματίζουν ζωτικό ρόλο στη διαδικασία ασφάλειας. Ωστόσο, πολύπλοκοι αλγόριθμοι κρυπτογράφησης ή πρωτόκολλα μετάδοσης μπορούν να επηρεάσουν σημαντικά τον ρυθμό μετάδοσης και ακόμη και να αποτύχουν στην εκτέλεση μετάδοσης δεδομένων. Επιπλέον, πρέπει να καταλαμβάνουν πολύτιμους ιατρικούς πόρους που δεν είναι διαθέσιμοι. Η σκληρή ισορροπία μεταξύ προστασίας ασφάλειας και κατανάλωσης ενέργειας του συστήματος πρέπει να λυθεί με επιστημονικό και προσεκτικό βήμα. Ο Πίνακας 4 δείχνει διάφορες προτάσεις κρυπτογράφησης δεδομένων στο MIoT.

Πίνακας 4. Μηχανισμοί ασφάλειας και απορρήτου και προτάσεις για κρυπτογράφηση δεδομένων.

Technologies	Application	Details
Key management scheme	Resource-constrained nodes	Solving the issue of the limited resources available through strong encryption and authentication means
Lightweight private algorithm; DES	Data transmission	Strong encryption considering the characteristic of IoT
Cloud computing	Monitoring the elder's biological data	Reducing the waste of medical resource
Authentication scheme	Mobile emergency medical systems	Guaranteeing the confidentiality of sensitive medical data

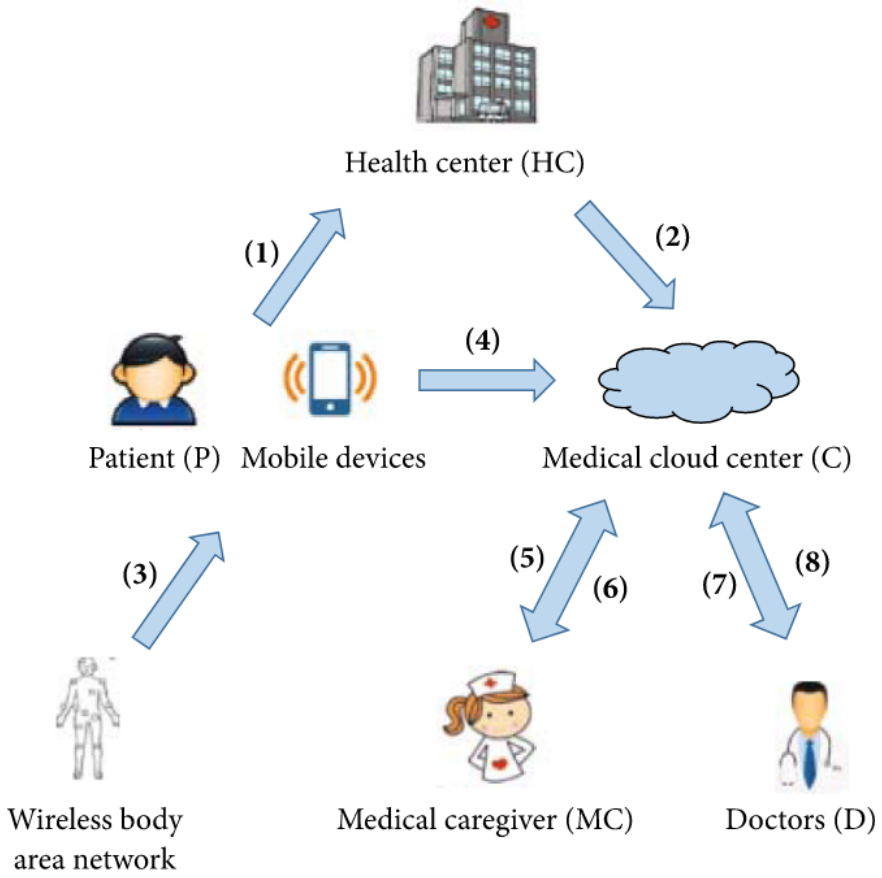
Λόγω των περιορισμένων διαθέσιμων πόρων και των ζητημάτων απορρήτου, τα ζητήματα ασφάλειας υπήρξαν σημαντικά εμπόδια στις εφαρμογές ηλεκτρονικής υγείας που παρέχουν διακριτική υποστήριξη για ηλικιωμένους και

αδύναμους ανθρώπους. Ο Abdmeziem και ο Tandjaoui [3] παρουσίασαν ένα ελαφρύ σύστημα διαχείρισης κλειδιών από άκρο σε άκρο, το οποίο διασφαλίζει την ανταλλαγή κλειδιών με ελάχιστη κατανάλωση πόρων. Στην πρότασή τους, το δίκτυο είναι ετερογενές που συνδυάζει κόμβους με διαφορετικές δυνατότητες. Ισχυρές μέθοδοι κρυπτογράφησης και μέσα ελέγχου ταυτότητας χρησιμοποιούνται για τη δημιουργία κλειδιών συνεδρίας για κόμβους με περιορισμό πόρων. Το προτεινόμενο πρωτόκολλο βασίζεται στη συνεργασία με την εκφόρτωση βαριών ασύμμετρων κρυπτογραφικών λειτουργιών σε ένα σύνολο τρίτων. Μέσω της ανάλυσης ασφάλειας, το σχέδιο μπορεί να παρέχει ισχυρά χαρακτηριστικά ασφαλείας, καθώς και την έλλειψη πόρων. [43]

Λαμβάνοντας υπόψη τα χαρακτηριστικά του IoT και της προστασίας της ιδιωτικής ζωής, οι Gong et al. συζήτησαν τα κύρια προβλήματα στο τρέχον σύστημα έξυπνης υγειονομικής περίθαλψης. Στη συνέχεια σχεδίασαν και ολοκλήρωσαν ένα πρωτότυπο σύστημα βασισμένο σε έναν ελαφρύ αλγόριθμο ιδιωτικού ομομορφισμού και έναν αλγόριθμο κρυπτογράφησης βελτιωμένο από το DES. Τέλος, με βάση την παραπάνω εργασία, σχεδίασαν και ολοκλήρωσαν ένα πρωτότυπο σύστημα βασισμένο σε λογισμικό και υλικό. Hu et al. [5] πρότεινε ένα σχήμα με αισθητήρα IoT που βασίζεται σε υπολογιστικό νέφος που σχετίζεται με τον ψηφιακό φάκελο, την ψηφιακή πιστοποίηση, την υπογραφή, τους μηχανισμούς χρονικής σήμανσης και την ασύμμετρη τεχνολογία κρυπτογράφησης, για την παρακολούθηση των βιολογικών δεδομένων των ηλικιωμένων και άλλων προσωπικών πληροφοριών. Το προτεινόμενο σχέδιο θα μπορούσε να παρέχει πιο ευέλικτη και ακριβή ιατρική υπηρεσία, καθώς και μείωση των σπαταλών ιατρικών πόρων.

Οι Li et al. [6] πρότειναν ένα ασφαλές σύστημα ελέγχου ταυτότητας και βασικής συμφωνίας για σύστημα WBAN που υποστηρίζεται από cloud χρησιμοποιώντας εκτεταμένους χαοτικούς χάρτες, όπως φαίνεται στο Σχήμα 11. Ο σχεδιασμός των χαοτικών χαρτών Chebyshev, που βασίζονται στην έννοια της ανταλλαγής κλειδιών Diffie – Hellman, μπορεί να δημιουργήσει ασφαλείς τρόπους ή κανάλια για τους συμμετέχοντες στο σύστημα κατά την εγγραφή τους. Τα μετρημένα είδη υγείας που συλλέχθηκαν από αισθητήρες σώματος του WBAN θα κρυπτογραφήθηκαν πριν από τη μετάδοση. Προκειμένου να υποστηρίξει την ανάλυση σε πραγματικό χρόνο με συνεχή

απομακρυσμένη παρακολούθηση σε είδη υγείας που προσανατολίζονται στη ροή, ο παρακολουθούμενος ασθενής μπορεί να εξουσιοδοτήσει τους ιατρικούς φροντιστές να έχουν πρόσβαση σε αντικείμενα υγείας που είναι αποθηκευμένα σε ένα σύννεφο, το οποίο όχι μόνο παρέχει φροντίδα στο σπίτι αλλά και βελτιώνει την ποιότητα ζωής . Οι αναλύσεις ασφάλειας και απόδοσης έδειξαν ότι ο προτεινόμενος μηχανισμός μπορεί να αντιμετωπίσει αποτελεσματικά την πρόκληση της ταυτότητας των συμμετεχόντων σε κινητά συστήματα ιατρικής περίθαλψης έκτακτης ανάγκης.



Εικόνα 11. Η αρχιτεκτονική του δικτύου ασύρματης περιοχής σώματος υποβοηθούμενη από σύννεφο στο κινητό σύστημα ιατρικής περίθαλψης έκτακτης ανάγκης.

4.2.2. Έλεγχος πρόσβασης

Ο έλεγχος πρόσβασης είναι το μέσο με το οποίο ένα σύστημα δεδομένων καθορίζει την ταυτότητα ενός χρήστη και τις προκαθορισμένες πολιτικές που εμποδίζουν την πρόσβαση σε πόρους από μη εξουσιοδοτημένους χρήστες [16]. Υπάρχουν διάφορες μέθοδοι κρυπτογράφησης που εφαρμόζονται στον έλεγχο πρόσβασης, όπως η κρυπτογράφηση συμμετρικού κλειδιού (SKE: symmetric key encryption), η ασύμμετρη κρυπτογράφηση κλειδιών (AKE: asymmetric key encryption) και η κρυπτογράφηση βάσει χαρακτηριστικών (ABE: attribute-based encryption) [17].

Σύμφωνα με τις γενικές γνώσεις, η κρυπτογραφία βασίζεται σε κλειδιά. Ο μηχανισμός μεγέθους και δημιουργίας μυστικών κλειδιών επηρεάζει άμεσα την ασφάλεια του κρυπτοσυστήματος. Επομένως, για ένα κρυπτοσύστημα, ο βασικός μηχανισμός διαχείρισης καθορίζει τον κύκλο ζωής του συστήματος ασφαλείας. Λόγω της κλιμακούμενης διαχείρισης κλειδιών και των ευέλικτων πολιτικών ελέγχου πρόσβασης, το ABE γίνεται σταδιακά ένα είδος μεθόδου mainstream. Ο Πίνακας 5 δείχνει μερικούς μηχανισμούς ελέγχου πρόσβασης.

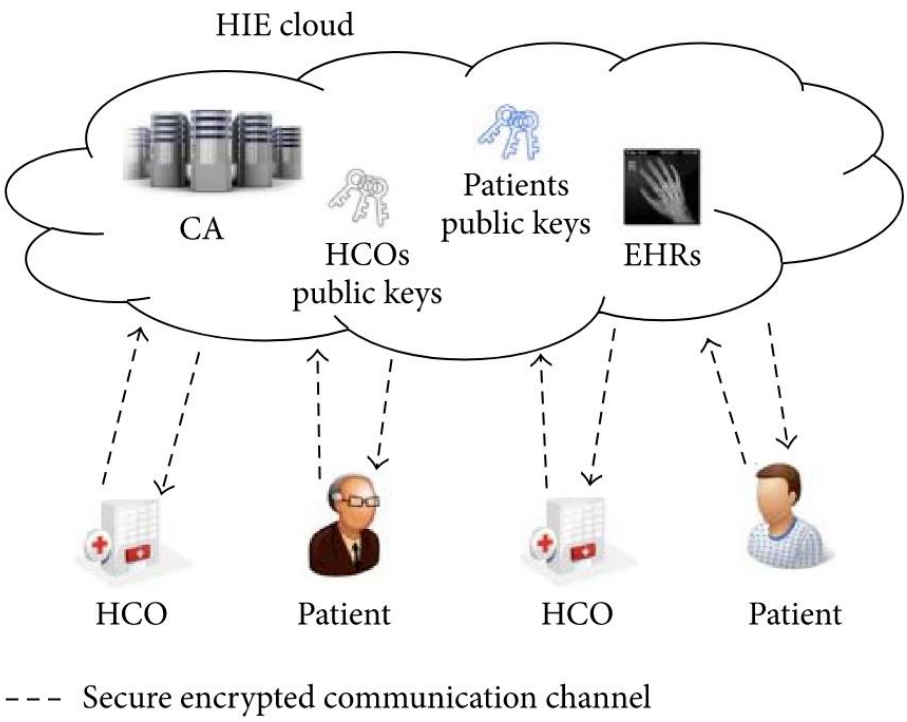
Πίνακας 5. Μηχανισμοί ασφάλειας και απορρήτου και προτάσεις για έλεγχο πρόσβασης.

