ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Πρόγραμμα Σπουδών
Τμήματος Μηχανικών Πληροφορικής Τ.Ε. Λάρισας

Διαδίκτυο των Πραγμάτων με δίκτυο 5G: Η εξέλιξη της καθημερινότητας και κίνδυνοι φυσικών και ηλεκτρονικών επιθέσεων στη νέα εποχή της τεχνολογίας.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Γκουντινούδης Γεώργιος (ΑΜ: 4417029)

Επιβλέπων: ***Κακαρόντζας Γεώργιος, Καθηγητής***

ΛΑΡΙΣΑ 2022

Ο κάτωθι υπογράφων Γκουντινούδης Γεώργιος, δηλώνω υπεύθυνα ότι η παρούσα Πτυχιακή Εργασία με τίτλο «Διαδίκτυο των Πραγμάτων με δίκτυο 5G: Η εξέλιξη της καθημερινότητας του ανθρώπου και κίνδυνοι φυσικών και ηλεκτρονικών επιθέσεων στην Νέα εποχή της Τεχνολογίας» αποτελεί προϊόν ατομικής προσπάθειας και βεβαιώνω ότι:

- *Επισημαίνονται με σχετική αναφορά σε όσες περιπτώσεις έχω συμβουλευτεί δημοσιευμένη εργασία τρίτων ή έχω αναφέρει λόγο τρίτων*
- *Αναφέρω όλες τις πηγές που χρησιμοποίησα.*
- *Αναφέρω ρητά τη συνεισφορά τρίτων και σε ποια τμήματα έχει συμβεί.*
- *Γνωρίζω πως η λογοκλοπή αποτελεί σοβαρότατο παράπτωμα και είμαι ενήμερος για τις νόμιμες συνέπειες»*

Γκουντινούδης Γεώργιος

Ο φοιτητής εντάχθηκε αυτοδίκαια στο Πανεπιστήμιο Θεσσαλίας, σύμφωνα με την παρ. 1 του άρθρου 6 του Ν.4589/2019 (ΦΕΚ 13/Α'/29.01.2019).

Η εκπαιδευτική λειτουργία του ανωτέρου προγράμματος σπουδών συνεχίζεται μεταβατικά σύμφωνα με την παρ. 2 του άρθρου 6 του Ν.4589/2019 (ΦΕΚ 13/Α'/29.01.2019).

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Τόπος: Λάρισα

Ημερομηνία: 12/10/2022

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Κακαρόντζας Γεώργιος
2. Κόκορας Φώτιος
3. Κουτσονικόλα Βασιλική

Περίληψη

Η παρούσα πτυχιακή εργασία στοχεύει στην εξοικείωση του ανθρώπου με την τεχνολογία του Διαδικτύου των Πραγμάτων και τον συνδυασμό της με το νέο δίκτυο 5G, καθώς και την ενημέρωση του ως προς τους κινδύνους που πιθανόν να αντιμετωπίσει κατά τη χρήση αυτής. Παράλληλα θα παρουσιαστούν τα βασικά στοιχεία των τεχνολογιών του Διαδικτύου των Πραγμάτων - ή IoT (Internet of Things) όπως θα αναφέρεται από εδώ και έπειτα - και του 5G, ενώ θα εμβαθύνουμε αρχικά στα οφέλη που θα προσφέρει ο συνδυασμός των συγκεκριμένων τεχνολογιών στη ζωή μας, αλλά και τους κινδύνους τους οποίους θα αντιμετωπίσουμε στην καθημερινότητα μας. Τέλος, θα αναφερθούν οι τρόποι με τους οποίους δύναται να ξεπεραστούν αυτοί οι κίνδυνοι ώστε να ασφαλίσουμε τους εαυτούς μας και το περιβάλλον μας από κάθε είδους υποβόσκουσα απειλή.

Ευχαριστίες

Δράττομαι της ευκαιρίας να ευχαριστήσω τους φίλους και τους συναδέλφους μου που επικοινώνησαν τις ιδέες, τις πληροφορίες και τη γνώση τους, τη σύντροφο μου για τη συνεισφορά της στη συγγραφή της εργασίας και την οικογένεια μου που με στήριξε και με στηρίζει σε κάθε μου προσπάθεια.

Γκουντινούδης Γεώργιος

12/10/2022

Περιεχόμενα

1 Εισαγωγή

Η βιομηχανική επανάσταση είναι μία έννοια η οποία με τα χρόνια πήρε πολλά πρόσωπα και πέρασε από πολλά στάδια και με πολλά επιτεύγματα για τον άνθρωπο. Ενώ πολλοί είναι αυτοί που γνωρίζουν τις τρείς αυτές επαναστάσεις που προηγήθηκαν, ελάχιστοι είναι εκείνοι που γνωρίζουν ότι αυτή διανύουμε την τέταρτη βιομηχανική επανάσταση, ή Βιομηχανία 4.0 (Industry 4.0) όπως πλέον είθισται να ονομάζεται. Τι είναι όμως η τέταρτη βιομηχανική επανάσταση, και γιατί είναι τόσο σημαντική στη ζωή, στην καθημερινότητα και στον κόσμο μας συνολικά; Θα προσεγγιστεί η απάντηση σε αυτό το ερώτημα με σκοπό την κατανόηση της και την εξερεύνηση αυτής της επιστημονικής ανάπτυξης που έχει τόσα να προσφέρει στον κόσμο.

Η έννοια του Διαδικτύου των Πραγμάτων και η έννοια του νέου, πρωτοποριακού δικτύου 5G αποτελούν δύο από έννοιες τις οποίες θα συναντούμε και θα ήταν θεμιτό να εδραιώσουμε από την αρχή, μιας και αυτές είναι οι έννοιες που αποτελούν την βάση της βιομηχανικής επανάστασης. Η πρώτη έννοια, όπου η ορολογία αυτής αναφέρεται ως “Internet of Thing” ή “IoT”, είναι η δυνατότητα του ανθρώπου στην σύγχρονη εποχή, να ελέγχει, να χρησιμοποιεί και να διαχειρίζεται κάθε είδους ηλεκτρονική συσκευή μέσα από ένα δίκτυο, τοπικό ή ακόμη και τον παγκόσμιο ιστό. Παράλληλα, το δίκτυο 5G είναι ο διάδοχος του τωρινού δικτύου 4G LTE (Long Term Evolution), με την διαφορά ότι υπερτερεί σε κάθε τομέα, και οι διαφορές μπορούν να χαρακτηριστούν ως τεράστιο τεχνολογικό άλμα.

2 Ιστορική ανασκόπηση

Από πού ξεκίνησε αυτή η τεχνολογία, ποια ήταν τα πρώτα σημάδια που έδειξαν πως ο άνθρωπος θα κατευθυνθεί στο να ελέγχει το περιβάλλον του μέσα από την παλάμη του χεριού του; Το πως φτάσαμε σήμερα να έχουμε απόλυτη κυριαρχία και γνώση του περιβάλλοντος μας είναι μία πρόσφατη και συναρπαστική ιστορία.

Η πρώτη εμφάνιση και εδραίωση του IoT έγινε στις αρχές της δεκαετίας του 80 στο πανεπιστήμιο Carnegie Mellon στο Pittsburgh της Πενσιλβάνιας. Η τοπική προγραμματιστική κοινότητα έκανε μια, τόσο απλή αλλά ταυτόχρονα επαναστατική κίνηση. Κατάφεραν να συνδεθούν μέσω διαδικτύου με το ψυγείο της Coca Cola που υπήρχε στον χώρο του πανεπιστημίου, ώστε να πληροφορούνται εάν υπήρχε διαθέσιμο απόθεμα και την θερμοκρασία αυτού, ώστε να αποφασίσουν εάν η διαδρομή μέχρι εκεί αξίζει ή όχι.

Η ιδέα του IoT πρώτη φορά να αναφέρθηκε στο ετήσιο νομοθετικό Σαββατοκύριακο του CBCF (Congressional Black Caucus Foundation) στην ~~πρωτεύουσα της Αμερικής,~~ Washington D.C. Σε αυτή τη συνάντηση ο Peter T. Lewis, συνιδρυτής της πρώτης εταιρίας κινητής τηλεφωνίας στην Αμερική και ειδικός τηλεπικοινωνιών ανέφερε το εξής: “Το Διαδίκτυο των Πραγμάτων, ή IoT, είναι η ενοποίηση ανθρώπων, διαδικασιών και τεχνολογίας με συνδεόμενες συσκευές και αισθητήρες ώστε να καταστεί δυνατή η απομακρυσμένη παρακολούθηση, η γνώση των καταστάσεων αυτών, ο χειρισμός και η αξιολόγηση των εξελίξεων τέτοιων συσκευών” (Βιβλιογραφία [3]). Αυτή είναι η εδραίωση την έννοιας του IoT όπως ο κόσμος την γνωρίζει σήμερα.

Όσο για την ονομασία του IoT, ευχαριστούμε τον Kevin Ashton, συνιδρυτή Auto-ID Center (πλέον Auto-ID Labs), το οποίο ξεκίνησε στο Massachusetts Institute of Technology, γνωστό στο ευρύ κοινό και ως MIT, όπου σε αυτό το ίδρυμα δημιουργήθηκε το παγκόσμιο πρότυπο σύστημα του RFID (Radio-frequency identification) και άλλων ελεγκτών και αισθητήρων. Να σημειωθεί πως ο ίδιος αναφέρει πως προτιμάει την έκφραση “Internet *for* things”.

2.1 Εξέλιξη των δικτύων και εμφάνιση του 5G

Τα δίκτυα κινητής τηλεφωνίας έχουν ωριμάσει τις τελευταίες δύο δεκαετίες από άποψη ταχύτητας δεδομένων, αλλά συνεχίζουν να εξελίσσονται ώστε να επιτρέπουν πολλές νέες περιπτώσεις χρήσης για τους ανθρώπους και τις συσκευές του IoT. Σήμερα, το 4G και το 5G χρησιμοποιούν τις ίδιες τεχνολογίες παγκοσμίως - ωστόσο, αυτό δεν συνέβαινε πριν από την τέταρτη γενιά δικτύων κινητής τηλεφωνίας. Τα δίκτυα 1G, 2G, 3G, 4G και 5G είναι οι πέντε γενιές δικτύων κινητής τηλεφωνίας, όπου το G σημαίνει Generation (γενιά) – προερχόμενο από το GPRS (General Packet Radio Service) - και ο αριθμός υποδηλώνει τη σειρά της γενιάς. Οι κυψελώδης τεχνολογίες GSM, UMTS, LTE και NR επιτρέπουν τη χρήση των τεχνολογιών 2G, 3G, 4G και 5G, αντίστοιχα. Η πρώτη γενιά δικτύων κινητής τηλεφωνίας έχει πλέον ξεπεραστεί, αλλά εξακολουθούν να είναι εδραιωμένα ενεργά δίκτυα 2G, 3G, 4G και 5G στα περισσότερα μέρη του κόσμου.

2.1.1 Δίκτυο 1G

Η πρώτη γενιά δικτύων κινητής τηλεφωνίας - ή 1G όπως ονομάστηκαν αναδρομικά όταν εισήχθη η επόμενη γενιά - κυκλοφόρησε από τη Nippon Telegraph and Telephone (NTT) στο Τόκιο το 1979. Μέχρι το 1984, η NTT είχε καταφέρει το δίκτυο 1G να καλύψει ολόκληρη την Ιαπωνία. Το 1983, οι ΗΠΑ ενέκριναν τις πρώτες λειτουργίες του 1G και το DynaTAC της Motorola έγινε ένα από τα πρώτα «κινητά» τηλέφωνα που ανέπτυξαν ευρεία χρήση στις πολιτείες. Άλλες χώρες όπως ο Καναδάς και το Ηνωμένο Βασίλειο δημιούργησαν τα δικά τους δίκτυα 1G λίγα χρόνια αργότερα.

Ωστόσο, η τεχνολογία 1G υπέφερε από ορισμένα μειονεκτήματα. Η κάλυψη ήταν φτωχή και η ποιότητα του ήχου χαμηλή. Δεν υπήρχε υποστήριξη περιαγωγής (roaming) μεταξύ διαφόρων χειριστών και, καθώς διαφορετικά συστήματα λειτουργούσαν σε διαφορετικές περιοχές συχνοτήτων, δεν υπήρχε συμβατότητα μεταξύ των συστημάτων. Το χειρότερο από όλα, οι κλήσεις δεν ήταν κρυπτογραφημένες, οπότε οποιοσδήποτε με σαρωτή ραδιοφώνου (radio scanner) μπορούσε να εισέλθει σε μια κλήση.

Παρά αυτές τις ελλείψεις και την πολύ υψηλή τιμή των 3.995 $ (9.660 $ σε σημερινά χρήματα, ή 8.673 €), το DynaTAC κατάφερε να συγκεντρώσει τον εκπληκτικό αριθμό των 20 εκατομμυρίων παγκόσμιων συνδρομητών μέχρι το 1990. Ήταν δρόμος χωρίς επιστροφή. Η επιτυχία του 1G άνοιξε το δρόμο για τη δεύτερη γενιά δικτύου κινητής τηλεφωνίας, που ονομάζεται 2G.

2.1.2 Δίκτυο 2G

Η δεύτερη γενιά δικτύων κινητής τηλεφωνίας (2G), κυκλοφόρησε με το πρότυπο GSM (και αργότερα εξελίχθηκε στο EDGE) στη Φινλανδία το 1991. Για πρώτη φορά, οι κλήσεις μπορούσαν να κρυπτογραφηθούν και οι ψηφιακές φωνητικές κλήσεις ήταν σημαντικά πιο καθαρές με λιγότερο στατικό θόρυβο στο παρασκήνιο.

Το 2G ήταν κάτι πολύ περισσότερο από απλή τηλεπικοινωνία. Βοήθησε να τεθούν οι βάσεις για μια πολιτιστική επανάσταση. Για πρώτη φορά οι άνθρωποι μπορούσαν να στείλουν μηνύματα κειμένου (SMS), εικονομηνύματα και μηνύματα πολυμέσων (MMS) στα τηλέφωνά τους. Το αναλογικό παρελθόν του 1G έδωσε τη θέση του στο ψηφιακό μέλλον που παρουσιάζει το 2G. Αυτό οδήγησε στη μαζική υιοθέτηση του τόσο από καταναλωτές όσο και από επιχειρήσεις σε μία κλίμακα που δεν είχαμε συναντήσει ξανά στις τηλεπικοινωνίες.

Αν και οι ταχύτητες μεταφοράς του 2G ήταν αρχικά μόνο περίπου 9,6 kbit/s, οι φορείς εκμετάλλευσης έσπευσαν να επενδύσουν σε νέες υποδομές, όπως πύργους κινητής τηλεφωνίας. Μέχρι το τέλος της εποχής του 2G, ταχύτητες 40 kbit/s ήταν επιτεύξιμες και οι συνδέσεις EDGE πρόσφεραν ταχύτητες έως και 500 kbit/s. Παρά τις σχετικά υποτονικές ταχύτητες, το 2G έφερε επανάσταση στο επιχειρηματικό τοπίο και άλλαξε τον κόσμο για πάντα.

2.1.3 Δίκτυο 3G

Το 3G κυκλοφόρησε από την NTT DoCoMo το 2001 και είχε στόχο να τυποποιήσει το πρωτόκολλο δικτύου που χρησιμοποιούν οι προμηθευτές. Αυτό σήμαινε ότι οι χρήστες μπορούσαν να έχουν πρόσβαση σε δεδομένα από οποιαδήποτε τοποθεσία στον κόσμο, καθώς τα «πακέτα δεδομένων» που οδηγούν τη συνδεσιμότητα στον ιστό ήταν τυποποιημένα. Αυτό έκανε για πρώτη φορά πραγματική την πιθανότητα για ύπαρξη υπηρεσιών διεθνούς περιαγωγής.

Οι αυξημένες δυνατότητες μεταφοράς δεδομένων του 3G (4 φορές ταχύτερη από το 2G) οδήγησαν επίσης στην άνοδο νέων υπηρεσιών όπως οι τηλεδιασκέψεις, η μετάδοση βίντεο σε πραγματικό χρόνο και τη λειτουργεία Voice over IP (όπως το Skype). Το 2002, κυκλοφόρησε η Blackberry και πολλά από τα ισχυρά χαρακτηριστικά των συσκευών της έγιναν δυνατά χάρη στη συνδεσιμότητα 3G.

Η δύση της εποχής του 3G είδε το λανσάρισμα του iPhone το 2007, πράγμα που σημαίνει ότι η δυνατότητα δικτύου του επρόκειτο να διευρυνθεί όσο ποτέ άλλοτε.

2.1.4 Δίκτυο 4G

Το 4G αναπτύχθηκε για πρώτη φορά στη Στοκχόλμη της Σουηδίας και στο Όσλο της Νορβηγίας το 2009 ως το πρότυπο 4G Long Term Evolution (LTE). Στη συνέχεια εισήχθη σε όλο τον κόσμο και έκανε πραγματικότητα τη μετάδοση ζωντανού βίντεο υψηλής ποιότητας για εκατομμύρια καταναλωτές. Τα δίκτυα LTE στηρίζονται πλήρως στη λειτουργεία μεταγωγής πακέτων (packet-switched) και δεν διαθέτουν τμήμα μεταγωγής κυκλώματος (circuit-switched). Η τεχνολογία Voice over LTE (VoLTE), που βασίζεται σε πακέτα, είναι υπεύθυνη για την πραγματοποίηση φωνητικών κλήσεων και μηνυμάτων κειμένου (SMS) στα δίκτυα 4G LTE. Ωστόσο, τα δίκτυα LTE διαθέτουν μια εφεδρική λειτουργία μεταγωγής κυκλώματος 2G/3G, η οποία τους επιτρέπει να διευκολύνουν τις φωνητικές κλήσεις και τα SMS μέσω δικτύων 2G ή 3G, εάν η χρήση της δυνατότητας VoLTE δεν υποστηρίζεται από το τηλέφωνο ή τον φορέα εκμετάλλευσης κινητής τηλεφωνίας.

Μετά την κυκλοφορία του LTE, εισήχθησαν ορισμένες βελτιώσεις με τη μορφή των LTE Advanced (LTE-A) και LTE Advanced Pro. Το LTE-Advanced και το LTE-Advanced Pro εμφανίζονται στην οθόνη του κινητού τηλεφώνου ως LTE+ και μπορούν να υποστηρίξουν μέγιστες θεωρητικές ταχύτητες από 1 Gbps έως και 3 Gbps, αντίστοιχα. Οι μέσες ταχύτητες του 4G LTE είναι σημαντικά χαμηλότερες από τις μέγιστες ταχύτητες. Κατά μέσο όρο, τα δίκτυα 4G LTE Advanced μπορούν να προσφέρουν ταχύτητες λήψης περίπου 65 Mbps.