Technologies	Application	Details
ABE	Access control	Solving the revocation problem of emergency key
CP-ABE	Medical sensor networks	Supporting complex and dynamic security policies
ABE	Access control to PHR	Leveraging ABE to encrypt PHR files

Στην Ανταλλαγή Πληροφοριών Υγείας (HIE), οι πληροφορίες για την υγεία των ασθενών μπορούν να κοινοποιούνται ηλεκτρονικά με ρητή εξουσιοδότηση της ανταλλαγής πληροφοριών με ελεγχόμενο τρόπο. Ωστόσο, οι υπάρχουσες προσεγγίσεις για την έγκριση σε συστήματα πληροφοριών υγείας παρουσιάζουν πολλά μειονεκτήματα στην κάλυψη των αναγκών του HIE, με τις

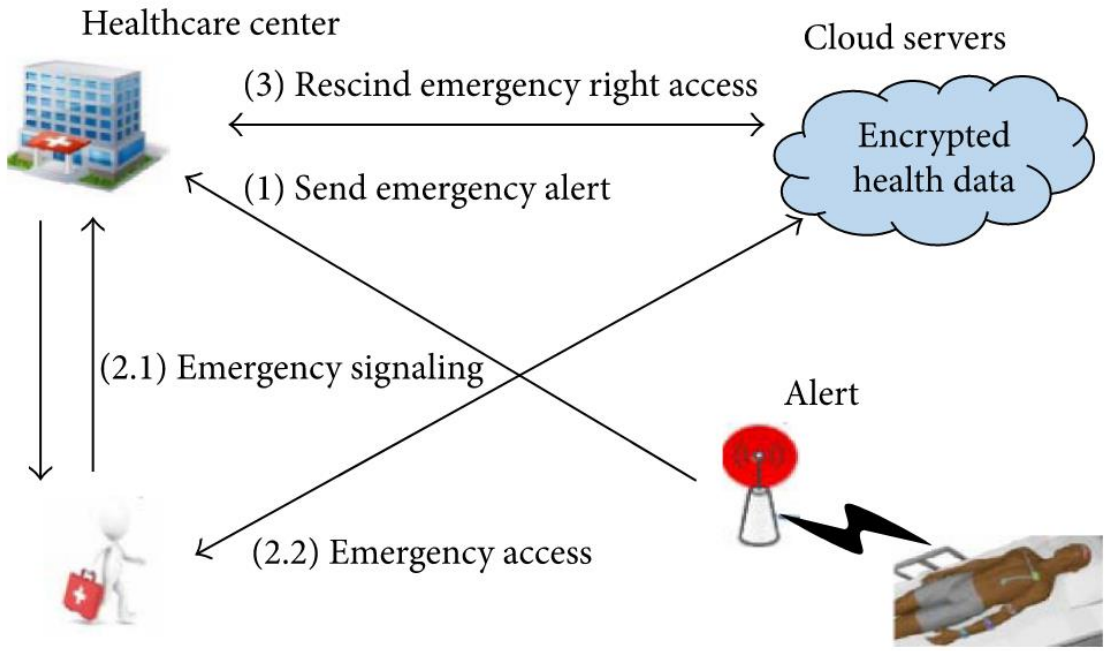
μη κρυπτογραφικές προσεγγίσεις να στερούνται ασφαλούς και αξιόπιστου μηχανισμού για την εφαρμογή της πολιτικής πρόσβασης, ενώ οι κρυπτογραφικές προσεγγίσεις είναι πολύ ακριβές, περίπλοκες και περιορισμένες στον καθορισμό πολιτικών.

Οι Chandrasekhar et al. [18] πρότειναν ένα πρωτόκολλο εξουσιοδότησης για HIE που βασίζεται σε σύννεφο, το οποίο καλύπτει το κενό μεταξύ κρυπτογραφικών και μη κρυπτογραφικών προσεγγίσεων. Το σύστημα αποτελείται από τρία κύρια συστατικά: το σύννεφο HIE, τους οργανισμούς υγειονομικής περίθαλψης (HCO) και τους ασθενείς, όπως φαίνεται στο Σχήμα 12. Ανέπτυξαν ένα νέο πρωτόκολλο βασισμένο σε υπογραφή διακομιστή μεσολάβησης, βασισμένο σε ένα νέο διακριτό σχήμα κατακερματισμού trapdoor, που επιτρέπει την επικυρωμένη και εξουσιοδοτημένη επιλεκτική κοινή χρήση πληροφοριών για την υγεία των ασθενών μέσω ενός HIE που βασίζεται σε σύννεφο. Σύμφωνα με τη λεπτομερή ανάλυση ασφάλειας και απόδοσης, το προτεινόμενο πρωτόκολλο, χρησιμοποιώντας το σύστημα υπογραφής διακομιστή μεσολάβησης με βάση το hash trapdoor, επιτυγχάνει την καλύτερη συνολική απόδοση, ενώ είναι απολύτως ασφαλές.



Εικόνα 12. Εξαρτήματα συστήματος.

Οι Lounis et al. [7] παρουσίασαν μια αρχιτεκτονική βασισμένη σε κρυπτογράφηση βάσει χαρακτηριστικών (ABE), όπως φαίνεται στο Σχήμα 13 . Δεδομένου ότι η πρόσβαση έκτακτης ανάγκης είναι προσωρινή, είναι ζωτικής σημασίας η ανάκληση των δικαιωμάτων πρόσβασης που έχουν δοθεί. Ωστόσο, η ανάκληση είναι ένα δύσκολο ζήτημα στα σχήματα ABE και μπορεί να προκαλέσει υψηλό κόστος. Οι ακέραιες τιμές και οι ακέραιες συγκρίσεις [19] εφαρμόστηκαν για την επίλυση του προβλήματος ανάκλησης του κλειδιού έκτακτης ανάγκης. Επιπλέον, παρουσίασαν ένα αριθμητικό χαρακτηριστικό που έχει μια τιμή δεδομένων για να εκφράσει τα δεδομένα εγκυρότητας του κλειδιού έκτακτης ανάγκης. Οι προσομοιώσεις σε τρία σενάρια έδειξαν ότι το προτεινόμενο σύστημα μπορεί να μειώσει το κόστος ανάκλησης και να μειώσει τον χρόνο απόκρισης έκτακτης ανάγκης, πράγμα που σημαίνει ότι το σχέδιο μπορεί να παρέχει έναν αποτελεσματικό και λεπτομερή έλεγχο πρόσβασης.



Εικόνα 13. Παράδειγμα επέμβασης έκτακτης ανάγκης.

Οι Lounis et al. [8] πρότειναν μια νέα αρχιτεκτονική που βασίζεται σε σύννεφο για ιατρικά ασύρματα δίκτυα αισθητήρων και ανέπτυξε έναν έλεγχο πρόσβασης που υποστηρίζει σύνθετες και δυναμικές πολιτικές ασφαλείας, που βασίζονται στην κρυπτογράφηση βασισμένη σε χαρακτηριστικά ciphertext-Policy (CP-ABE). Τα αποτελέσματα προσομοίωσης έδειξαν ότι ο έλεγχος πρόσβασης είναι αποτελεσματικός, λεπτομερής και επεκτάσιμος. Οι Li et al. [9] πρότειναν ένα νέο πλαίσιο που εστιάζει στον ασθενή και μια σειρά μηχανισμών για τον έλεγχο της πρόσβασης δεδομένων σε PHR που είναι αποθηκευμένα σε διακομιστές ημι-αξιόπιστους. Για να επιτύχουν λεπτομερή και επεκτάσιμο έλεγχο πρόσβασης δεδομένων για PHRs, αξιοποίησαν τεχνικές κρυπτογράφησης βάσει χαρακτηριστικών (ABE) για την κρυπτογράφηση του αρχείου PHR κάθε ασθενούς και εκμεταλλεύτηκαν την πολυδύναμη ABE για να εγγυηθούν υψηλό βαθμό ιδιωτικότητας των ασθενών.

4.2.3. Αξιόπιστος έλεγχος τρίτων

Οι διακομιστές Cloud δεν είναι πλήρως αξιόπιστοι. Η ακεραιότητα και η συνέπεια των ιατρικών δεδομένων που είναι αποθηκευμένα στο cloud θα μπορούσαν να διακυβευτούν εάν η καταστροφή δεδομένων ή ακόμη και η διαγραφή πραγματοποιηθεί χωρίς την άδεια του χρήστη. Για λόγους ασφαλείας, οι κανόνες δεδομένων καθορίζονται συνήθως από τον χρήστη, έτσι ώστε ο πάροχος διακομιστή να μην έχει άμεση επαφή με τα δεδομένα προέλευσης. Επιπλέον, το αξιόπιστο τρίτο μέρος (TTP) με μεγάλη φήμη που παρέχει τα αμερόληπτα αποτελέσματα ελέγχου μπορεί να εισαχθεί σωστά, για να επιτρέψει την υπευθυνότητα των παρόχων υπηρεσιών cloud και να προστατεύσει τα νόμιμα οφέλη των χρηστών cloud [20]. Τα ερευνητικά ζητήματα του TTP αποτελούνται από δυναμικό έλεγχο, μαζικό έλεγχο και έλεγχο σχετικά με τη μέτρηση απόδοσης.

Τις τελευταίες δεκαετίες, έχουν παρουσιαστεί πολλές μέθοδοι ελέγχου. Αρκετές εποπτευόμενες προσεγγίσεις μηχανικής μάθησης, όπως η λογιστική παλινδρόμηση και η μηχανή φορέα υποστήριξης, έχουν εφαρμοστεί για την ανίχνευση ύποπτης πρόσβασης [21]. Ωστόσο, το να βασίζεστε πάρα πολύ στις αναμενόμενες κρίσεις και στις προκαθορισμένες ετικέτες περιορίζει την προαγωγή μεγάλης κλίμακας. Επί του παρόντος, οι μη εποπτευόμενες προσεγγίσεις προσελκύουν σταδιακά περισσότερη προσοχή.

Οι Chen et al. [22] επέκτειναν τις σχεσιακές μεθόδους μάθησης του Malin και των συναδέλφων της, για την κατασκευή του παγκόσμιου δικτύου αλληλεπιδράσεων με τμήματα. Με βάση τη δομή του δικτύου, πρότειναν δύο μέτρα για τον χαρακτηρισμό των τμηματικών σχέσεων. Πρώτον, εφάρμοσαν βεβαιότητα για να χαρακτηρίσουν τη δύναμη των αλληλεπιδράσεων των τμημάτων με την πάροδο του χρόνου, η οποία σχεδιάστηκε για να εκτιμήσει το βαθμό στον οποίο οι αλλαγές στο δίκτυο επηρεάζουν τη συνάφεια των τμημάτων μεταξύ τους. Δεύτερον, εφάρμοσαν την αμοιβαιότητα για να μετρήσουν το βαθμό στον οποίο τα τμήματα παρουσιάζουν παρόμοια συμπεριφορά το ένα με το άλλο. Μελέτησαν ημερολόγια πρόσβασης τριών μηνών από ένα μεγάλο ακαδημαϊκό ιατρικό κέντρο και τα αποτελέσματα έδειξαν

ότι τα τμηματικά δίκτυα αλληλεπίδρασης εμφανίζουν ορισμένα αναλλοίωτα, όπως ο αριθμός, η δύναμη και η αμοιβαιότητα των σχέσεων,

Οι Govaert et al. [23] προχώρησαν σε προκαταρκτική ανασκόπηση της σχέσης μεταξύ ελέγχων και λειτουργικού κόστους. Σύμφωνα με τη μελέτη τους, ο χειρουργικός έλεγχος μπορεί να λειτουργήσει ως ποιοτικό όργανο και ως εκ τούτου ως εργαλείο για τη μείωση του κόστους και θα πρέπει να διεξαχθούν περαιτέρω μελέτες για διερεύνηση.

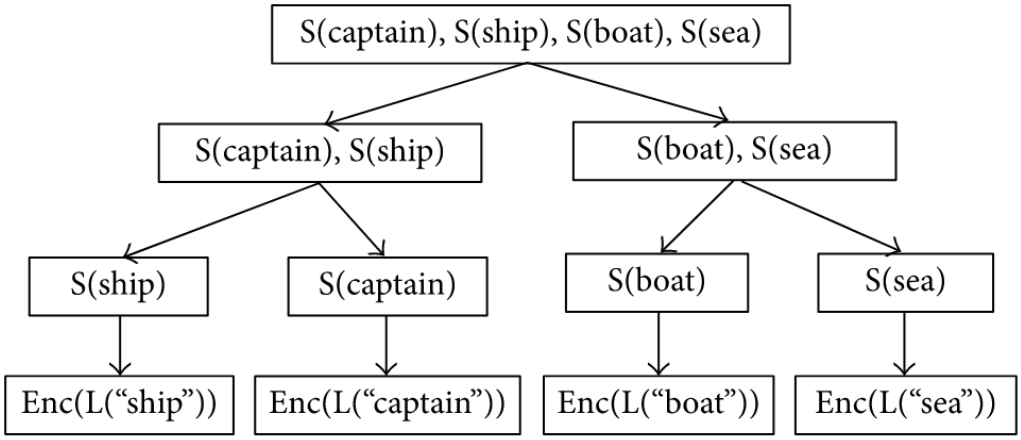
4.2.4. Αναζήτηση δεδομένων

Για την προστασία του απορρήτου των δεδομένων, τα ευαίσθητα δεδομένα πρέπει να κρυπτογραφούνται πριν από την εξωτερική ανάθεση, η οποία ξεπερνά την παραδοσιακή χρήση δεδομένων με βάση την αναζήτηση λέξεων-κλειδιών απλού κειμένου. Επομένως, η ενεργοποίηση μιας κρυπτογραφημένης υπηρεσίας αναζήτησης δεδομένων cloud είναι υψίστης σημασίας [24]. Οι κύριες μέθοδοι για κρυπτογράφηση με δυνατότητα αναζήτησης περιλαμβάνουν συμμετρική κρυπτογράφηση με δυνατότητα αναζήτησης (SSE) και κρυπτογράφηση δημόσιου κλειδιού με αναζήτηση λέξεων-κλειδιών (PEKS). Και πρέπει να σημειωθεί ότι όσο πιο περίπλοκα είναι τα μέτρα κρυπτογράφησης, τόσο πιο δύσκολη είναι η αναζήτηση των δεδομένων και τόσο πιο δύσκολη ελέγχεται η συνέπεια των αποτελεσμάτων αναζήτησης. Εάν τα αποτελέσματα αναζήτησης δεν μπορούν να εφαρμοστούν εγκαίρως, τότε όλα τα μέτρα ασφάλειας και απορρήτου έχουν λιγότερο νόημα. Ο Πίνακας 6 δείχνει μερικούς μηχανισμούς αναζήτησης δεδομένων.

Πίνακας 6. Μηχανισμοί ασφάλειας και απορρήτου και προτάσεις για αναζήτηση δεδομένων.

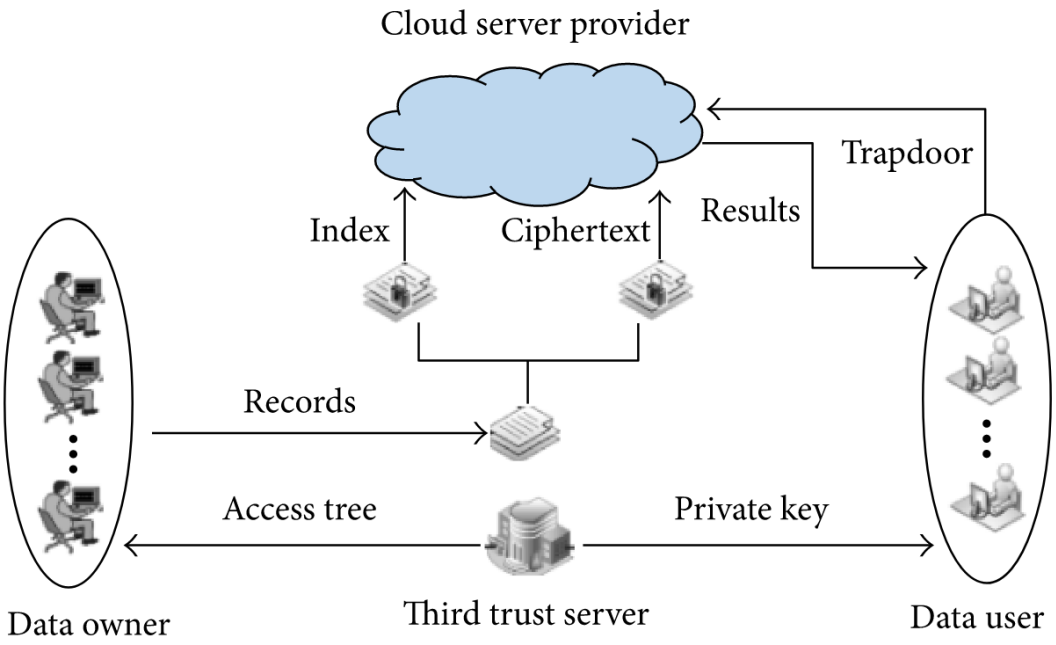
Technologies	Application	Details
Symmetric key	Supporting privacy preserving string matching	Providing strong privacy guarantees against attacks from a semihonest adversary
LKE	Searching over encrypted image	Better estimating of edges using smoothing kernels with edges information
APKS	Searching over encrypted PHR	Allowing users to obtain query capabilities from localized trusted authorities according to their attributes
CP-ABE	Searching over encrypted PHR	Supporting both fine-grained access control and multikeyword search

Για να επιτύχουν πλούσια λειτουργικότητα ερωτημάτων πάνω από τα κρυπτογραφημένα δεδομένα, οι Bezawada et al. ανέπτυξαν μια προσέγγιση βασισμένη σε συμμετρικό κλειδί για την υποστήριξη της προστασίας απορρήτου που αντιστοιχεί στις συμβολοσειρές στο cloud computing. Ανέπτυξαν μια αποτελεσματική και ακριβή δομή ευρετηρίου, το δέντρο Pattern Aware Secure Search (PASS), ένα πολύ ισορροπημένο δυαδικό δέντρο χωρίς να αποκαλύψουν ομοιότητες περιεχομένου των λέξεων-κλειδιών. Η διαδικασία δράσης του δέντρου PASS φαίνεται στο σχήμα 14 . Επιπλέον, περιέγραψαν επίσης έναν αλγόριθμο κατάταξης συνάφειας για την επιστροφή των πιο σχετικών εγγράφων στον χρήστη βάσει του ερωτήματος μοτίβου. Πειράματα σε μεγάλα δεδομένα πραγματικής ζωής που περιέχουν έως και 100000 λέξεις-κλειδιά έδειξαν ότι ο προτεινόμενος αλγόριθμος μπορεί να επιτύχει αναζήτηση μοτίβων σε λιγότερο από μερικά χιλιοστά του δευτερολέπτου με ακρίβεια 100%.



Εικόνα 14. Διαδικασία δράσης του δέντρου PASS

Για να χρησιμοποιήσετε τους ελαστικούς πόρους και το υπολογιστικό βάρος του μαθήματος, το προσωπικό αρχείο υγείας (PHR) μεταφέρεται σταδιακά στο cloud storage. Οι Miao et al. [11] σχεδίασαν ένα ασφαλές κρυπτογραφικό αρχικό που ονομάζεται αναζήτηση πολλαπλών λέξεων βασισμένο σε χαρακτηριστικά πάνω από κρυπτογραφημένα προσωπικά αρχεία υγείας σε ρύθμιση πολλών χρηστών για να υποστηρίξει τόσο λεπτομερή έλεγχο πρόσβασης όσο και αναζήτηση πολλαπλών λέξεων μέσω κρυπτογράφησης βασισμένης σε χαρακτηριστικά ciphertext-Policy (CP-ABE). Το σχήμα 15 παρέχει μια επισκόπηση του σχήματος m2-ABKS. Πραγματοποιήθηκαν εμπειρικά πειράματα πάνω σε σύνολο δεδομένων πραγματικού κόσμου για να δείξουν τη σκοπιμότητα και την πρακτικότητά του σε ένα ευρύ φάσμα πραγματικών σεναρίων.



Εικόνα 15. Σχήμα με το Μοντέλο συστήματος m2-ABKS.

Οι μέθοδοι που βασίζονται στην παλινδρόμηση του πυρήνα μπορούν να αποκαταστήσουν την εικόνα από την έκδοση του κάτω δείγματος με χαμηλό υπολογιστικό κόστος, αλλά με χαμηλή ποιότητα γύρω από τις άκρες. Οι Song et. al., πρότεινε μια μέθοδο παλινδρόμησης καθοδηγούμενου πυρήνα Laplace (LKR), στην οποία χρησιμοποιείται ένας νέος σταθμισμένος χάρτης Laplace για τη βελτίωση του πυρήνα εξομάλυνσης στο KR και η βασική εικόνα του LKR είναι ότι οι μέθοδοι που βασίζονται σε KR μπορούν να εκτιμήσουν καλύτερα τα άκρα όταν χρησιμοποιούν εξομάλυνση πυρήνων με πληροφορίες άκρων. Οι Li et al. διατύπωσαν και αντιμετώπισαν το πρόβλημα των εξουσιοδοτημένων ιδιωτικών αναζητήσεων λέξεων-κλειδιών (APKS) στο κρυπτογραφημένο προσωπικό αρχείο υγείας σε περιβάλλοντα υπολογιστικού νέφους. Επιτρέπουν στους χρήστες να αποκτήσουν δυνατότητες ερωτήματος από τοπικές αξιόπιστες αρχές σύμφωνα με τα χαρακτηριστικά τους. Εκτός από το απόρρητο των εγγράφων και το απόρρητο των ερωτημάτων, άλλες σημαντικές δυνατότητες των συστημάτων μας περιλαμβάνουν αποτελεσματική υποστήριξη πολυδιάστατων και πολλαπλών αναζητήσεων λέξεων-κλειδιών με απλό ερώτημα εύρους και επιτρέπουν ανάθεση και ανάκληση δυνατοτήτων αναζήτησης.

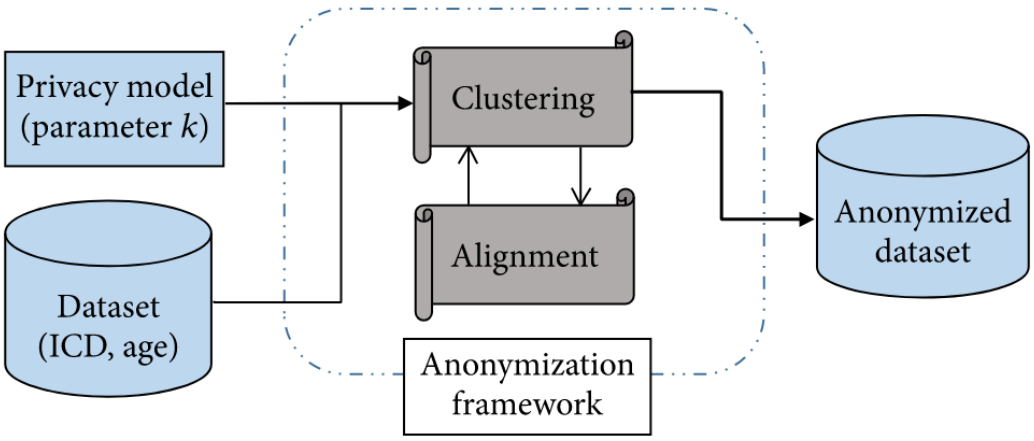
4.2.5. Ανωνυμοποίηση δεδομένων

Τα ευαίσθητα δεδομένα ασθενών μπορούν να χωριστούν σε τρεις κατηγορίες: ρητά αναγνωριστικά, οιονεί αναγνωριστικά και χαρακτηριστικά απορρήτου. Το ρητό αναγνωριστικό μπορεί να υποδείξει μοναδικά έναν ασθενή, όπως έναν αριθμό ταυτότητας, ένα όνομα και έναν αριθμό κινητού τηλεφώνου. Ένας συνδυασμός οιονεί αναγνωριστικών μπορεί επίσης να δείξει μοναδικά έναν ασθενή, όπως ηλικία, δεδομένα γέννησης και διεύθυνση. Οι πληροφορίες απορρήτου αναφέρονται σε ευαίσθητα χαρακτηριστικά ενός ασθενούς, συμπεριλαμβανομένης της ασθένειας και του εισοδήματος. Κατά τη διαδικασία δημοσίευσης δεδομένων, λαμβάνοντας υπόψη τα χαρακτηριστικά διανομής των αρχικών δεδομένων, είναι απαραίτητο να διασφαλιστεί ότι η επεξεργασία των μεμονωμένων χαρακτηριστικών του νέου συνόλου δεδομένων είναι σωστή, ώστε να προστατεύεται το απόρρητο του ασθενούς. Προς το παρόν, η τεχνολογία τυχαίας διαταραχής και η ανώνυμη τεχνολογία δεδομένων χρησιμοποιούνται συνήθως για την επίλυση αυτών των ζητημάτων, όπως k-anonymity, l-diversity και εμπιστοσύνη. Συγκεκριμένα, η παραδοσιακή-ανωνυμία εφαρμόζεται ευρέως. Ωστόσο, το μειονέκτημα είναι ότι δεν κάνει περιορισμούς στα ευαίσθητα δεδομένα και οι εισβολείς μπορούν να χρησιμοποιήσουν επίθεση συνέπειας και επίθεση γνώσης στο παρασκήνιο για να προσδιορίσουν ευαίσθητα δεδομένα και προσωπικές επαφές, οι οποίες οδηγούν σε απώλεια απορρήτου.

Μετά τη μελέτη των ανησυχιών περί απορρήτου της ανταλλαγής πληροφοριών για τους ασθενείς μεταξύ των Υπηρεσιών Μετάγγισης Ερυθρού Σταυρού Χονγκ Κονγκ (BTS) και των δημόσιων νοσοκομείων, οι Miao et al. διαπίστωσαν ότι υπάρχουν τρεις προκλήσεις, η υψηλή διάσταση, η χρησιμότητα δεδομένων και η ποιότητα του αλγορίθμου, που περιορίζουν την εφαρμογή των παραδοσιακών μεθόδων ανωνυμοποίησης δεδομένων. Πρότειναν ένα νέο μοντέλο απορρήτου που ονομάζεται LKC-privacy, χρησιμοποιώντας δύο αλγόριθμους με διαφορετικές προσαρμογές, για την αντιμετώπιση των προβλημάτων της κεντρικής ανωνυμοποίησης και της κατανεμημένης ανωνυμοποίησης. Η πρώτη προσαρμογή μεγιστοποιεί τις πληροφορίες που διατηρούνται για ανάλυση ταξινόμησης και η δεύτερη ελαχιστοποιεί την

παραμόρφωση των ανώνυμων δεδομένων για γενική ανάλυση δεδομένων. Οι δύο αλγόριθμοι εφαρμόστηκαν σε δύο σύνολα δεδομένων πραγματικής ζωής, το Blood και το Adult. Τα αποτελέσματα έδειξαν ότι οι προτεινόμενοι αλγόριθμοι ήταν ευέλικτοι και αρκετά επεκτάσιμοι για να χειριστούν μεγάλους όγκους δεδομένων μετάγγισης αίματος με αριθμητικά χαρακτηριστικά.

Πολλοί αλγόριθμοι συμπλέγματος μπορούν να εφαρμοστούν στην ανωνυμοποίηση δεδομένων για τα k-ανώνυμα δεδομένα. Στο πλαίσιο των διαχρονικών δεδομένων, η πρόκληση είναι να καθοριστεί μια μέτρηση απόστασης για τις τροχιές. Το Σχήμα 16 παρέχει μια επισκόπηση της διαδικασίας διαχρονικής ανωνυμοποίησης δεδομένων. Οι Fung et al. [25] επέλεξαν τον αλγόριθμο Μέγιστη απόσταση από τον μέσο όρο φορέα (MDAV) [26], έναν αποτελεσματικό ευρετικό για την ανωνυμία, για να αναπτύξει τον αλγόριθμο ομαδοποίησης. Ο προτεινόμενος αλγόριθμος επιλέγει επαναληπτικά την πιο συχνή τροχιά σε ένα διαμήκη σύνολο δεδομένων και σχηματίζει ένα σύμπλεγμα από τουλάχιστον k καταγραφές γύρω από το τελευταίο. Επιπλέον, ορίζουν την απόσταση μεταξύ δύο τροχιών ως το κόστος της ανωνυμοποίησής τους. Πειράματα σε αρκετές ομάδες ασθενών που προέρχονται από το σύστημα EMR του Ιατρικού Κέντρου του Πανεπιστημίου Vanderbilt έδειξαν ότι η προτεινόμενη προσέγγιση μπορεί να δημιουργήσει ανώνυμα δεδομένα που επιτρέπουν αποτελεσματική βιοϊατρική ανάλυση, χρησιμοποιώντας ευρετικά στοιχεία εμπνευσμένα από ευθυγράμμιση ακολουθιών και μεθόδους ομαδοποίησης.