Το 4G προσφέρει γρήγορη πρόσβαση στο διαδίκτυο για φορητές συσκευές που διευκολύνει τις υπηρεσίες παιχνιδιών, βίντεο και τηλεδιασκέψεων σε ποιότητα HD. Το πρόβλημα ήταν ότι ενώ η μετάβαση από το 2G στο 3G ήταν τόσο απλή όσο η εναλλαγή καρτών SIM, οι κινητές συσκευές έπρεπε να είναι ειδικά σχεδιασμένες για να υποστηρίζουν 4G. Αυτό βοήθησε τους κατασκευαστές συσκευών να κλιμακώσουν δραματικά τα κέρδη τους παρουσιάζοντας νέες συσκευές 4G και ήταν ένας παράγοντας πίσω από την άνοδο της Apple να γίνει η πρώτη εταιρεία τρισεκατομμυρίων δολαρίων στον κόσμο.

Ενώ το 4G είναι το τρέχον πρότυπο σε όλο τον κόσμο, ορισμένες περιοχές μαστίζονται από προβλήματα δικτύου και έχουν χαμηλή διείσδυση του 4G LTE. Σύμφωνα με την Ogury, μια πλατφόρμα δεδομένων κινητής τηλεφωνίας, οι κάτοικοι του Ηνωμένου Βασιλείου μπορούν για παράδειγμα να έχουν πρόσβαση σε δίκτυα 4G μόνο το 53% του χρόνου στην καθημερινότητα τους.

2.1.5 Δίκτυο 5G

Αν και υπήρχε πολύ χαμηλή κάλυψη σε ορισμένες περιοχές, δημιουργείται το ερώτημα, γιατί υπήρξε έντονη εστίαση στη δημιουργία του 5G. Η απάντηση είναι ότι το 5G σχεδιαζόταν ταυτόχρονα.

Κατά τη διάρκεια συνέντευξης με την Tech Republic, ο Kevin Ashton περιέγραψε πώς επινόησε τον όρο "Διαδίκτυο των Πραγμάτων" (IoT) κατά τη διάρκεια μιας παρουσίασης PowerPoint που έδωσε τη δεκαετία του 1990 για να πείσει την Procter & Gamble να αρχίσει να χρησιμοποιεί την τεχνολογία ετικετών RFID.

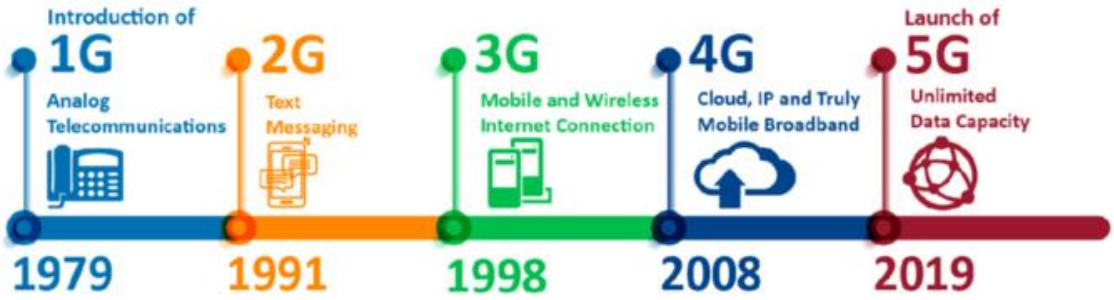
Η φράση έγινε γνωστή και το IoT σύντομα διαφημίστηκε ως η επόμενη μεγάλη ψηφιακή επανάσταση που θα έβλεπε δισεκατομμύρια συνδεδεμένες συσκευές να μοιράζονται απρόσκοπτα δεδομένα σε όλο τον κόσμο. Σύμφωνα με τον Ashton, ένα κινητό τηλέφωνο δεν είναι απλά μια συσκευή τηλεφωνίας, είναι το IoT στην τσέπη σου. Μια σειρά από αισθητήρες συνδεδεμένους στο δίκτυο που βοηθούν στην επίτευξη πολλών πραγμάτων, από την πλοήγηση, τη λήψη φωτογραφιών έως την επικοινωνία και πολλά άλλα. Το IoT θα μετακινήσει τα δεδομένα από τα κέντρα διακομιστών (server centers) και σε αυτό που είναι γνωστό ως «συσκευές αιχμής» (edge devices), όπως συσκευές με δυνατότητα σύνδεσης στο Wi-Fi, όπως ψυγεία, πλυντήρια ρούχων και αυτοκίνητα.

Στις αρχές της δεκαετίας του 2000, οι προγραμματιστές γνώριζαν ότι τα δίκτυα 3G και ακόμη και 4G δεν θα μπορούσαν να υποστηρίξουν ένα τέτοιο δίκτυο. Καθώς η καθυστέρηση (latency) του 4G μεταξύ και είναι πολύ αργή για αποκρίσεις σε πραγματικό χρόνο, αρκετοί ερευνητές άρχισαν να αναπτύσσουν την επόμενη γενιά δικτύων κινητής τηλεφωνίας.

Το 2008, η NASA βοήθησε στην δημιουργία του Machine-to-Machine Intelligence (M2Mi) Corp για την ανάπτυξη της τεχνολογίας IoT και M2M, καθώς και της τεχνολογίας 5G που απαιτείται για την υποστήριξή της. Την ίδια χρονιά, η Νότια Κορέα ανέπτυξε ένα πρόγραμμα Έρευνας και Ανάπτυξης 5G, ενώ το Πανεπιστήμιο της Νέας Υόρκης ίδρυσε το NYU WIRELESS με εστίαση στο 5G το 2012.

Η ανώτερη συνδεσιμότητα που προσφέρεται από το 5G υποσχέθηκε να μεταμορφώσει τα πάντα, από τον τραπεζικό τομέα στην υγειονομική περίθαλψη. Το 5G προσφέρει τη δυνατότητα καινοτομιών όπως εξ αποστάσεως χειρουργικές επεμβάσεις, τηλεϊατρική και ακόμη και απομακρυσμένη παρακολούθηση ζωτικών σημείων που θα μπορούσαν να σώσουν ζωές.

Τρεις εταιρείες από τη Νότια Κορέα – η KT, η LG Uplus και η SK Telecom – παρουσίασαν ζωντανές εμπορικές υπηρεσίες 5G τον Δεκέμβριο του 2018 και υποσχέθηκαν μια ταυτόχρονη κυκλοφορία του 5G τον Μάρτιο του 2019 σε ολόκληρη τη χώρα. Στην Εικόνα 2.1 απεικονίζεται η εξέλιξη των δικτύων με το πέρασμα του χρόνου και τις δυνατότητες τις οποίες πρόσφεραν.

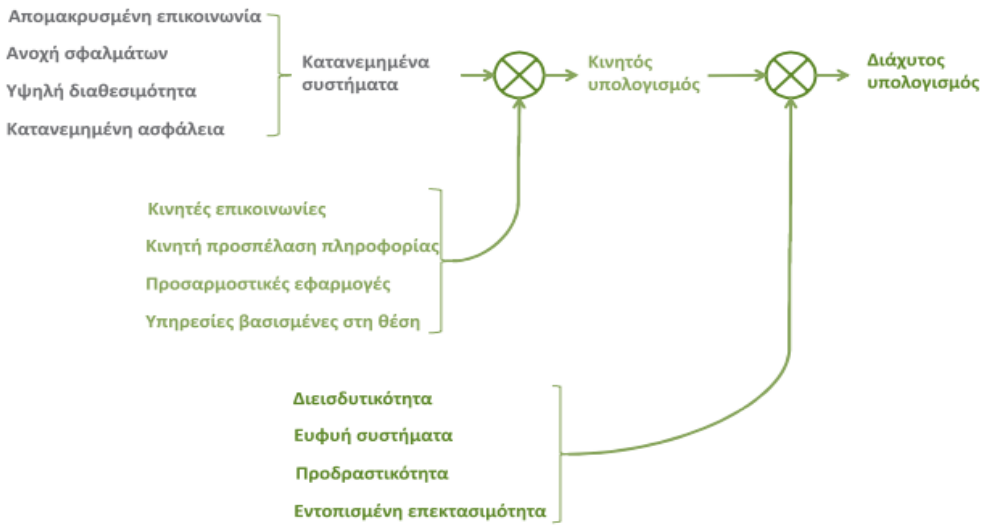


Εικόνα 2.1: Η εξέλιξη των δικτύων (OKportal Technology, 2019) [7.6]

2.2 Διάχυτος Υπολογισμός

Διάχυτος υπολογισμός, ή Ubiquitous computing, είναι μια έννοια στη μηχανική λογισμικού, τη μηχανική υλικού και την επιστήμη των υπολογιστών όπου οι υπολογισμοί είναι φτιαγμένοι να εμφανίζονται οποτεδήποτε και παντού. Σε αντίθεση με τους επιτραπέζιους υπολογιστές, ο διάχυτος υπολογισμός μπορεί να συμβεί χρησιμοποιώντας οποιαδήποτε συσκευή, σε οποιαδήποτε τοποθεσία και σε οποιαδήποτε μορφή. Ένας χρήστης αλληλοεπιδρά με τον υπολογιστή, ο οποίος μπορεί να υπάρχει με πολλές διαφορετικές μορφές, συμπεριλαμβανομένων φορητών υπολογιστών, tablet, έξυπνων τηλεφώνων και τερματικών σε καθημερινά αντικείμενα, όπως ένα ψυγείο ή ένα ζευγάρι γυαλιά. Οι υποκείμενες τεχνολογίες οι οποίες υποστηρίζουν τον διάχυτο υπολογισμό περιλαμβάνουν το Διαδίκτυο, το προηγμένο ενδιάμεσο λογισμικό, το λειτουργικό σύστημα, τον κώδικα κινητής τηλεφωνίας, τους αισθητήρες, τους μικροεπεξεργαστές, τις νέες διεπαφές χρήστη εισόδου / εξόδου (New I/O ή NIO), τα δίκτυα υπολογιστών, τα πρωτόκολλα κινητής τηλεφωνίας, την τοποθεσία και την τοποθέτηση και νέα υλικά. Στην Εικόνα 2.2 παρουσιάζεται μια ταξινόμηση των εννοιών που περιβάλλουν τον διάχυτο υπολογισμό.