Εικόνα 16. Μια γενική αρχιτεκτονική της διαδικασίας διαχρονικής ανωνυμοποίησης δεδομένων.

Οι Liu και Li [7] εισήγαγαν έναν αλγόριθμο k-ανωνυμίας που βασίζεται στη μέθοδο ομαδοποίησης ως το θεμέλιο στοιχείο της προστασίας της ιδιωτικής ζωής για ιατρικές φορητές συσκευές. Η ομαδοποίηση k-ανωνυμίας θα εκχωρήσει παρόμοιες εγγραφές στο ίδιο ισοδύναμο σύνολο, ενώ η ομοιότητα μεταξύ αυτών των εγγραφών καθιστά δυσκολότερη τη διάκριση διαφορετικών ταυτοτήτων από πριν. Στη συνέχεια, ενοποιούν τα οιονεί αναγνωριστικά στις ίδιες συστάδες γενικεύοντας και καταστέλλοντας τις λειτουργίες. Η έξοδος αυτού του αλγορίθμου είναι ένας πίνακας που ικανοποιεί την αρχή της-ανωνυμίας. Όλες οι εγγραφές στο ίδιο ισοδύναμο σύνολο είναι παρόμοιες μεταξύ τους. Με αυτόν τον τρόπο, θα ήταν πιο δύσκολο να αναγνωριστούν οι ταυτότητες των χρηστών σε ένα ισοδύναμο σύνολο και η προστασία της ιδιωτικής ζωής αυτών των θεμάτων θα ήταν ασφαλής.

4.3. Χρησιμοποίηση φορητών συσκευών

Προβλήματα ασφαλείας εμφανίζονται με την ευρεία ανάπτυξη ιατρικών φορητών συσκευών. Η πιο σοβαρή απειλή θα ήταν η διαρροή απορρήτου των δεδομένων ιατρικών φορητών συσκευών. Μετά τη συλλογή δεδομένων από τα έξυπνα τερματικά, οι κάτοχοι δεδομένων ιατρικών φορητών συσκευών είναι πρόθυμοι να κοινοποιήσουν τα δεδομένα σε προγραμματιστές εφαρμογών για να εμπλουτίσουν τις υπηρεσίες τους ή να αποκτήσουν χρηματικά οφέλη. Τα

δεδομένα που συλλέγονται περιέχουν άφθονες πληροφορίες απορρήτου. Επιπλέον, κατά την κοινοποίηση των δεδομένων που έχουν καταγραφεί από φορητούς αισθητήρες που φοριούνται από τον άνθρωπο, ορισμένες προσωπικές πληροφορίες, όπως ηλικία, ύψος και βάρος, μπορούν επίσης να υποβληθούν με εγγύηση. Επομένως, αν και η αρχική πρόθεση της κοινής χρήσης δεδομένων είναι πάντα θετική, οι ανεξέλεγκτες προσωπικές πληροφορίες μπορεί να αυξήσουν τον κίνδυνο αποκάλυψης απορρήτου.

Σε αυτήν την ενότητα, συγκρίνουμε 4 είδη ανωνυμίας, όπως το Partial Datafly-anonymity, Total Datafly-anonymity [28], -Argus- anonymity [29] και το clustering- anonymity, τα οποία διαφέρουν στην κατανομή των συνόλων δεδομένων. Θέλουμε να επαληθεύσουμε εάν η διαίρεση του συνόλου δεδομένων επηρεάζει την ασφάλεια των δεδομένων απορρήτου. Τα δεδομένα συλλέγονται από μια πραγματική βάση δεδομένων νοσοκομείου. Τα αποτελέσματα του πειράματος δείχνουν την αποτελεσματικότητα της ομαδοποίησης- ανωνυμίας.

4.3.1. Ένα παράδειγμα αποκάλυψης απορρήτου

Για παράδειγμα, όπως δείχνει ο Πίνακας 7 , η Alice είναι κάτοχος μιας ιατρικής φορητής συσκευής και ο κατασκευαστής της συσκευής συλλέγει τα δεδομένα που παράγονται από αυτήν τη συσκευή και τις πληροφορίες σχετικά με την ηλικία, το ύψος και το βάρος της. Στη συνέχεια, ο κάτοχος δεδομένων μοιράστηκε ένα σύνολο δεδομένων (όπως φαίνεται στον Πίνακα 7) που περιέχει τα δεδομένα της Alice. Ο αντίπαλος Evil παίρνει αυτές τις πληροφορίες και ξέρει ότι η Alice είναι 178 cm, 75 kg και σε ηλικία 34 ετών. Επομένως, ο Evil θα μπορούσε να πάρει τα ευαίσθητα δεδομένα της Alice εύκολα συνδυάζοντας το σύνολο δεδομένων με τις βασικές γνώσεις.

Πίνακας 7. Αρχικά δεδομένα.

Height	Weight	Age	Sensitive data
172	63	27	Time serials
178	75	34	Time serials
180	72	26	Time serials
185	77	22	Time serials

Ο κάτοχος δεδομένων διακόπτει τη σύνδεση μεταξύ της ταυτότητας και των ευαίσθητων δεδομένων γενικεύοντας τα οιονεί αναγνωριστικά πριν από την κοινή χρήση σύμφωνα με την k-ανωνυμία. Ο Πίνακας 8 δείχνει το αποτέλεσμα 2-ανωνυμίας του Πίνακα 4 . Στον Πίνακα 8, θα ήταν δύσκολο να αναγνωρίσουμε την ταυτότητα της Alice με τη σύνδεση-επίθεση. Ωστόσο, τα δεδομένα που περιέχονται σε ευαίσθητα δεδομένα θα μπορούσαν να αποκαλύψουν την ταυτότητα της Alice. Συγκεκριμένα, εάν εξαγάγουμε το κατάλληλο χαρακτηριστικό αυτών των δεδομένων και τα βάλουμε σε κατάλληλο ταξινομητή, η ταυτότητα θα μπορούσε να αναγνωριστεί.

Πίνακας 8. Αποτέλεσμα ανωνυμίας των αρχικών δεδομένων.

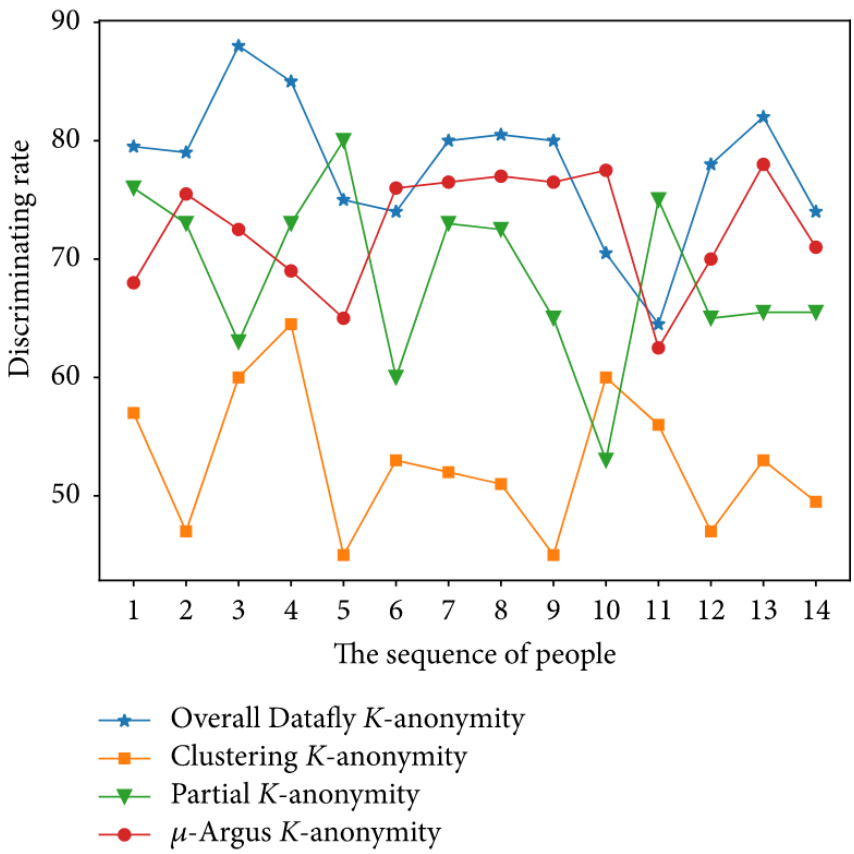
Height	Weight	Age	Sensitive data
17^*	$**$	$**$	Time serials
17^*	$**$	$**$	Time serials
18^*	7^*	2^*	Time serials
18^*	7^*	2^*	Time serials

$*$ and $**$ represent anonymous information.

4.4. Συγκριτικά αποτελέσματα και ανάλυση

4.4.1. Συγκριτικά αποτελέσματα

Το Σχήμα 17 δείχνει το διακριτικό ποσοστό των ταυτοτήτων σε κάθε ισοδύναμο σύνολο. Το σύνολο δεδομένων διαιρείται σύμφωνα με την αρχή της 2-ανωνυμίας. Είναι σαφές ότι το διακριτικό ποσοστό της ομαδοποίησης 2-ανωνυμίας είναι σχετικά χαμηλότερο από το άλλο 2-ανωνυμίας. Μπορούμε λοιπόν να ισχυριστούμε ότι η ομαδοποίηση 2-ανωνυμίας είναι η πιο ασφαλής μέθοδος μεταξύ των τεσσάρων εξεταζόμενων μεθόδων.



Εικόνα 17. Το διακριτικό ποσοστό 2-ανωνυμίας.

4.4.2. Ανάλυση

Σε αυτό το πείραμα, τα ευαίσθητα δεδομένα όλων των αρχείων διατηρούνται αμετάβλητα. Λόγω του διαφορετικού συνδυασμού σχετικά με το ισοδύναμο σύνολο, το ποσοστό διάκρισης σε κάθε ισοδύναμο σύνολο θα ήταν διαφορετικό. Η εύλογη εκχώρηση αρχείων βελτιώνει το επίπεδο ασφάλειας της ομαδοποίησης- ανωνυμίας.

4.5. Μελλοντικές προκλήσεις ασφάλειας και απορρήτου στο MIoT

Οποιοσδήποτε προγραμματιστής στην ανάπτυξη του συστήματος ασφάλειας και απορρήτου του MIoT θα λάβει υπόψη τον αντίκτυπο διαφόρων παραγόντων, για να αποκτήσει καλύτερη ισορροπία μεταξύ τους. Προκειμένου να επιτευχθεί ένα καλύτερο περιβάλλον ασφάλειας, πολλές προκλήσεις απαιτούν ιδιαίτερη προσοχή.

4.5.1. Μη ασφαλές δίκτυο

Λόγω της ευκολίας και του χαμηλού κόστους, μια σειρά συσκευών και υπηρεσιών λογισμικού βασίζονται σε μεγάλο βαθμό σε ασύρματα δίκτυα, όπως το WiFi, τα οποία είναι γνωστό ότι είναι ευάλωτα σε διάφορες εισβολές, όπως μη εξουσιοδοτημένη πρόσβαση δρομολογητή, επιθέσεις man-in-the-middle, πλαστογράφηση, επιθέσεις άρνησης υπηρεσίας και επιθέσεις βίας [30]. Επιπλέον, τα περισσότερα δωρεάν ασύρματα δίκτυα σε δημόσιο χώρο, τα οποία δεν έχουν πιστοποιηθεί, είναι μη αξιόπιστα δίκτυα [31].

4.5.2. Ελαφριά πρωτόκολλα για συσκευές

Οι συσκευές και οι εφαρμογές λογισμικού χαμηλού κόστους που βασίζονται σε αισθητήρες πρέπει να ακολουθούν συγκεκριμένους κανόνες πολιτικής και διακομιστές μεσολάβησης για την παροχή υπηρεσιών. Προς το παρόν, εάν θέλουμε να παρέχουμε ασφάλεια υψηλής ποιότητας για τους αισθητήρες, πρέπει να εφαρμόσουμε τις λύσεις υψηλού κόστους. Είναι μια σύγκρουση στο σύστημα MIoT. Η ανάπτυξη διαφορετικών επιπέδων πρωτοκόλλων ασφαλείας σύμφωνα με τα σενάρια εφαρμογών, ειδικά τα ελαφριά πρωτόκολλα ασφαλείας, είναι το κύριο καθήκον της προστασίας της ασφάλειας στο μέλλον.

4.5.3. Κοινή χρήση δεδομένων

Παρά την ταχεία ανάπτυξη της ιατρικής τεχνολογίας πληροφοριών, το φαινόμενο του νησιού πληροφοριών είναι όλο και πιο σοβαρό. Τα πρότυπα των δεδομένων που συλλέγονται από συσκευές διαφορετικών κατασκευαστών ποικίλλουν πολύ, γεγονός που καθιστά δύσκολη την ενοποίηση της διαχείρισης. Ωστόσο, η συνεργασία και η ανταλλαγή πληροφοριών μεταξύ ετερογενών συστημάτων του MIoT αποτελούν την αναπόφευκτη τάση του μέλλοντος. Η ιδιωτικοποίηση των πληροφοριών των ασθενών θα μπορούσε να είναι πολύ επιζήμια για την ασφάλεια του συστήματος MIoT. Η χρήση γενικών πολιτικών δεδομένων για το συνδυασμό διαφορετικών δεδομένων θα μπορούσε να παρέχει πιο κατανοητές πληροφορίες και να ενισχύσει την ασφάλεια και το απόρρητο με το ιεραρχικό μοντέλο ασφάλειας.

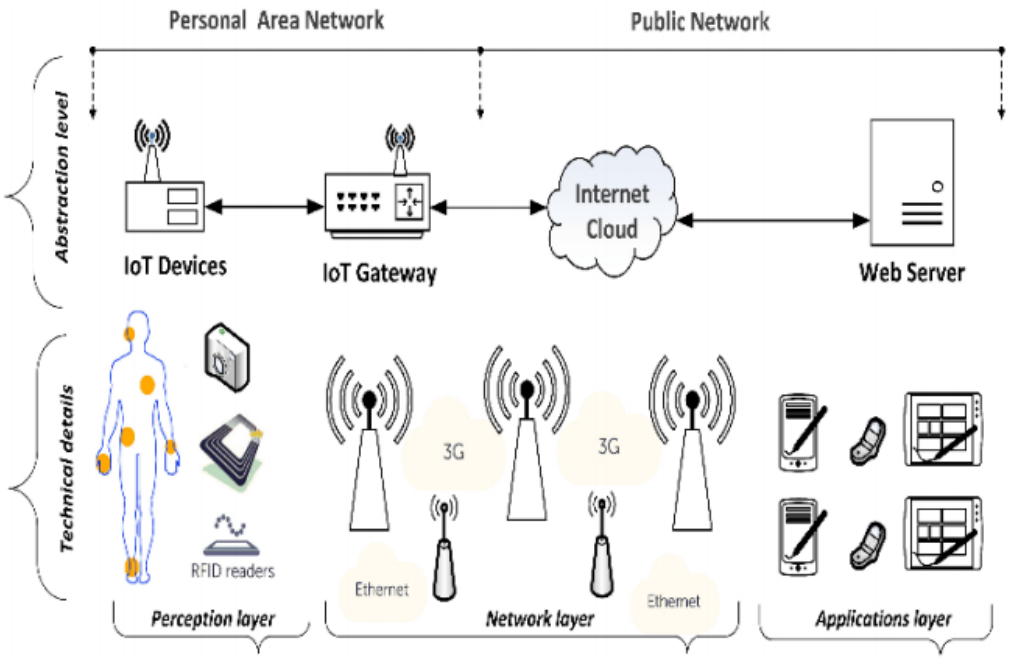
5. Ζητήματα ιδιωτικότητας στο έξυπνο σπίτι

Η πρόοδος της τεχνολογίας των πληροφοριών και των επικοινωνιών στην εποχή της παγκοσμιοποίησης είναι ένα φαινόμενο που αποτελεί μεγάλη πρόκληση. Η εφαρμογή του κατάλληλου συστήματος ασφαλείας και η διαθεσιμότητα πολλών εργαλείων ασφαλείας που είναι είτε pro είτε anti γίνονται πρόκληση για την εμφάνιση της ευπάθειας του συστήματος. Επίσης, η ποιότητα του δικτύου και τα μέσα μετάδοσης δεδομένων μπορούν να αποτελέσουν παράγοντα ευπάθειας της ακεραιότητας και της διαθεσιμότητας πληροφοριών [1]. Διάφορες εταιρείες συνεχίζουν να προσαρμόζονται, τόσο όσον αφορά τα προϊόντα, τις υπηρεσίες, όσο και τις στρατηγικές μάρκετινγκ για να είναι σε θέση να ανταγωνίζονται στις αντίστοιχες αγορές τους. Στον τομέα των τηλεπικοινωνιακών υπηρεσιών, η εταιρεία οφείλει να συνεχίσει να παρέχει την καλύτερη εξυπηρέτηση προκειμένου να διατηρήσει τη σταθερότητα της εταιρείας και να επιτύχει το μέγιστο κέρδος.

Η χρήση υπολογιστών στο μέλλον θα κυριαρχήσει στην ανθρώπινη εργασία και θα νικήσει τις ανθρώπινες υπολογιστικές δυνατότητες, όπως η χρήση ηλεκτρονικού εξοπλισμού από απόσταση, χρησιμοποιώντας μέσα Internet, IoT (Internet of Things). Αυτό επιτρέπει στους χρήστες να διαχειρίζονται και να βελτιστοποιούν τον ηλεκτρονικό εξοπλισμό που χρησιμοποιεί το Διαδίκτυο. Αυτό δείχνει ότι στο εγγύς μέλλον οι υπολογιστές και ο ηλεκτρονικός εξοπλισμός μπορούν να ανταλλάσσουν πληροφορίες μέσω αυτών των μέσων, μειώνοντας έτσι την άμεση ανθρώπινη αλληλεπίδραση. Αυτό θα αυξήσει επίσης τον αριθμό των χρηστών του Διαδικτύου με διάφορες εγκαταστάσεις και υπηρεσίες Διαδικτύου. Η κύρια πρόκληση στο IoT είναι να γεφυρωθεί το χάσμα μεταξύ του φυσικού κόσμου και του κόσμου των πληροφοριών, όπως ο τρόπος επεξεργασίας δεδομένων που λαμβάνονται από ηλεκτρονικό εξοπλισμό μέσω διεπαφής μεταξύ χρηστών και εξοπλισμού. Η αναπτυσσόμενη διάταξη IoT πλησίασε με βασικές ανάγκες για να την επηρεάσει στην ασφαλή. Πολλά ζητήματα ασφαλείας έχουν μετατραπεί σε πρόκληση για την οργάνωση του IoT.

Εμπειρογνώμονες στον τομέα της ασφάλειας έχουν προειδοποιήσει για τον πιθανό κίνδυνο μεγάλου αριθμού μη ασφαλών συσκευών που συνδέονται με

το Διαδίκτυο, δεδομένου ότι η ιδέα του IoT προτάθηκε για πρώτη φορά στα τέλη της δεκαετίας του 1990. Υπάρχουν SixLayer IoT Architecture, δηλαδή ένα στρώμα κωδικοποίησης, ένα επίπεδο αντίληψης, ένα επίπεδο δικτύου, ένα στρώμα μεσαίου λογισμικού, ένα επίπεδο εφαρμογών και ένα επιχειρησιακό επίπεδο. Όλα αυτά τα επίπεδα μπορούν επίσης να εφαρμοστούν στο Smart Home. Η αρχιτεκτονική ενός κοινού συστήματος IoT χωρίζεται σε τρία επίπεδα: επίπεδο αντίληψης, επίπεδο δικτύου και επίπεδο εφαρμογών. Ο τρόπος με τον οποίο τα συστατικά ομαδοποιούνται στα τρία στρώματα ενός γενικού συστήματος IoT φαίνεται στο Σχήμα 18.



Εικόνα 18. Μια γενική αρχιτεκτονική ενός συστήματος IoT περιλαμβάνει συσκευές IoT, μια πύλη και έναν διακομιστή ιστού. Το σχήμα δείχνει τις εσωτερικές και εξωτερικές πλευρές του συστήματος

Ένας εισβολέας μπορεί να έχει πρόσβαση ή να εισβάλει σε μια έξυπνη συσκευή στο ασύρματο δίκτυο. Σε αυτήν τη μελέτη, οι απαιτήσεις ασφαλείας για ασφαλή έξυπνη οικιακή υπηρεσία, συμπεριλαμβανομένης της ακεραιότητας, της

διαθεσιμότητας και του ελέγχου ταυτότητας. Ο σκοπός του Διαδικτύου των πραγμάτων είναι να επιτρέψει στα πράγματα να συνδέονται οποιαδήποτε στιγμή, οπουδήποτε, με οτιδήποτε και οποιοσδήποτε χρησιμοποιεί ιδανικά διαδρομές ή δίκτυα και υπηρεσίες . Το Διαδίκτυο των πραγμάτων είναι μια νέα επανάσταση του Διαδικτύου. Τα αγαθά θα γίνουν εύκολα αναγνωρίσιμα και θα αποκτήσουν ευφυΐα δημιουργώντας ή επιτρέποντας περιβάλλοντα που σχετίζονται με το γεγονός ότι μπορούν να επικοινωνούν πληροφορίες για τον εαυτό τους. Αυτό έρχεται μαζί με την εμφάνιση ενός συστήματος cloud ή cloud computing που έχει μετάβαση από το Διαδίκτυο στο IPv6 στο χειριστείτε περιορισμένη χωρητικότητα [3].

5.1. Επισκόπηση έξυπνου οικιακού συστήματος

Οι υπηρεσίες έξυπνου σπιτιού IoT αυξάνονται μέρα με τη μέρα, οι ψηφιακές συσκευές μπορούν να επικοινωνούν αποτελεσματικά μεταξύ τους χρησιμοποιώντας διευθύνσεις πρωτοκόλλου διαδικτύου (IP). Όλες οι έξυπνες οικιακές συσκευές είναι συνδεδεμένες στο Διαδίκτυο σε ένα έξυπνο οικιακό περιβάλλον. Καθώς ο αριθμός των συσκευών αυξάνεται στο έξυπνο οικιακό περιβάλλον, αυξάνονται επίσης οι πιθανότητες κακόβουλων επιθέσεων [4]. Εάν οι έξυπνες οικιακές συσκευές λειτουργούν ανεξάρτητα, οι πιθανότητες κακόβουλων επιθέσεων μειώνονται επίσης. Προς το παρόν, οι έξυπνες οικιακές συσκευές είναι προσβάσιμες μέσω του Διαδικτύου παντού ανά πάσα στιγμή. Έτσι, αυξάνει τις πιθανότητες κακόβουλων επιθέσεων σε αυτές τις συσκευές [5][29]. Ένα έξυπνο σπίτι αποτελείται από τέσσερα μέρη: την πλατφόρμα υπηρεσιών, έξυπνες συσκευές, πύλη οικίας και ένα οικιακό δίκτυο. Στο έξυπνο σπίτι, πολλές συσκευές είναι συνδεδεμένες και μοιράζονται έξυπνα πληροφορίες χρησιμοποιώντας ένα οικιακό δίκτυο. Κατά συνέπεια, υπάρχει μια αρχική πύλη που ελέγχει τη ροή πληροφοριών μεταξύ έξυπνων συσκευών που είναι συνδεδεμένες στο εξωτερικό δίκτυο. Η πλατφόρμα υπηρεσιών χρησιμοποιεί τις υπηρεσίες ενός παρόχου υπηρεσιών που παρέχει διαφορετικές υπηρεσίες στο οικιακό δίκτυο.

5.1.1. Στόχοι ασφάλειας στο σπίτι

Η σαφής περιγραφή των στόχων ασφαλείας που αναμένεται να επιτύχει το έξυπνο οικιακό περιβάλλον, χρησιμεύει ως το πρώτο βήμα στην προσπάθεια εξασφάλισης συνεπούς λειτουργίας. Για τους σκοπούς αυτού του εγγράφου, λαμβάνοντας υπόψη έξι κοινώς αποδεκτούς στόχους που περιγράφονται παρακάτω [6] ως τους πιο σημαντικούς για την έξυπνη ασφάλεια στο σπίτι, αυτοί οι στόχοι είναι:

- Εμπιστευτικότητα: η διασφάλιση ότι τα δεδομένα θα αποκαλυφθούν μόνο σε εξουσιοδοτημένα άτομα ή συστήματα.
- Ακεραιότητα: Μια έξυπνη συσκευή θα είναι προσβάσιμη μέσω του ασύρματου δικτύου, προκειμένου να χρειάζεται ένα σύστημα ασφαλείας. ένας εισβολέας είναι σε θέση να εισαγάγει μια κακοήθη εφαρμογή λογισμικού και να αλλάξει έναν σκοπό υπηρεσίας μέσω κακόβουλου κώδικα. Για το λόγο, ενώ δεν είναι ακεραιότητα, ολόκληρο το έξυπνο οικιακό σύστημα θα μολυνθεί με κακόβουλο κώδικα από έναν εισβολέα και έτσι η παροχή έξυπνης οικιακής υπηρεσίας μπορεί να μειωθεί. Επομένως, απαιτείται η ακεραιότητα της έξυπνης οικιακής υπηρεσίας. Για να επιβεβαιώσετε την ακεραιότητα των έξυπνων συσκευών, είναι απαραίτητο να χρησιμοποιήσετε μια λειτουργία κατακερματισμού και μια ψηφιακή υπογραφή για ζωτικά δεδομένα ή κωδικούς μονάδων [7][8][30].
- Διαθεσιμότητα: Μια έξυπνη συσκευή στέλνει και λαμβάνει δεδομένα από και προς την επιφάνεια μέσω ασύρματου δικτύου, εάν είναι πληροφορίες εκτός σύνδεσης, είναι σε θέση να κατασκευάσει και να τροποποιήσει τα δεδομένα. Τα πλασματικά δεδομένα μπορούν να προκαλέσουν δυσλειτουργία έξυπνων συσκευών που επιδεινώνουν την ευκολία ενός χρήστη για έξυπνες συσκευές. Η επιδείνωση της ευχρηστίας μπορεί να οδηγήσει σε υπερφόρτωση των υπηρεσιών και η δυσλειτουργία μπορεί να προκαλέσει οικονομικές απώλειες από την αύξηση του ηλεκτρικού ρυθμού και συνεπώς τον κίνδυνο ζωής. Για να διασφαλιστεί η

διαθεσιμότητα, είναι απαραίτητο να περιοριστούν διαφορετικές ενέργειες από τις βασικές λειτουργίες και να παρέχεται πρόσβαση σε λειτουργική πρόσβαση [9] [10][31].