Ο ορισμός του διάχυτου υπολογισμού από τον Satyanarayanan το 2001 είναι ο εξής: “Η έννοια του διάχυτου υπολογισμού αναφέρεται σε μια πιο γενική κλάση συστημάτων κινητού υπολογισμού τα οποία είναι ικανά να εντοπίσουν και να προσδιορίσουν το πλαίσιο των οντοτήτων που επενεργούν στο σύστημα, προκειμένου να προσαρμοστούν κατάλληλα στη συμπεριφορά αυτών των οντοτήτων.”



Εικόνα 2.2: Ταξινομία εννοιών κατανεμημένων συστημάτων, κινητού και διάχυτου [1]

2.3 Τεχνητή Νοημοσύνη

Στο πρώτο μισό του 20ού αιώνα, η επιστημονική φαντασία εξοικείωσε τον κόσμο με την έννοια των τεχνητά ευφυών ρομπότ. Ξεκίνησε με τον "άκαρδο" Τενεκεδένιο άνθρωπο (Tin man) από τον Μάγο του Οζ (Wizard of Oz) και συνεχίστηκε με το ανθρωποειδές ρομπότ που υποδυόταν τη Μαρία στο Metropolis (Maria in Metropolis). Μέχρι τη δεκαετία του 1950, υπήρξε μια γενιά επιστημόνων, μαθηματικών και φιλοσόφων με την έννοια της τεχνητής νοημοσύνης (ή AI από το Artificial Intelligence) πολιτισμικά αφομοιωμένη στο μυαλό τους. Ένας τέτοιος επιστήμονας ήταν ο Άλαν Τούρινγκ (Alan Turing), ένας νεαρός Βρετανός πολυμαθής που διερεύνησε τη μαθηματική δυνατότητα της τεχνητής νοημοσύνης. Ο Τούρινγκ διατύπωσε την άποψη ότι οι άνθρωποι χρησιμοποιούν τις διαθέσιμες πληροφορίες καθώς και τη λογική προκειμένου να επιλύουν προβλήματα και να λαμβάνουν αποφάσεις, οπότε γιατί να μην μπορούν οι μηχανές να κάνουν το ίδιο πράγμα; Αυτό ήταν το λογικό πλαίσιο της εργασίας του 1950, Computing Machinery and Intelligence, στην οποία συζητούσε πώς να κατασκευάσει ευφυείς μηχανές και πώς να ελέγξει τη νοημοσύνη τους.

2.3.1 Κάνοντας την επιδίωξη δυνατή

Τι εμπόδισε όμως τον Τούρινγκ από το να πιάσει δουλειά εκεί και τότε; Πρώτον, οι υπολογιστές έπρεπε να αλλάξουν ριζικά. Πριν από το 1949 οι υπολογιστές στερούνταν μιας βασικής προϋπόθεσης για τη νοημοσύνη: δεν μπορούσαν να αποθηκεύουν εντολές, παρά μόνο να τις εκτελούν. Με άλλα λόγια, οι υπολογιστές μπορούσαν να λάβουν εντολές για το τι να κάνουν, αλλά δεν μπορούσαν να θυμηθούν τι έκαναν. Δεύτερον, οι υπολογιστές ήταν εξαιρετικά ακριβοί. Στις αρχές της δεκαετίας του 1950, το κόστος μίσθωσης ενός υπολογιστή έφτανε τα 200.000 δολάρια το μήνα. Η αξία αυτών των δολαρίων σήμερα υπολογίζεται περίπου στα 2.4 εκατομμύρια, συνεπώς το κόστος ήταν πολύ υψηλότερο από όσο φανταζόμαστε. Μόνο διάσημα πανεπιστήμια και μεγάλες τεχνολογικές εταιρείες μπορούσαν να αντέξουν οικονομικά να περιπλανηθούν σε αυτά τα αχαρτογράφητα νερά. Για να πειστούν οι πηγές χρηματοδότησης ότι η μηχανική νοημοσύνη άξιζε να επιδιωχθεί, χρειαζόταν μια απόδειξη της έννοιας καθώς και την υποστήριξη από ανθρώπους υψηλού προφίλ.

2.3.2 Το αρχικό συνέδριο

Πέντε χρόνια αργότερα, το 1955, η απόδειξη της έννοιας της μηχανικής νοημοσύνης αρχικοποιήθηκε μέσω του Logic Theorist των Allen Newell, Cliff Shaw και Herbert Simon. Το Logic Theorist ήταν ένα πρόγραμμα που είχε σχεδιαστεί για να μιμείται τις ικανότητες επίλυσης προβλημάτων ενός ανθρώπου και χρηματοδοτήθηκε από την Εταιρεία Έρευνας και Ανάπτυξης (Research and Development, RAND). Θεωρείται από πολλούς ως το πρώτο πρόγραμμα τεχνητής νοημοσύνης και παρουσιάστηκε στο Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI) που φιλοξενήθηκε από τους John McCarthy και Marvin Minsky το 1956. Το DSRPAI ήταν ένα θερινό εργαστήριο (workshop) του 1956 που θεωρείται ευρέως ως το ιδρυτικό γεγονός της τεχνητής νοημοσύνης ως τομέα επιστήμης. Το πρόγραμμα διήρκεσε περίπου έξι έως οκτώ εβδομάδες και ήταν ουσιαστικά μια εκτεταμένη συνεδρία καταιγισμού ιδεών. Έντεκα μαθηματικοί και επιστήμονες σχεδίαζαν αρχικά να συμμετάσχουν - δεν συμμετείχαν όλοι τους, αλλά περισσότεροι από δέκα άλλοι ήρθαν για σύντομο χρονικό διάστημα. Σε αυτό το ιστορικό συνέδριο, ο McCarthy, επιθυμώντας μια μεγάλη συλλογική προσπάθεια, συγκέντρωσε κορυφαίους ερευνητές από διάφορους τομείς για μια ανοιχτή συζήτηση σχετικά με την τεχνητή νοημοσύνη, τον όρο που επινόησε στην ίδια εκδήλωση. Δυστυχώς, το συνέδριο δεν ανταποκρίθηκε στις προσδοκίες του McCarthy, όπως αναφέρθηκε παραπάνω - οι άνθρωποι έρχονταν και έφευγαν όπως ήθελαν - και έτσι δεν κατάφεραν να συμφωνήσουν σε τυποποιημένες μεθόδους για το πεδίο. Παρά ταύτα, όλοι συντάχθηκαν ολόψυχα με την άποψη ότι η τεχνητή νοημοσύνη ήταν εφικτή. Η σημασία αυτού του γεγονότος δεν μπορεί να υπονομευθεί, καθώς αποτέλεσε καταλύτη για τα επόμενα είκοσι χρόνια της έρευνας για το AI.

2.3.3 Κύκλος των επιτυχιών και οπισθοδρομήσεων

Από το 1957 έως το 1974, η τεχνητή νοημοσύνη άνθισε. Οι υπολογιστές μπορούσαν να αποθηκεύουν περισσότερες πληροφορίες και έγιναν ταχύτεροι, φθηνότεροι και πιο προσιτοί. Οι αλγόριθμοι μηχανικής μάθησης βελτιώθηκαν επίσης και οι άνθρωποι έγιναν καλύτεροι στο να γνωρίζουν ποιον αλγόριθμο να εφαρμόσουν στο πρόβλημά τους. Οι πρώτες επιδείξεις, όπως ο Γενικός Επιλύτης Προβλημάτων (General Problem Solver) των Newell και Simon και το ELIZA του Joseph Weizenbaum, έδειχναν υποσχέσεις προς τους στόχους της επίλυσης προβλημάτων και της ερμηνείας της προφορικής γλώσσας αντίστοιχα. Αυτές οι επιτυχίες, καθώς και η συνηγορία κορυφαίων ερευνητών (συγκε-