- Αυθεντικότητα: πολλές συσκευές των οποίων η ασφάλεια δεν λαμβάνεται υπόψη. Εάν ένας επιτιθέμενος ΑΝ εισάγει μια παράγωγη λειτουργική μονάδα ή έναν κακοήθη κωδικό σε μια εξαιρετικά έξυπνη συσκευή, είναι πιθανό να μολύνει ένα έξυπνο περιβάλλον υπηρεσίας σπιτιού και να κάνει τη συσκευή που χρησιμοποιείται για κακόβουλες λειτουργίες, όπως κατανεμημένη άρνηση υπηρεσίας (DDoS), άρνηση υπηρεσίας (DoS και ιδιωτική απαλλαγή δεδομένων. Επιπλέον, εάν ένας επιτιθέμενος ΑΝ μεταμφιέζει μια τροποποιημένη μονάδα ως κανονική μονάδα, η μονάδα μπορεί να λειτουργήσει την πίσω πόρτα του κλειδιού για κακόβουλη ενέργεια που μπορεί να μειώσει τη λειτουργία της κανονικής μονάδας και έτσι να επιδεινώσει τη διαθεσιμότητα. Επομένως, πρέπει να παρέχεται έλεγχος ταυτότητας μιας έξυπνης συσκευής. Για τον έλεγχο ταυτότητας, μπορείτε να χρησιμοποιήσετε ένα πιστοποιητικό [8] [11][32].
- Εξουσιοδότηση: η διασφάλιση ότι τα δικαιώματα πρόσβασης κάθε οντότητας στο σύστημα καθορίζονται για τους σκοπούς του ελέγχου πρόσβασης [11][33].
- Μη απόρριψη: η διαβεβαίωση ότι θα υπάρχει αναμφισβήτητη απόδειξη για την επαλήθευση της αλήθειας οποιασδήποτε αξίωσης μιας οντότητας. Υπάρχουν τρεις διαφορετικές ορολογίες, ασφαλές κανάλι, εμπιστευτικό κανάλι και αυθεντικό κανάλι. Ένα ασφαλές κανάλι είναι ένας τρόπος ασφαλούς μεταφοράς δεδομένων ενάντια στις προσπάθειες παραβίασης και ακρόασης. Εν τω μεταξύ, το εμπιστευτικό κανάλι είναι ένας τρόπος για τη μεταφορά δεδομένων που είναι ανθεκτική σε απόπειρες ακρόασης αν και δεν αντιστέκεται πάντοτε σε παραβίαση. Επιπλέον, το αυθεντικό κανάλι είναι ένας τρόπος μεταφοράς δεδομένων που δεν επηρεάζονται από παραβίαση αν και δεν είναι απαραίτητα ανθεκτικό σε απόπειρες ακρόασης. Για τους σκοπούς της επιβολής του νόμου, είναι απαραίτητο να επιλέξετε ένα ασφαλές

κανάλι, επειδή η χρήση μόνο εμπιστευτικού ή αυθεντικού καναλιού δεν αρκεί [12][34].

5.1.2. Επιθέσεις ασφαλείας

Οι απειλές για την ασφάλεια εντός του έξυπνου οικιακού περιβάλλοντος συνήθως προσπαθούν να θέσουν σε κίνδυνο έναν ή περισσότερους από τους στόχους ασφαλείας που μόλις περιγράφηκαν. Αυτές οι απειλές μπορούν να ταξινομηθούν σε δύο ευρείες κατηγορίες. Στην πρώτη κατηγορία, δηλαδή «παθητικές επιθέσεις», αυτή η μελέτη τοποθετεί επιθέσεις που προσπαθούν να μάθουν ή να χρησιμοποιήσουν πληροφορίες από το σύστημα χωρίς να επηρεάσουν τους πόρους του συστήματος. Με άλλα λόγια, σε παθητικές επιθέσεις, ο αντίπαλος σκοπεύει να λάβει πληροφορίες που μεταδίδονται όχι για να τις τροποποιήσει αλλά για να μάθει κάτι από αυτήν. Οι παθητικές επιθέσεις μπορούν να λάβουν τη μορφή υποκλοπής ή ανάλυσης κίνησης. Παρατηρώντας, οι συγγραφείς αναφέρονται στη μη εξουσιοδοτημένη παρακολούθηση μιας συνεχιζόμενης επικοινωνίας χωρίς τη συγκατάθεση των επικοινωνιακών μερών. [35]

Με την ανάλυση της κυκλοφορίας, οι συγγραφείς αναφέρονται σε κάτι πιο λεπτό. Αντί να προσπαθεί να κρατήσει το περιεχόμενο των μηνυμάτων, όπως σε μια επίθεση υποκλοπής, στην ανάλυση της κυκλοφορίας, ο αντίπαλος παρακολουθεί τα μοτίβα κυκλοφορίας προκειμένου να εξαγάγει χρήσιμες πληροφορίες από αυτά. Και οι δύο αυτές επιθέσεις θεωρούνται δύσκολο να εντοπιστούν αφού δεν αλλοιώνουν δεδομένα. Έτσι, κατά την αντιμετώπισή τους προσπαθούν να επικεντρωθούν στην πρόληψη παρά στην ανίχνευση. Η δεύτερη κατηγορία, δηλαδή οι «ενεργές επιθέσεις», είναι η κατηγορία όπου οι επιθέσεις επιχειρούν να αλλάξουν πόρους του συστήματος ή να επηρεάσουν τη λειτουργία του. Οι ενεργές επιθέσεις μπορεί να περιλαμβάνουν κάποια τροποποίηση των δεδομένων ή την εισαγωγή ψευδών δεδομένων στο σύστημα. [36]

Οι πιο συνηθισμένες μεταξύ αυτών των επιθέσεων είναι μια μεταμφίεση, επανάληψη, τροποποίηση μηνυμάτων, άρνηση υπηρεσίας και κακόβουλο λογισμικό. Μια μεταμφίεση επιτίθεται όταν ένας εισβολέας προσποιείται ότι είναι νόμιμη οντότητα για να αποκτήσει προνόμια. Μια επίθεση επανάληψης περιλαμβάνει την παθητική σύλληψη μηνυμάτων στην επικοινωνία και την αναμετάδοσή τους για να παράγει ένα μη εξουσιοδοτημένο αποτέλεσμα. Μια επίθεση τροποποίησης μηνυμάτων, περιλαμβάνει την τροποποίηση του περιεχομένου ενός νόμιμου μηνύματος ή την καθυστέρηση ή την αναδιάταξη μιας ροής μηνυμάτων, με στόχο την παραγωγή μη εξουσιοδοτημένου αποτελέσματος [11]. Μια επίθεση άρνησης υπηρεσίας στοχεύει είτε προσωρινά είτε μόνιμα να διακόψει ή να αναστείλει τη διαθεσιμότητα των πόρων επικοινωνίας ενός συστήματος. Τέλος, κακόβουλες επιθέσεις λογισμικού, είναι επιθέσεις που στοχεύουν στην εκμετάλλευση εσωτερικών τρωτών σημείων για τροποποίηση, καταστροφή και κλοπή πληροφοριών ή απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πόρους συστήματος [13][37].

5.1.3. Αξιολόγηση επιπτώσεων

Για την αξιολόγηση της κρίσιμης σημασίας και της ευαισθησίας ορισμένων αλληλεπιδράσεων και την αξιολόγηση του επιπέδου των επιπτώσεων των απειλών κατά αυτών των αλληλεπιδράσεων στο περιβάλλον έξυπνου σπιτιού / έξυπνου δικτύου, αυτή η μελέτη υιοθετεί το FIPS 199, κριτήρια αξιολόγησης επιπτώσεων [1]. Το FIPS199 χαρακτηρίζει τον πιθανό αντίκτυπο των απειλών ως Χαμηλό, Μέτριο ή Υψηλό. Όπου λέγεται πιθανός αντίκτυπος [13][38]:

Χαμηλός (L): εάν η παραβίαση ενός ή περισσοτέρων από τους στόχους ασφαλείας που περιγράφονται παραπάνω μπορεί να αναμένεται να έχει περιορισμένη αρνητική επίδραση στις λειτουργίες έξυπνου σπιτιού, τα περιουσιακά στοιχεία ή τα άτομα. Περιορισμένη αρνητική επίδραση θα μπορούσε να σημαίνει την υποβάθμιση της ικανότητας μιας οντότητας να εκτελεί αποτελεσματικά τις κύριες λειτουργίες της, μικρές ζημιές σε περιουσιακά στοιχεία, μικρές οικονομικές απώλειες ή μικρή ζημιά σε άτομα.

Μέτριος (M): εάν η παραβίαση ενός ή περισσοτέρων από τους στόχους ασφαλείας που περιγράφονται παραπάνω μπορεί να αναμένεται να έχει σημαντική δυσμενή επίδραση στις λειτουργίες έξυπνου σπιτιού, τα περιουσιακά στοιχεία ή τα άτομα. Σημαντική ανεπιθύμητη ενέργεια θα μπορούσε να σημαίνει σημαντική υποβάθμιση της ικανότητας μιας οντότητας να εκτελεί αποτελεσματικά τις πρωταρχικές της λειτουργίες, σημαντική ζημιά σε περιουσιακά στοιχεία, σημαντικές οικονομικές απώλειες ή σημαντική ζημία σε άτομα (μη συμπεριλαμβανομένης της απώλειας ζωής ή απειλητικών για τη ζωή τραυματισμών). [39]

Υψηλός (H): εάν η παραβίαση ενός ή περισσοτέρων από τους στόχους ασφαλείας που περιγράφονται παραπάνω μπορεί να αναμένεται να έχει σοβαρή ή καταστροφική δυσμενή επίδραση στις λειτουργίες έξυπνου σπιτιού, τα περιουσιακά στοιχεία ή τα άτομα. Σοβαρή ή καταστροφική δυσμενή επίδραση θα μπορούσε να σημαίνει σοβαρή υποβάθμιση ή απώλεια της ικανότητας μιας οντότητας να εκτελεί τις κύριες λειτουργίες της, σοβαρές ζημιές σε περιουσιακά στοιχεία, σημαντικές οικονομικές απώλειες ή σοβαρή ζημιά σε άτομα [40].

Πίνακας 9. Ζητήματα ασφάλειας στο σπίτι

Scenario num:	Possible Threads	Security Goals Compromised	Degree of Impact
SH_1	Eavesdropping (N) Traffic Analysis (N) Message Modification (N) Replay Attack (N) EMS Impersonation (SH)	Confidentiality Integrity Authenticity	L-M
SH_2	Repudiation (N) Message Modification(N) Replay Attack (N)	Non repudiation Integrity Authentication	M
SH_3	Tampering/Reversal/ Removal of Meter (SH) Illegal Software Modification/Update(SH)	Authentication Integrity	L
SH_4	Customer Impersonation (N) Device Impersonation (SH) Message Modification(N) Replay attack(N) Repudiation(N)	Integrity Non repudiation Authentication	L-H
SH_5	Customer Impersonation(N) Eavesdropping/Message(N) Interception (N)	Confidentiality Integrity Authenticity	L-M

5.2. Υφιστάμενες μελέτες για έξυπνη οικιακή ασφάλεια

Το Διαδίκτυο των πραγμάτων είναι ένα σχετικά νέο πράγμα στον κόσμο της τεχνολογίας σήμερα. Ωστόσο, το Διαδίκτυο των πραγμάτων προβλέπεται ότι θα είναι μια εξαιρετική τάση στο μέλλον. Σε αυτήν την ενότητα, εξετάζονται τα προηγούμενα έργα που σχετίζονται με την ασφάλεια και το απόρρητο στο έξυπνο σπίτι. Εφαρμογές ασφάλειας και απορρήτου. Άλλα έργα ταξινομούνται σε μικρές κατηγορίες σύμφωνα με τις δραστηριότητες ασφάλειας και την αποτελεσματικότητα σε συστήματα έξυπνων σπιτιών που βασίζονται στο IoT. Αυτά τα έργα επικεντρώνονται σε συστήματα ασφαλείας και εφαρμογές για έξυπνα σπίτια χρησιμοποιώντας IoT. Ασφαλής διαχείριση δεδομένων σε διάφορες συσκευές, βελτίωση της ασφάλειας σε έξυπνα οικιακά συστήματα και

εφαρμογές, καθώς και ασφάλεια συστήματος δικτύου και έλεγχος απορρήτου για οικιακές πληροφορίες και συσκευές IoT [18][42].

Άλλα έργα συζητούν την ασφαλή αρχιτεκτονική υγειονομικής περίθαλψης και την επικοινωνία των κόμβων σε ένα Πρωτόκολλο Περιορισμένης Εφαρμογής (CoAP, ένα πρωτόκολλο επιπέδου εφαρμογής που είναι προετοιμασμένο για χρήση σε συσκευές Διαδικτύου σε έξυπνα σπίτια IoT, όπως κόμβοι δικτύου ασύρματων αισθητήρων) [19], καθώς και προκλήσεις ασφάλειας μεταξύ ετερογενών συσκευών και διαφορετικών εφαρμογών σε έξυπνα σπίτια [7]. Ορισμένες μελέτες επικεντρώνονται στην ασφάλεια κωδικών πρόσβασης και εφαρμογές για έξυπνα οικιακά συστήματα IoT [20], ασφαλείς ενημερώσεις λογισμικού σε έξυπνες οικιακές συσκευές και συσκευές συστήματος ασφαλείας (π.χ. κάμερες παρακολούθησης) και τη χρήση τους σε έξυπνα σπίτια [22]. Οικιακός αυτοματισμός και απειλές ασφάλειας ορίζονται επίσης, Μια νέα λύση παρουσιάζεται για την αντιμετώπιση της μείωσης του κινδύνου σε περιπτώσεις παραβίασης της ιδιωτικής ζωής σε έξυπνα συστήματα διαχείρισης ενέργειας [23][43].