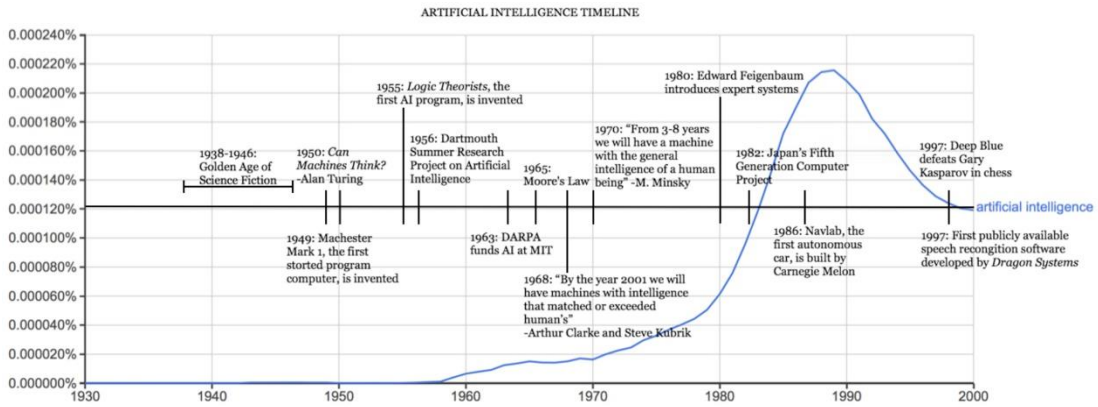
κριμένα των συμμετεχόντων στο DSRPAI) έπεισαν κυβερνητικές υπηρεσίες όπως η Υπηρεσία Προηγμένων Αμυντικών Ερευνητικών Προγραμμάτων (DARPA) να χρηματοδοτήσουν την έρευνα AI σε διάφορα ιδρύματα. Η κυβέρνηση ενδιαφερόταν ιδιαίτερα για μια μηχανή που θα μπορούσε να μεταγράφει και να μεταφράζει την προφορική γλώσσα, καθώς και για την επεξεργασία δεδομένων υψηλής απόδοσης. Η αισιοδοξία ήταν μεγάλη και οι προσδοκίες ακόμη μεγαλύτερες. Το 1970 ο Marvin Minsky δήλωσε στο περιοδικό Life ότι "σε τρία έως οκτώ χρόνια θα έχουμε μια μηχανή με τη γενική νοημοσύνη ενός μέσου ανθρώπου". Ωστόσο, ενώ υπήρχε η βασική απόδειξη της αρχής, υπήρχε ακόμη πολύς δρόμος μέχρι να επιτευχθούν οι τελικοί στόχοι της επεξεργασίας φυσικής γλώσσας, της αφηρημένης σκέψης και της αυτοαναγνώρισης.

Η ολοένα μεγαλύτερη προσέγγιση της Τεχνητής Νοημοσύνης αποκάλυψε ένα βουνό από εμπόδια. Το μεγαλύτερο ήταν η έλλειψη υπολογιστικής ισχύος για να γίνει κάτι ουσιαστικό: οι υπολογιστές απλώς δεν μπορούσαν να αποθηκεύσουν αρκετές πληροφορίες ή να τις επεξεργαστούν αρκετά γρήγορα. Για να επικοινωνήσει κανείς, για παράδειγμα, πρέπει να γνωρίζει τη σημασία πολλών λέξεων και να τις κατανοεί σε πολλούς συνδυασμούς. Ο Hans Moravec, διδακτορικός φοιτητής του McCarthy εκείνη την εποχή, δήλωσε ότι "οι υπολογιστές ήταν ακόμη εκατομμύρια φορές πολύ αδύναμοι για να επιδείξουν νοημοσύνη". Καθώς η υπομονή λιγόστευε, λιγόστευε και η χρηματοδότηση, και η έρευνα διεξήχθη με αργό ρυθμό για δέκα χρόνια.

Στη δεκαετία του 1980, η τεχνητή νοημοσύνη αναζωπυρώθηκε από δύο πηγές: η πρώτη ήταν η επέκταση της εργαλειοθήκης αλγορίθμων και την ενίσχυση των κονδυλίων. Ο John Hopfield και ο David Rumelhart διέδωσαν τις τεχνικές "βαθιάς μάθησης" που επέτρεπαν στους υπολογιστές να μαθαίνουν χρησιμοποιώντας την εμπειρία. Η δεύτερη ήταν ο Edward Feigenbaum που εισήγαγε συστήματα εμπειρογνωμόνων τα οποία μιμούνταν τη διαδικασία λήψης αποφάσεων ενός ανθρώπινου εμπειρογνώμονα. Το πρόγραμμα ρωτούσε έναν εμπειρογνώμονα σε έναν τομέα πώς να αντιδράσει σε μια δεδομένη κατάσταση, και μόλις αυτό μαθευόταν για σχεδόν κάθε κατάσταση, οι μη ειδικοί μπορούσαν να λάβουν συμβουλές από το πρόγραμμα αυτό. Τα συστήματα εμπειρογνωμόνων χρησιμοποιήθηκαν ευρέως στις βιομηχανίες. Η ιαπωνική κυβέρνηση χρηματοδότησε σε μεγάλο βαθμό τα συστήματα εμπειρογνωμόνων και άλλες προσπάθειες σχετικές με το AI στο πλαίσιο του προγράμματος υπολογιστών πέμπτης γενιάς (FGCP). Από το 1982 έως το 1990, επένδυσε 400 εκατομμύρια δολάρια με στόχο την επανάσταση στην

επεξεργασία των υπολογιστών, την εφαρμογή του λογικού προγραμματισμού και τη βελτίωση της τεχνητής νοημοσύνης. Δυστυχώς, οι περισσότεροι από τους φιλόδοξους στόχους δεν επιτεύχθηκαν. Ωστόσο, θα μπορούσε να υποστηριχθεί ότι οι έμμεσες επιπτώσεις του FGCP ενέπνευσαν μια ταλαντούχα νέα γενιά μηχανικών και επιστημόνων. Ανεξάρτητα από αυτό, η χρηματοδότηση του FGCP σταμάτησε και η τεχνητή νοημοσύνη έφυγε από το προσκήνιο.

Κατά τρόπο απροσδόκητο, κατά την απουσία κρατικής χρηματοδότησης και δημόσιας δημοσιότητας, το AI ευδοκίμησε. Κατά τις δεκαετίες του 1990 και του 2000, πολλοί από τους στόχους-ορόσημα της τεχνητής νοημοσύνης είχαν επιτευχθεί. Το 1997, ο απερχόμενος παγκόσμιος πρωταθλητής στο σκάκι και μεγάλος δάσκαλος Garry Kasparov ητττήθηκε από το Deep Blue της IBM, ένα πρόγραμμα υπολογιστή που έπαιζε σκάκι, όπως απεικονίζεται στην Εικόνα 2.3. Αυτός ο πολύ προβεβλημένος αγώνας ήταν η πρώτη φορά που ένας εν ενεργεία παγκόσμιος πρωταθλητής σκακιού έχασε από έναν υπολογιστή και λειτούργησε ως ένα τεράστιο βήμα προς ένα πρόγραμμα λήψης αποφάσεων με τεχνητή νοημοσύνη. Την ίδια χρονιά, το λογισμικό αναγνώρισης ομιλίας, που αναπτύχθηκε από την Dragon Systems, εφαρμόστηκε στα Windows. Αυτό ήταν ένα ακόμη μεγάλο βήμα προς την κατεύθυνση της προσπάθειας διερμηνείας προφορικού λόγου. Φαινόταν ότι δεν υπήρχε πρόβλημα που οι μηχανές δεν μπορούσαν να χειριστούν. Ακόμη και τα ανθρώπινα συναισθήματα ήταν μέσα στις δυνατότητες τους, όπως αποδεικνύεται από το Kismet, ένα ρομπότ που αναπτύχθηκε από τη Cynthia Breazeal και μπορούσε να αναγνωρίζει και να εμφανίζει συναισθήματα.



Εικόνα 2.3: Χρονοδιάγραμμα Τεχνητής Νοημοσύνης έως το 2000

3 Βασικές εφαρμογές του IoT

Στην καθημερινότητα μας οι περισσότεροι από εμάς κάνουμε κινήσεις τις οποίες θεωρούμε πλέον δεδομένες, χωρίς να γνωρίζουμε πως αυτές οι κινήσεις είναι η απαρχή της εδραίωσης του IoT. Σε αυτό το κεφάλαιο θα αναφερθούν μερικές από αυτές τις λειτουργείες και θα εξετάσουμε την συνεισφορά τους στην ζωή μας.

3.1 Κυκλοφοριακή κίνηση

Μία εξαιρετικά χρησιμοποιούμενη λειτουργεία που όλοι μας έχουμε δει είτε στα κινητά μας είτε στα GPS του αυτοκινήτου μας είναι η ανάλυση της κίνησης της κυκλοφορίας (χάρτες της Google) που θα συναντήσουμε στο δρόμο και η πρόταση διαδρομών από το εκάστοτε λογισμικό ώστε να αποφύγουμε τυχόν κυκλοφοριακές συμφορήσεις. (εφόσον στατιστικά το μεγαλύτερο μέρος του πληθυσμού χρησιμοποιεί χάρτες της Google αυτούς θα χρησιμοποιήσουμε για το συγκεκριμένο παράδειγμα).

Δημιουργεί η απορία πως η Google εκείνη τη στιγμή γνωρίζει σε τι επίπεδα βρίσκεται η κίνηση στην εκάστοτε περιοχή που εμείς βρισκόμαστε. Παρακολουθεί από κάμερες; Ενημερώνεται από κρατικούς φορείς; Ή μήπως πολύ απλά εμείς οι ίδιοι είμαστε αυτοί που συμβάλουν στην δημιουργία αυτής της γνώσης; Προφανώς η απάντηση είναι πως εμείς ενημερώνουμε τη Google και την προμηθεύουμε με ότι στοιχεία χρειάζεται ώστε να παράγει το αποτέλεσμα που ο χρήστης βλέπει στην οθόνη. Όταν κάποιος χρήστης ανοίγει το χάρτη της Google, είτε στο κινητό, στο GPS, είτε ακόμη και στο smartwatch, αυτόματα προσφέρονται στη Google πληροφορίες όπως η τοποθεσία, ο τελικός προορισμός, η ταχύτητα κίνησης κάθε στιγμή και η πορεία του χρήστη. Αυτό το κάνει ο κάθε χρήστης τη στιγμή που ανοίγει τους χάρτες ώστε να λάβει κατευθύνσεις ως προς έναν προορισμό, και έτσι, συγκεντρώνοντας όλα τα δεδομένα και αναλύοντας τις κινήσεις κάθε οδηγού σε πραγματικό χρόνο, η Google μπορεί να καθορίσει, με ένα περιθώριο λάθους διότι δεν χρησιμοποιούν όλοι οι οδηγοί χάρτες σε κάθε διαδρομή τους, την κίνηση που θα συναντήσουμε στη συνέχεια της διαδρομής μας.