Το έργο του Andrea Zanella et. al. πρότεινε τη χρήση ετικετών αναγνώρισης ραδιοσυχνοτήτων (RFID) για την επιτυχή αναγνώριση διαφόρων αντικειμένων μέσα σε ένα έξυπνο ψυγείο. Αυτή η τεχνική θα μπορούσε να επεκταθεί για να βελτιώσει την ασφάλεια του σπιτιού, αλλά απαιτεί τα περισσότερα αντικείμενα μέσα στο σπίτι, συμπεριλαμβανομένων των κατοίκων του σπιτιού που είναι εξοπλισμένα με ετικέτες RFID, κάτι που είναι άβολο και δύσκολο να εφαρμοστεί, λαμβάνοντας υπόψη την ξεχασμένη ανθρώπινη φύση [44].

Η αρχιτεκτονική ασφαλείας που προωθείται από το απόρρητο που προτείνει ο S. Lee εφαρμόζεται σε ένα έξυπνο οικιακό περιβάλλον. Η αρχιτεκτονική έχει άμυνα ενάντια σε επιθέσεις όπως η εισβολή προσωπικών πληροφοριών και η επίθεση έκρηξης μεταξύ ενός εισβολέα και συσκευών σε ένα έξυπνο περιβάλλον σπιτιού. Η μελέτη πρότεινε ένα πλαίσιο ασφάλειας που εφαρμόζεται σε ένα έξυπνο οικιακό περιβάλλον, το οποίο περιλαμβάνει κρυπτογράφηση, έλεγχο πρόσβασης, ψηφιακή υπογραφή, έλεγχο ταυτότητας και καταγραφή. Το προτεινόμενο πλαίσιο βασίζεται στο πλαίσιο ανοιχτού κώδικα «AllJoyn». Αποτελείται από συσκευή, AllJoyn Core, μονάδα άδειας, και

ACL και άγκυρα εμπιστοσύνης πιστοποιητικού πολιτικής. Στο πλαίσιο, τα κρίσιμα δεδομένα μεταδίδονται μετά τον έλεγχο ταυτότητας μεταξύ συσκευών. Ο διαχειριστής ασφαλείας του τελικού χρήστη παρέχει υπηρεσίες παροχής και συντήρησης ασφαλείας για συσκευές. Δημιουργείται μια συνεδρία μεταξύ των εφαρμογών συσκευών για μετάδοση δεδομένων.

Ο έλεγχος ταυτότητας πραγματοποιείται με τη χρήση κλειδιού ομάδας και πιστοποιητικού. Οι πιστοποιημένες συσκευές μεταδίδουν τα μηνύματα κρυπτογραφημένα με μια δεδομένη πολιτική. [45] Ο S. Lee χρησιμοποιεί τη διαδικασία ελέγχου ταυτότητας έξυπνων συσκευών και ελαφρού ομοιόμορφου κρυπτοσυστήματος βασισμένου σε πλέγμα για την κρυπτογράφηση ενός μηνύματος. Χωρίζεται στη φάση προετοιμασίας και ανάγνωσης. Δεδομένου ότι το σχήμα επιτρέπει την παρακολούθηση του ελέγχου ταυτότητας μεταξύ έξυπνων συσκευών, κέντρου ελέγχου, έξυπνου μετρητή και επικοινωνίας μεταξύ AP, το κέντρο ελέγχου μπορεί να αποκρυπτογραφήσει ένα κρυπτογραφημένο μήνυμα για τη βελτίωση της εμπιστευτικότητας και του απορρήτου των συσκευών. Για τον έλεγχο ταυτότητας smartphone και την αποστολή μηνυμάτων με ασφάλεια σε ένα έξυπνο οικιακό περιβάλλον, στην διεθνή βιβλιογραφία χρησιμοποιείται ένας αλγόριθμος κρυπτογράφησης και μια λειτουργία κατακερματισμού. Ο αλγόριθμος εφαρμόζει AES256, ephemeral Diffie-Hellman key exchange, και RC4 hash function. Με τη χρήση ενός κεντρικού διανομέα, όλα τα μηνύματα προς μετάδοση παρακολουθούνται και τα μηνύματα που αποστέλλονται από smartphone περνούν τον κεντρικό διανομέα για μετάδοση. Ένα μήνυμα προς μετάδοση κρυπτογραφείται με τρεις αλγόριθμους και δημιουργείται μια τιμή κατακερματισμού. [46]Το 2014, η άποψη του Διαδικτύου των πραγμάτων έχει εξελιχθεί μαζί με την ανάπτυξη της τεχνολογίας και την ενσωμάτωση πολλών τεχνολογιών, που κυμαίνονται από την ασύρματη επικοινωνία στο Διαδίκτυο και από τα ενσωματωμένα συστήματα έως τα μικροηλεκτρομηχανικά συστήματα (MEMS), αυτό σημαίνει ότι όλα τα πεδία ο κόσμος θα συμβάλει στην οικοδόμηση του Διαδικτύου των πραγμάτων [3].

6. Συμπεράσματα

Συνοψίζοντας, συμπεραίνουμε το IoT είναι σύμφυτο με ζητήματα προσωπικών δεδομένων. Πιο συγκεκριμένα παρουσιάζονται κίνδυνοι για ιδιωτικότητα και προστασία προσωπικών δεδομένων:

- Χρήση για δευτερεύοντες σκοπούς
- Απουσία δυνατότητας συγκατάθεσης
- Δημιουργία ατομικού προφίλ
- Λεπτομερή παρακολούθηση
- Λήψη αυτοματοποιημένων αποφάσεων
- Απουσία δυνατότητας να παραμένει κανείς ανώνυμος

Έπειτα, παρουσιάζονται ζητήματα σχετικά με έλλειψη ασφάλειας:

- Ανάγκη βελτιστοποίησης των υπολογιστικών πόρων/ενέργειας από αισθητήρες και αντικείμενα, υλοποίηση μέτρων για εξασφάλιση εμπιστευτικότητας/ακεραιότητας/διαθεσιμότητας
- Διαφορετικά επίπεδα επεξεργασίας που συνεπάγονται δυσκολία στον συντονισμό εμπλεκομένων μερών (stakeholders). Ως εκ τούτου παρατηρείται η ύπαρξη τρωτών σημείων. Για παράδειγμα, οι περισσότεροι από τους αισθητήρες δεν έχουν τη δυνατότητα να δημιουργήσουν κρυπτογραφημένη σύνδεση, επειδή η χρήση πόρων είναι υπερβολική και έχει συνέπεια στην φυσική αυτονομία της συσκευής

Ακόμα, στα ζητήματα ιδιωτικότητας συμπεριλαμβάνεται η φορητότητα και η συγκατάθεση σχετικά με το ποιος πρέπει να την παρέχει (ιδιοκτήτης συσκευής, φέρων συσκευή, υποκείμενο των δεδομένων ...), σε ποιον και πότε.

Σε μια έξυπνη πόλη, το IoT παρεμβαίνει έντονα στη ζωή των κατοίκων. Το IoT, το οποίο δεν είναι πλέον στα σπάργανα, παρουσιάζει διάφορες ευπάθειες και απειλές, που προκαλούνται από την τεχνολογική πρόοδο και πολλαπλασιάζονται λόγω της έλλειψης ευαισθητοποίησης των χρηστών. Αυξάνεται από την εκτεταμένη χρήση νέων τεχνολογιών όπως RFID, NFC, ZigBee, αισθητήρες, 3G και 4G που φέρνουν μαζί την προσαρμογή των

παραδοσιακών απειλών για την ασφάλεια πληροφοριών σε αυτό το νέο περιβάλλον, καθώς και την εμφάνιση νέων κινδύνων.

Τα προβλήματα που αντιμετωπίζονται εδώ είναι ενδιαφέροντα τόσο για τον καθένα από εμάς, ως πολίτες, όσο και για τους διαχειριστές πόλεων, τους εθνικούς και διεθνείς ρυθμιστικούς φορείς, ειδικά σε έναν κόσμο στον οποίο η διαχωριστική γραμμή μεταξύ της φυσικής και της εικονικής ζωής καθίσταται όλο και πιο δύσκολη. Σε αυτό το πλαίσιο, οι αστικοί διαχειριστές πρέπει να αντιμετωπίσουν προσεκτικά τις έννοιες της εμπιστοσύνης, του κινδύνου, της ασφάλειας και της ιδιωτικής ζωής. Οι αρχές της πόλης πρέπει να είναι καλά ενημερωμένες για όλα τα προβλήματα που σχετίζονται με έξυπνα πράγματα, χώρους, υπηρεσίες και ασφάλεια των πολιτών. Επίσης, οι λύσεις που προσφέρουν οι πάροχοι ασφαλείας πρέπει να είναι γνωστές και να επιλέγονται με μέγιστη διάκριση.

Στον τομέα της υγείας, μια ποικιλία ιατρικών συσκευών και εφαρμογών λογισμικού εφαρμόζονται για τη βελτίωση της ποιότητας των ιατρικών υπηρεσιών και παράγουν επίσης μεγάλες ποσότητες δεδομένων. Προς το παρόν, η σημασία των δεδομένων είναι αυτονόητη. Ο τρόπος αποτελεσματικής προστασίας της ασφάλειας και της ιδιωτικής ζωής των δεδομένων σε όλα τα στάδια της ροής δεδομένων θα κατέχει σημαντική θέση στη μελλοντική σχετική έρευνα. Ξεκινώντας από τις απαιτήσεις ασφάλειας και απορρήτου του MIoT, στην παρούσα εργασία μελετήθηκαν θέματα ασφάλειας και απορρήτου από πέντε τεχνικές πτυχές και παρουσιάστηκαν οι προκλήσεις της μελλοντικής έρευνας. Έχει δοθεί μεγάλη προσοχή στο MIoT. Ωστόσο, τα σχετικά πρότυπα και οι τεχνικές προδιαγραφές εξακολουθούν να βελτιώνονται, ειδικά οι ειδικές απαιτήσεις εφαρμογής της υγειονομικής περίθαλψης και απαιτείται πιο επιτυχημένη εξερεύνηση.

Το σύστημα ασφαλείας στο περιβάλλον Smart Home είναι ένα σύστημα που μπορεί να βοηθήσει τους αξιωματικούς ασφαλείας και τους κατοίκους του περιβάλλοντος να είναι σε θέση να παρακολουθούν το περιβάλλον. Αυτό στοχεύει στην ελαχιστοποίηση της πιθανότητας εγκληματικής επέμβασης τόσο από το εξωτερικό όσο και από το ίδιο το περιβάλλον. Το Smart Home προσφέρει μια πιο πρακτική ποιότητα ζωής εισάγοντας αυτοματισμό οικιακών

συσκευών και οικιακών βοηθών. Ο αυτοματισμός βασίζεται σε μια συνειδητοποίηση που λαμβάνεται από τα αποτελέσματα της παρακολούθησης του ίδιου του οικιακού περιβάλλοντος. Οι χρήστες μπορούν να ελέγχουν τις οικιακές συσκευές τους από απόσταση, για παράδειγμα όταν ο χρήστης κατευθύνεται προς το σπίτι του, είναι σε θέση να ενεργοποιήσει το κλιματιστικό για να κρυώσει το δωμάτιο, να ελέγξει τον θερμοσίφωνα για μπάνιο και ούτω καθεξής. Ένα από τα προβλήματα ασφαλείας στις συσκευές IoT είναι ότι ο προεπιλεγμένος κωδικός πρόσβασης στη συσκευή δεν μπορεί εύκολα να αλλάξει από τον χρήστη. Αυτό επιτρέπει σε έναν χάκερ να ελέγχει τη συσκευή σε μια επίθεση DDoS. Το λογισμικό που χρησιμοποιείται για τον έλεγχο της συσκευής είναι ένα πακέτο κακόβουλου λογισμικού που ονομάζεται Mirai.

Το ίδιο το κακόβουλο λογισμικό Mirai παρουσιάστηκε για πρώτη φορά από έναν χάκερ που ονομάζεται Anna-senpai σε ένα φόρουμ χάκερ. Από τότε, το Mirai εκτιμάται ότι έχει μολύνει εκατομμύρια συσκευές IoT σε όλο τον κόσμο. Επιπλέον, το Mirai είναι πολύ δύσκολο να εντοπιστεί και έτσι οι χάκερ αισθάνονται ασφαλέστεροι όταν το χρησιμοποιούν. Το Girai είναι ένα botnet ειδικά σχεδιασμένο για να επιτίθεται σε συσκευές IoT, όπως δρομολογητές, κάμερες CCTV, σε εκτυπωτές που είναι όλοι συνδεδεμένοι στο δίκτυο Internet.