Αυτή είναι μία βασική χρήση του IoT, μια χρήση που ο καθένας από εμάς έχει ήδη ή πρόκειται να συναντήσει στο μέλλον καθώς ταξιδεύει. Αυτός ο διαμοιρασμός της πληροφορίας μεταξύ συσκευών μέσω του διαδικτύου, είναι ο ορισμός του IoT.

Η διαδικασία με την οποία η Google δημιουργεί τα δεδομένα της κυκλοφοριακής κίνησης είναι πολύ πιο περίπλοκη από την απλή περιγραφή την οποία μόλις αναφέρθηκε. Πέρα από την ανάλυση των κινήσεων των αυτοκινήτων σε πραγματικό χρόνο, η Google την ίδια στιγμή αναλύει δεδομένα και μοτίβα προηγούμενων χρονικών στιγμών της συγκεκριμένης περιοχής και συνδυάζοντας την προϋπάρχουσα γνώση και τις νέες πληροφορίες μέσω της μηχανικής μάθησης (Machine Learning) καταλήγει στο να προβλέψει την πιο πιθανή κατάσταση στην οποία θα βρίσκεται το κυκλοφοριακό δίκτυο εκείνη τη στιγμή.

3.2 Σπίτι και χώρος εργασίας

Στην ζωή μας τον τελευταίο καιρό έχει αρχίσει να εισέρχεται και ο απομακρυσμένος έλεγχος του σπιτιού ή του χώρου εργασίας μας με διαφόρους τρόπους, χρησιμοποιώντας τις δυνατότητες του IoT. Παρότι ακόμη δεν είναι διαδεδομένο χαρακτηριστικό της σύγχρονης εποχής διότι προς το παρόν υπάρχουν κενά ασφαλείας στις συγκεκριμένες λειτουργίες, επιλέγεται από αρκετούς η αυτοματοποίηση και η μεταφορά βασικών λειτουργιών συστημάτων του χώρου του στο κινητό του ή στον υπολογιστή του.

Παράδειγμα μίας τέτοιας λειτουργείας είναι η ενεργοποίηση της θέρμανσης, πρόκειται για μία συσκευή όπως το κλιματιστικό είτε για ολοκληρωτικές λειτουργίες θέρμανσης όπως τα καλοριφέρ. Πλέον, με το άγγισμα ενός κουμπιού στο κινητό μπορεί να ενεργοποιηθούν συσκευές και να ελέγχουμε το χώρο μας οποιαδήποτε στιγμή. Δύναται να μετακινηθούν τα παντζούρια ώστε να εισέλθει το φως να εισέλθει στο χώρο, ή να ~~τα~~ κλείσουν ασφαλίζοντας τον, να ενεργοποιηθεί η θέρμανση μας πριν την άφιξη ώστε ο χώρος να είναι ζεστός, είτε ακόμη να ανοίξουν οι πόρτες ή να ασφαλιστούν. Ακόμη, μπορεί να ενεργοποιηθεί το σύστημα ύδρευσης του κήπου μας στις επιθυμητές, ή ακόμη να υπάρχει πρόσβαση σε κάμερες ώστε να υφίσταται απομακρυσμένη γνώση της κίνησης σε χώρους οποιαδήποτε στιγμή.

Με τον ίδιο τρόπο υπάρχει η δυνατότητα ελέγχου του χώρου εργασίας, από κάμερες, αισθητήρες, ενεργοποίηση και χρήση μηχανημάτων έως ενεργοποίηση ή απενεργοποίηση πρωτοκόλλων ασφαλείας, συναγερμών και κλειδαριών

3.3 Φορετή τεχνολογία (Wearable Technology)

Θα αναλυθεί η έννοια του wearable ώστε να κατανοήσουμε καλύτερα τις ιδιότητες του. Τα wearables είναι μια κατηγορία ηλεκτρονικών συσκευών που μπορούν να φορεθούν ως αξεσουάρ, να ενσωματωθούν σε ρούχα, να εμφυτευθούν στο σώμα του χρήστη ή ακόμη και να γίνουν τατουάζ στο δέρμα.

Αυτές οι συσκευές υγείας είναι τόσο ελκυστικές όσο και χρήσιμες. Περιλαμβάνουν έξυπνα ρούχα, έξυπνα βραχιόλια και ιατρικά wearables που παρέχουν υψηλής ποιότητας υπηρεσίες υγείας. Έχουν σχεδιαστεί για να παρακολουθούν δραστηριότητες όπως ο σφυγμός, ο αριθμός των βημάτων, ο καρδιακός ρυθμός κ.λπ. Τα δεδομένα αυτά καταγράφονται και μπορούν να αποσταλούν σε ιατρικό προσωπικό για λεπτομερή ανάλυση της φυσικής μας κατάστασης. Αυτές οι έξυπνες φορητές (ή φορούμενες) συσκευές που βασίζονται στο IoT επηρεάζουν πολύ τον τρόπο ζωής μας. Εκτός από την εκτέλεση αυτών των βασικών λειτουργιών, μπορούν επίσης να σημάνουν συναγερμό και να στείλουν ειδοποιήσεις σε περίπτωση ιατρικής έκτακτης ανάγκης, όπως κρίση άσθματος, επιληπτικές κρίσεις, καρδιακή προσβολή κ.λπ.

Επιπλέον, με τη χρήση αυτών μπορούμε και οι ίδιοι να έχουμε μια εικόνα της υγείας μας σε γενικό πλαίσιο και πως τις κινήσεις τις οποίες κάνουμε μέσα στην μέρα. Με αυτόν τον τρόπο μας δίνεται η δυνατότητα να βελτιώσουμε τις συνήθειες μας, να αποφύγουμε επιβλαβές κινήσεις και να ενημερωθούμε για τυχόν ανωμαλίες τις οποίες διαφορετικά δεν θα γνωρίζαμε, όπως η υπερβολική κατανάλωση φαγητού, επικίνδυνες ασκήσεις και ανάστατο ύπνο αντίστοιχα.

Οι φορητές συσκευές θα μπορούσαν επίσης να συνδεθούν αυτόματα με συσκευές στο σπίτι. Παραδείγματα αποτελούν ένα προτιμώμενο επίπεδο φωτισμού όταν κάποιος παρακολουθεί τηλεόραση από μια συγκεκριμένη καρέκλα και η ρύθμιση της τηλεόρασης και της φορητή συσκευή για το έλεγχο του επίπεδου φωτισμού από τα συνδεδεμένα φώτα LED μέσα στο δωμάτιο. Ένα έξυπνο σπίτι θα μπορούσε ακόμη και να υποστηρίζει την αυτόματη παρεμπόδιση του φωτός από τα παράθυρα που δημιουργούν θάμβωση στην τηλεόραση. Ακόμη και ο οπίσθιος φωτισμός στην οθόνη της τηλεόρασης LCD θα μπορούσε να ρυθμιστεί και όλες οι λειτουργείες να βελτιστοποιηθούν για την εξοικονόμηση ενέργειας, καθώς και για τη δημιουργία της πιο ευνοϊκής εμπειρίας θέασης. Όλες αυτές

οι αλληλεπιδράσεις θα μπορούσαν να γίνουν αυτόματα, απευθείας μεταξύ των συσκευών, αφού ρυθμιστεί η συνολική στρατηγική μέσω μιας διεπαφής έξυπνου τηλεφώνου.

Οι δυνατότητες και τα πιο ισχυρά στοιχεία του IoT βασίζονται στη διάχυτη συνδεσιμότητα και όταν αυτή σχετίζεται με μεγάλες συλλογές συνδεδεμένων συσκευών, μπορούν να προκύψουν σημαντικά οφέλη. Πώς μπορούν να επωφεληθούν και οι φορητές συσκευές από αυτή την ιδέα; Για παράδειγμα, θα μπορούσαν οι φορητές συσκευές σας να αλληλοεπιδρούν με τις συσκευές άλλων ατόμων σε ένα πλήθος; Υφίσταται το ερώτημα αν επιθυμείτε να γνωρίζετε αν κάποιος που κάθεται δίπλα σας στο τρένο έχει υψηλό πυρετό; Πιθανότατα η απάντηση να είναι καταφατική, αλλά το άτομο με πυρετό μπορεί να μην θέλει να μεταδώσει τη συγκεκριμένη πληροφορία. Αν όμως χρησιμοποιούσατε και οι δύο τον ίδιο πάροχο υγειονομικής περίθαλψης, ίσως αυτές οι πληροφορίες να μοιράζονταν στο σύνολο, ίσως να ήταν ελεγχόμενες μέσω ενός φίλτρου έξυπνων τηλεφώνων. Τα ζητήματα προστασίας θα συνεχίσουν να αποτελούν μεγάλο μέρος του προβληματισμού των ανθρώπων για τα επόμενα χρόνια, αλλά θα υπάρχουν τομείς όπου κάποια διαδεδομένη κοινή χρήση βιομετρικών στοιχείων θα ήταν χρήσιμη.