Το Mirai botnet μπορεί να σαρώσει αυτόματα διάφορες συσκευές IoT. Ο στόχος είναι μια συσκευή IoT με αδύναμο σύστημα ασφαλείας, ειδικά συσκευές των οποίων το όνομα χρήστη και ο κωδικός πρόσβασης δεν έχουν αλλάξει [3]. Οι συσκευές που έχουν μολυνθεί από το Mirai θα συνεχίσουν να αναζητούν διευθύνσεις IP από άλλες συσκευές IoT, παρόλο που είναι συνδεδεμένες στο δίκτυο. Υπάρχει μια λίστα εξαιρέσεων διευθύνσεων IP που δεν θα μολυνθούν από τη Mirai, συμπεριλαμβανομένου του ιδιωτικού δικτύου και των διευθύνσεων IP διαφόρων τμημάτων στην Αμερική και ορισμένων εταιρειών. Αφού βρήκε με επιτυχία τη συσκευή IoT που ήταν ο στόχος, ο Mirai περιμένει τότε να ενεργοποιηθεί μια παραγγελία από τον χάκερ. Μόλις ενεργοποιηθεί, το Mirai θα στείλει ένα ανώνυμο πακέτο δεδομένων στον διακομιστή που είναι ο στόχος της επίθεσης. Το πακέτο δεδομένων είναι πράγματι μικρό, αλλά εάν αποστέλλεται ταυτόχρονα από εκατοντάδες εκατομμύρια συσκευές IoT, το αποτέλεσμα θα είναι μια επίθεση DDoS που δεν θα αποκλειστεί.

Υπάρχουν εκατοντάδες χιλιάδες συσκευές IoT που χρησιμοποιούν προεπιλεγμένες ρυθμίσεις, καθιστώντας τις ευάλωτες σε μολύνσεις. Αφού μολυνθεί, η συσκευή θα συνδεθεί στον διακομιστή εντολών και ελέγχου που δείχνει τον στόχο της επίθεσης. Η επίθεση Mirai μπορεί να προβλεφθεί με επανεκκίνηση του συστήματος. Ωστόσο, οι ειδικοί δήλωσαν ότι η επανεκκίνηση δεν εξάλειψε το Mirai, περιορίζοντας μόνο τις επιθέσεις για λίγο. Επειδή μέσα σε λίγα λεπτά, ο Μιράι μπορεί να αναπτύξει ξανά τα στρατεύματά του. Μια άλλη επιλογή για να σταματήσουν οι επιθέσεις Mirai είναι να αλλάξει ο προεπιλεγμένος κωδικός πρόσβασης σε συσκευές IoT. Ο κατασκευαστής Mirai δήλωσε ότι αυτό το botnet δημιουργήθηκε εν αναμονή της υψηλής ευαισθητοποίησης διαφόρων ιδρυμάτων. Με το αυξανόμενο επίπεδο ευαισθητοποίησης για την ασφάλεια, κατηγορήθηκε. Εκτός από το Mirai και την εγκατάσταση κλειδιών (KRACKs), υπάρχει επίσης μια επίθεση Bricker Bot. Ο Bricker Bot είναι υπεύθυνος για το χτύπημα μιας μη ασφαλούς συσκευής IoT εκτός σύνδεσης, αντί να το πειραχτεί σε άλλο botnet και να το χρησιμοποιήσει για επιθέσεις DDoS. Αυτό είναι το τρίτο botnet που στοχεύει μη ασφαλείς συσκευές IoT, αλλά η μόνη που είναι καταστροφική. Ο δεύτερος, ονομαζόμενος Hajime, σπάζει τις συσκευές IoT, αλλά αντί να μπλοκάρουν, απενεργοποιούν την απομακρυσμένη πρόσβαση σε συσκευές από το Διαδίκτυο. Φυσικά, το Mirai είναι το πρώτο, αλλά έχει τον ίδιο στόχο με άλλα botnets, δηλαδή να υποδουλώσει συσκευές IoT και να χρησιμοποιήσει την υπολογιστική δύναμη της συλλογής bots για οτιδήποτε μπορεί να ευχαριστήσει τους απειλητικούς παράγοντες πίσω από αυτό.

Η βιβλιογραφική επισκόπηση όπως ολοκληρώνεται στην παρούσα εργασία δεν επέτρεψε την μελέτη πολλών κρίσιμων ζητημάτων που αφορούν ζητήματα ιδιωτικότητας στο Iot. Με την ραγδαία ανάπτυξη της τεχνολογίας ολοένα και εμφανίζονται νέα ζητήματα ιδιωτικότητας τα οποία χρήζουν επισταμένης μελέτης.

Μελλοντικά θα ήταν σκόπιμο να πραγματοποιηθεί επιπλέον έρευνα σχετικά με ζητήματα ιδιωτικότητας και ασφάλειας στο διαδίκτυο των πραγμάτων που επαφίονται στη λειτουργία επιχειρήσεων και στη δραστηριότητα των καταναλωτών. Για παράδειγμα, θα ήταν σκόπιμο να ερευνηθεί η επιρροή που ασκούν στον καταναλωτή, η εξέλιξη των κοινωνικών δικτύων και της

τεχνολογίας. Με άλλη διατύπωση, πώς οι επιχειρήσεις μπορούν να αποκτήσουν μεγαλύτερη δημοφιλία, αλλά και πώς να επιτύχουν αύξηση των κερδών τους, μέσω της συλλογής όλο και περισσότερων στοιχείων καταναλωτών και χρηστών από τα κοινωνικά δίκτυα.

Βιβλιογραφία

1. Rida Khatoun and Sherali Zeadally. Smart cities: concepts, architectures, researchopportunities. Communications of the ACM, 59(8):46–57, 2016.

2. Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things. Technical report,Gartner, Inc, 2016.

3. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and MarimuthuPalaniswami. Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7):1645 – 1660, 2013.

4. Coordination And Support Action for Global RFID-related Activities and Standardisation: RFID and the Inclusive Model for the Internet of Things. Technicalreport, CASAGRAS, 2009.

5. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A

survey. Computer networks, 54(15):2787–2805, 2010.

6. Debasis Bandyopadhyay and Jaydip Sen. Internet of things: Applications andchallenges in technology and standardization. Wireless Personal Communications,58(1):49–69, 2011.

7. Debiao He and Sherali Zeadally. An analysis of rfid authentication schemes forinternet of things in healthcare environment using elliptic curve cryptography.IEEE internet of things journal, 2(1):72–83, 2015.

8. Next Generation Networks - Frameworks and functional architecture models. Recommendation ITU-T Y.2060. Overview of the Internet of things. Technical report,International Telecommunication Union, 2012.

9. Oladayo Bello, Sherali Zeadally, and Mohamad Badra. Network layer interoperation of device-to-device communication technologies in internet of things(iot). Ad Hoc Networks, 57:52 – 62, 2017. Special Issue on Internet of Thingsand Smart Cities: security, privacy and new technologies.

10. Hanna Okkonen, Oleksiy Mazhelis, Petri Ahokangas, Pasi Pussinen, Mervi Rajahonka, Riikka Siuruainen, Seppo Leminen, Alexey Shveykovskiy, Jenni Myllykoski, and Henna Warma. Internet-of-things market, value networks, and business models: state of the art report. Computer science and information systemsreports. TR, Technical reports 39., 2013.

11. Damian Christie. IoT Standards, Why so many? https : / /www.linkedin.com / pulse / iot - standards - why - so - many -damian-christie, 2016.

12. Xue Li, Jing Liu, Quan Z. Sheng, Sherali Zeadally, and Weicai Zhong. Tmsrfid: Temporal management of large-scale rfid applications. Information Systems Frontiers, 13(4):481–500, 2011.

13. Quan Z Sheng, Xue Li, and Sherali Zeadally. Enabling next-generation rfid applications: Solutions and challenges. Computer, 41(9):21–28, 2008.

14. Wordpress. The Internet of Things Protocol stack âA ¸S from sensors to business ˘ value. https://entrepreneurshiptalk.wordpress.com/2014/01/ 29/the-internet-of-thing-protocol-stack-from-sensorsto-business-value/, 2014.

15 Colin Harrison, Barbara Eckman, Rick Hamilton, Perry Hartswick, Jayant Kalagnanam, Jurij Paraszczak, and Peter Williams. Foundations for smarter cities. IBM Journal of Research and Development, 54(4):1–16, 2010.

16. Jiong Jin, Jayavardhana Gubbi, Slaven Marusic, and Marimuthu Palaniswami. An information framework for creating a smart city through internet of things. IEEE Internet of Things Journal, 1(2):112–121, 2014.

17. LoRa Alliance. Wide Area Networks For IoT. https : / / www.lora - alliance.org, 2017.

18. LoRa Alliance. LoRa Technology. https://www.lora-alliance.org/ What-Is-LoRa/Technology, 2017.

19. Keith E Nolan, Wael Guibene, and Mark Y Kelly. An evaluation of low power wide area network technologies for the Internet of Things. In Wireless Communications and Mobile Computing Conference (IWCMC), 2016 International, pages 439–444. IEEE, 2016.

20. LoRaWAN, What is it. A Technical Overview of LoRa and LoRaWAN. Technical report, LoRa Alliance. Technical Marketing Workgroup 1.0, November 2015.

21. CNXSOFT. Comparison Table of Low Power WAN Standards for Industrial Applications. http : / / www.cnx - software.com / 2015 / 09 / 21/comparison-table- of- low- power- wan- standards- forindustrial-applications/, 2015.

22. Worldwide Internet of Things Forecast Update, 2016âA ¸S2020. Technical report, ˇ IDC, 2016.

23. J. A. Guerrero-Ibáñez, C. Flores-Cortés, and Sherali Zeadally. Vehicular Adhoc Networks (VANETs): Architecture, Protocols and Applications, pages 49–70. Springer London, 2013.

24. J. A. Guerrero-ibanez, S. Zeadally, and J. Contreras-Castillo. Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. IEEE Wireless Communications, 22(6):122–128, 2015.

25. Tomás Sánchez López, Damith C Ranasinghe, Mark Harrison, and Duncan McFarlane. Adding sense to the Internet of Things. Personal and Ubiquitous Computing, 16(3):291–308, 2012.

26. Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities. IEEE Internet of Things journal, 1(1):22– 32, 2014.

27. A. Jose, R. M.- SmartCR, and undefined 2015, “Smart home automation security,” researchgate.net.

28. G. Agosta, A. Antonini, … A. B.-S. T., and undefined 2015, “Cyber-security analysis and evaluation for smart home management solutions,” ieeexplore.ieee.org.

29. S. Chitnis, N. Deshpande, and A. Shaligram, “An Investigative Study for Smart Home Security: Issues, Challenges, and Countermeasures,” Wirel. Sens. Netw., vol. 08, no. 04, pp. 61–68, Apr. 2016.

30. Y. Prayudi and A. Ashari, “A Study on Secure Communication for Digital Forensics Environment,” Artic. Int. J. Sci. Eng. Res., 2015.

31. N. Komninos, E. Philippou, and A. Pitsillides, “Survey in Smart Grid and Smart Home Security: Issues, Challenges, and Countermeasures,” IEEE Commun. Surv. Tutorials, vol. 16, no. 4, pp. 1933–1954, 2014.

32. C. Huth, J. Zibuschka, P. Duplys, and T. Guneysu, “Securing systems on the Internet of Things via physical properties of devices and communications,” in 2015 Annual IEEE Systems Conference (SysCon) Proceedings, 2015, pp. 8–13.

33. J. Greensmith and Julie, “Securing the Internet of Things with Responsive Artificial Immune Systems,” in Proceedings of 2015 on Genetic and Evolutionary Computation Conference - GECCO ’15, 2015, pp. 113– 120.

34. R. A. Rahman and B. Shah, “Security analysis of IoT protocols: A focus in CoAP,” in 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), 2016, pp. 1–7.

35. V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, “Network-level security and privacy control for smart-home IoT devices,” in 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking, and Communications (WiMob), 2015, pp. 163–167.

36. I. Sanchez et al., “Privacy leakages in Smart Home wireless technologies,” in 2014 International Carnahan Conference on Security Technology (ICCST), 2014, pp. 1–6.

37. O. Bergmann, S. Gerdes, … S. S.-W., and undefined 2012, “Secure bootstrapping of nodes in a CoAP network,” ieeexplore.ieee.org.

38. V. L. Shivraj, M. A. Rajan, M. Singh, and P. Balamuralidhar, “One time password authentication scheme based on elliptic curves for Internet of Things (IoT),” in 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), 2015, pp. 1–6.

39. A. O. Santin, J. E. Marynowski, A. Witkovski, A. Santin, V. Abreu, and J. Marynowski, “An IdM and Key-based Authentication Method for providing Single Sign-On in IoT Secure E-Voting System View project Testing the Fault Tolerance and Security of MapReduce Systems View project An IdM and Key-based Authentication Method for providing Single Sign-On in IoT.”

40. P. Rajiv, R. Raj, and M. Chandra, “Email based remote access and surveillance system for smart home infrastructure,” Perspect. Sci., vol. 8, pp. 459–461, Sep. 2016.

41. A. Ukil, S. Bandyopadhyay, and A. Pal, “Privacy for IoT: Involuntary privacy enablement for smart energy systems,” in 2015 IEEE International Conference on Communications (ICC), 2015, pp. 536–541.

42. D. Konidala, D. Kim, … C. Y.-J. of I., and undefined 2011, “Security framework for RFID-based applications in smart home environment,” koreascience.or.kr.

43. O. Tomanek and L. Kencl, “Security and privacy of using AllJoyn IoT framework at home and beyond,” in 2016 2nd International Conference on Intelligent Green Building and Smart Grid (IGBSG), 2016, pp. 1–6.

44. T. Mantoro, M. A. Ayu, and S. M. binti Mahmod, “Securing the authentication and message integrity for Smart Home using smart phone,” in 2014 International Conference on Multimedia Computing and Systems (ICMCS), 2014, pp. 985–989.

45. J. He, Q. Xiao, P. He, and M. S. Pathan, “An Adaptive Privacy Protection Method for Smart Home Environments Using Supervised Learning,” 2017.

46. B. Ali, A. Awad, B. Ali, and A. I. Awad, “Cyber and Physical Security Vulnerability Assessment for IoTBased Smart Homes,” Sensors, vol. 18, no. 3, p. 817, Mar. 2018.

47. Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: a review. Security and Communication Networks, 2018.

48. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250-1258.