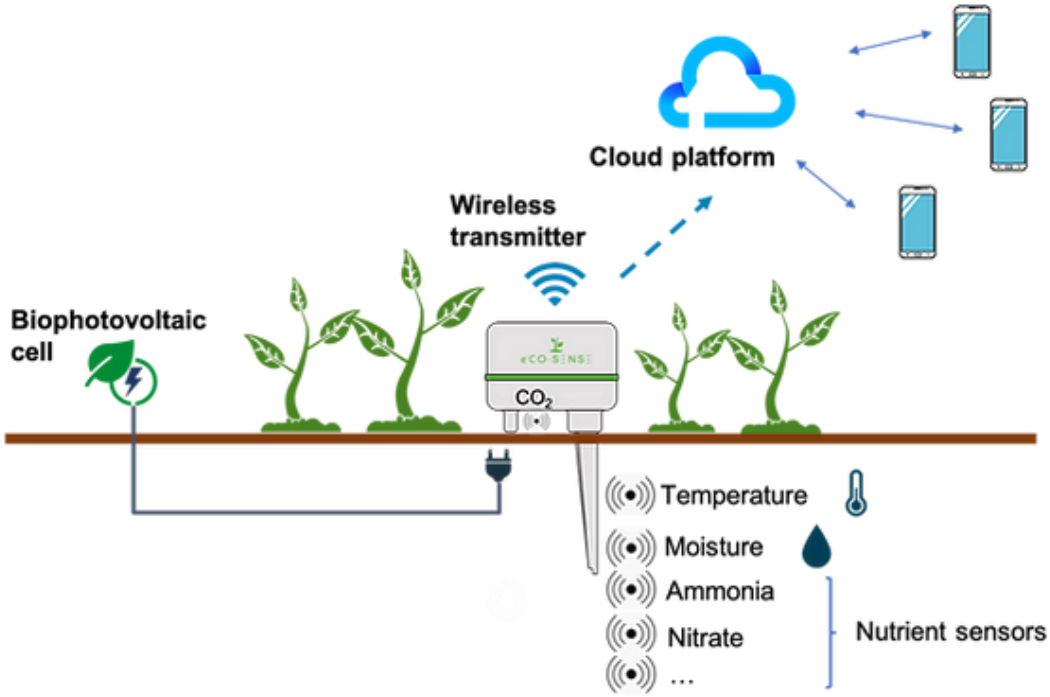
3.4 Γεωργία και καλλιέργεια

Φανταστείτε έναν γεωργό ή κτηνοτρόφο ο οποίος κάθετε στο σπίτι του ενώ τα μηχανήματα του οργώνουν το χωράφι, τα ζώα του τρώνε αυτόματα, τα φυτά του ποτίζονται όποτε το θελήσει και οποιαδήποτε στιγμή γνωρίζει που βρίσκονται τα ζωντανά του. Είναι μια εικόνα που δύσκολα ο κόσμος μπορεί να φανταστεί, αλλά είναι μια εικόνα που ήδη έχει γίνει πραγματικότητα με τη χρήση του IoT. Λόγω της κλιματικής αλλαγής και της κρίσης του νερού, οι αγρότες αντιμετωπίζουν πολλά προβλήματα, όπως ισοπέδωση των καλλιεργειών, διάβρωση του εδάφους, ξηρασία κ.α.

Εργαλεία όπως αισθητήρες, ασύρματοι ελεγκτές και αυτόματα μηχανήματα σε συνδυασμό με ένα τοπικό δίκτυο ή ακόμη και ενός υπολογιστικού νέφους (Cloud Computing) μπορούν να συμβάλουν στην καλυτέρευση της εργασίας ενός επαγγελματία αγρότη και να του δώσουν τη δυνατότητα να γνωρίζει σε πραγματικό χρόνο την κατάσταση στην οποία βρίσκετε η σπορά του, τα ζώα του και ακόμη τα καιρικά φαινόμενα. Το IoT βοηθά επίσης τους αγρότες να εξετάσουν την υγεία του εδάφους. Πριν σχεδιάσει να καλλιεργήσει μια νέα παρτίδα καλλιεργειών, ο αγρότης πρέπει να ανακτήσει τα θρεπτικά συστατικά του εδάφους. Το εμπλουτισμένο με στοιχεία του IoT λογισμικό επιτρέπει στον χρήστη ή

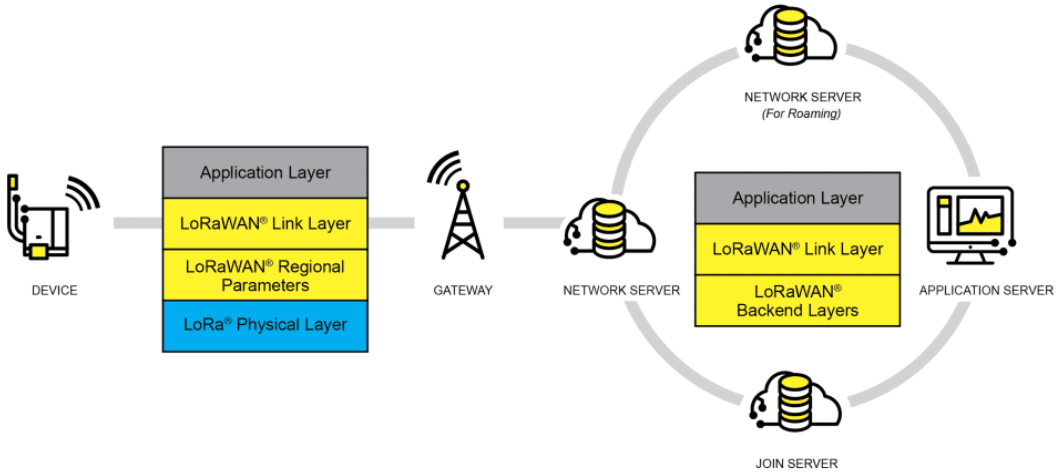
τον αγρότη να επιλέξει τις καλύτερες καλλιέργειες με σκοπό την αποκατάσταση των θρεπτικών στοιχείων. Βοηθά επίσης στην ανίχνευση της ανάγκης για χρήση λιπασμάτων και πολλών ακόμα γεωργικών αναγκών.

Αισθητήρες, όπως αυτοί που απεικονίζονται στην Εικόνα 3.1, είναι η βάση της αγροτικής και κτηνοτροφικής εξέλιξης οι οποίοι δίνουν την δυνατότητα στους επαγγελματίες του είδους να γνωρίζουν τις καταστάσεις στις οποίες βρίσκονται οι εγκαταστάσεις, τα μηχανήματα, τα ζώα και οτιδήποτε μπορεί να συνδεθεί με έναν αισθητήρα.



Εικόνα 3.1: Αισθητήρες και δίκτυο σε αγροτικό χώρο [7.11]

Επιπλέον, με την χρήση τεχνολογιών όπως το δίκτυο LoRaWAN οι κτηνοτρόφοι έχουν την δυνατότητα να ελέγχουν την τοποθεσία των ζώων τους μεμονωμένα, με την απλή τοποθέτηση ενός εξωτερικού chip επάνω τους. Αυτού του είδους οι ανιχνευτές είναι εξοπλισμένοι με μπαταρίες ικανές να διαρκέσουν επάνω από μία δεκαετία, με αυτόν τον τρόπο η εγκατάσταση γίνεται μία φορά σε κάθε ζώο και μπορεί αργότερα εάν κριθεί απαραίτητο να αλλάξει από ζώο σε ζώο. Στην Εικόνα 3.2 απεικονίζεται ένα παράδειγμα ενός τέτοιου δικτύου, συγκεκριμένα του LoRaWAN, που διαπρέπει στον συγκεκριμένο τομέα αλλά παράλληλα προσφέρει πολλές ακόμα δυνατότητες.



Εικόνα 3.2: Χαρακτηριστικά της τεχνολογίας LoRaWAN [7.12]

Η γεωργία είναι ένας από τους σημαντικότερους τομείς που ενσωματώνουν τα μη επανδρωμένα αεροσκάφη (drones). Τα drones που είναι εξοπλισμένα με αισθητήρες και κάμερες χρησιμοποιούνται για την απεικόνιση, τη χαρτογράφηση και την τοπογράφηση γεωργικών εκμεταλλεύσεων. Υπάρχουν επίγεια drones και εναέρια drones. Τα επίγεια drones είναι ρομπότ που επιθεωρούν τα χωράφια με ρόδες. Τα εναέρια drones, γνωστά ως μη επανδρωμένα εναέρια οχήματα (UAV) ή μη επανδρωμένα συστήματα αεροσκαφών (UAS), είναι ιπτάμενα ρομπότ. Τα drones μπορούν να ελέγχονται εξ αποστάσεως μέσω ειδικών χειριστηρίων ή να πετούν αυτόματα μέσω σχεδίων πτήσης ελεγχόμενων από λογισμικό στα ενσωματωμένα συστήματά τους, τα οποία λειτουργούν σε συντονισμό με αισθητήρες και GPS. Από τα δεδομένα τα οποία παρέχουν τα drones μπορούν να εξαχθούν πληροφορίες σχετικά με την υγεία των καλλιεργειών, την άρδευση, τον ψεκασμό, τη φύτευση, το έδαφος και τον αγρό, την καταμέτρηση των φυτών, την πρόβλεψη της απόδοσης και πολλά άλλα. Τα drones μπορούν είτε να προγραμματιστούν για έρευνες σε αγροκτήματα (drone as a service) είτε να αγοραστούν και να αποθηκευτούν κοντά σε αγροκτήματα όπου μπορούν να φορτιστούν και να συντηρηθούν. Μετά τις έρευνες, τα μη επανδρωμένα αεροσκάφη πρέπει να μεταφέρονται σε κοντινά εργαστήρια για την ανάλυση των δεδομένων που έχουν συλλεχθεί, συμβάλλοντας έτσι στην καλύτερη αξιοποίηση του IoT στη γεωργία. Η γεωργία με τη βοήθεια του IoT έχει βοηθήσει στην εφαρμογή σύγχρονων τεχνολογικών λύσεων σε δοκιμασμένες στο χρόνο γνώσεις. Αυτό βοήθησε να γεφυρωθεί το χάσμα μεταξύ της παραγωγής και της ποιοτικής και ποσοτικής απόδοσης. Η εισαγωγή δεδομένων με τη λήψη και την εισαγωγή πληροφοριών από τους

πολλαπλούς αισθητήρες για χρήση σε πραγματικό χρόνο ή αποθήκευση σε μια βάση δεδομένων εξασφαλίζει ταχεία δράση και λιγότερες ζημιές στις καλλιέργειες.

Συνεπώς, με την χρήση μερικών αισθητήρων, μίας οθόνης και των νέων ανερχόμενων τεχνολογιών ο αγρότης πλέον μπορεί να διαχειρίζεται την φάρμα και τα χωράφια του μέσα από το χέρι του και να έχει απόλυτο έλεγχο και γνώση σε κάθε σημείο των εγκαταστάσεων του μέσα από μια ευφυέστατη και ταυτόχρονα απόλυτα κατανοητή για τον άνθρωπο τεχνολογία. Προβλήματα τα οποία μέχρι σήμερα μάστιζαν την αγροτική παραγωγή μπορούν πλέον εύκολα να ελεγχθούν σημαντικά με τη χρήση συστήματος γεωργίας που βασίζεται στο IoT.

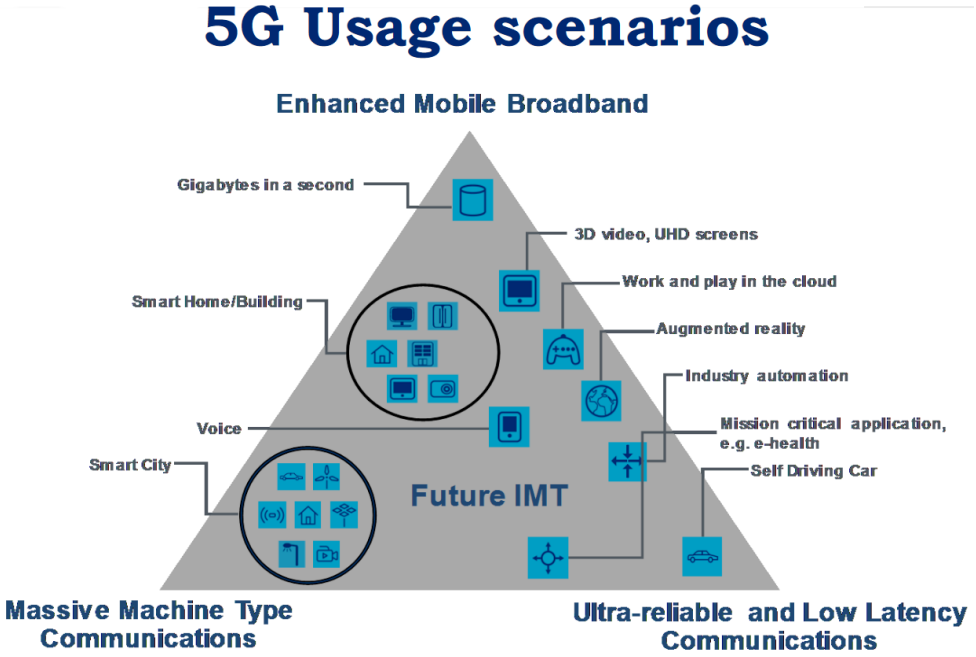
3.5 Αυτοματοποίηση διαδικασιών

Στη μεταποιητική βιομηχανία, η εκτέλεση επαναλαμβανόμενων εργασιών, όπως η περιτύλιξη ετικετών, η συσκευασία κ.λπ., με το χέρι είναι δύσκολη και επιρρεπής σε ανθρώπινα λάθη. Το Διαδίκτυο των πραγμάτων (IoT) στη βιομηχανία αποδεικνύεται ότι αλλάζει τα δεδομένα για τις εταιρείες αυτοματισμού. Οι εταιρείες βιομηχανικού αυτοματισμού που χρησιμοποιούν λύσεις IoT μπορούν να αποκομίσουν νέα οφέλη. Το IoT συμβάλλει στη δημιουργία νέων τεχνολογιών για την επίλυση προβλημάτων, τη βελτίωση των λειτουργιών και την αύξηση της παραγωγικότητας. Επιπλέον μπορεί να αναφερθεί ως η σύνδεση αμιγώς αναγνωρίσιμων ηλεκτρονικών συσκευών με τη χρήση "data plumbing" του Διαδικτύου, συμπεριλαμβανομένων του πρωτοκόλλου Διαδικτύου (IP), του υπολογιστικού νέφους και των υπηρεσιών ιστού. Με τη χρήση tablet, έξυπνων τηλεφώνων, εικονικών συστημάτων και αποθήκευση δεδομένων στο σύννεφο, ο αντίκτυπος του IoT στον βιομηχανικό αυτοματισμό είναι εξαιρετικά μεγάλος.

Στη βιομηχανία παραγωγής κρύων ποτών. Εδώ, απαιτείται η διασύνδεση μεταξύ των μηχανημάτων παραγωγής και των μεταφορικών ταινιών προκειμένου να ανταλλάσσουν πληροφορίες, κατάσταση και δεδομένα. Αυτή η διασύνδεση εξαρτάται από το IoT. Η κατάσταση του παραγόμενου προϊόντος και η αναφορά για την κατάσταση των μηχανημάτων αποστέλλονται στον κατασκευαστή σε τακτά χρονικά διαστήματα, προκειμένου να εντοπίζονται εκ των προτέρων τυχόν βλάβες. Μια βιομηχανία εξοπλισμένη με IoT είναι επωφελής, καθώς αυξάνει την ταχύτητα παραγωγής και διατηρεί την ομοιόμορφη ποιότητα του προϊόντος καθ' όλη τη διάρκεια της παραγωγής. Βοηθά επίσης να γίνει ο χώρος εργασίας πιο αποτελεσματικός και ασφαλής μειώνοντας έτσι τα ανθρώπινα λάθη.

4 Βασικές εφαρμογές του 5G

Το 5G δεν είναι διαδεδομένη έννοια στην καθημερινότητα μας, πολλοί από εμάς το γνωρίζουμε ελάχιστα ή μονάχα το έχουμε ακούσει αναφορικά. Όπως απεικονίζεται στην εικόνα 4.1, οι προοπτικές που ~~μας~~ προσφέρει το 5G ξεπερνούν κάθε προσδοκία προηγουμένων δικτύων κινητής τηλεφωνίας. Σε αυτό το κεφάλαιο θα συναντήσουμε μερικές βασικές αναβαθμίσεις οι οποίες είναι ικανές να εισαχθούν στη ζωή μας με την συνεισφορά του 5G και τους τρόπους με τους οποίους μπορούν να βελτιώσουν τη ζωή μας.



Εικόνα 4.1: Χρήσεις του 5G [7.15]

4.1 Βελτιωμένη εξ αποστάσεως εκπαίδευση

Οι περιορισμοί της εποχής της πανδημίας που οδήγησαν στην εξ αποστάσεως μάθηση ανέδειξαν τα τρωτά σημεία των σημερινών υποδομών συνδεσιμότητας. Οι μαθητές αναγκάστηκαν να βασίζονται σε ανομοιογενή και αναξιόπιστα δίκτυα τα οποία δεν ήταν ικανά να στηρίξουν τη διαδικασία της μόρφωσης τους στα αναμενόμενα επίπεδα. Ωστόσο, καθώς οι εταιρείες τηλεπικοινωνιών αναπτύσσουν τα δίκτυα 5G, περισσότερες κοινότητες θα έχουν πρόσβαση σε υψηλές ταχύτητες, μεγαλύτερη χωρητικότητα και την υψηλή αξιοπιστία που προσφέρει το 5G.

Με τη σειρά του, το 5G θα επιτρέψει την καλύτερη πρόσβαση σε απομακρυσμένες εκπαιδευτικές εμπειρίες, δήλωσε ο Shamik Mishra, CTO υπεύθυνος για τη συνδεσιμότητα στην Capgemini Engineering. Το πιο σημαντικό είναι ότι τα εκπαιδευτικά ιδρύματα μπορούν να αναπτύξουν και να παρέχουν νέα και διαφορετικά είδη μαθησιακού περιεχομένου, όπως η ζωντανή ροή εκδηλώσεων, μέσω του 5G.

4.2 Ευφυέστερη εφοδιαστική (Logistics)

Ο τομέας της εφοδιαστικής αλυσίδας, συμπεριλαμβανομένων των μεταφορών, έχει επεκτείνει τη χρήση του IoT για την παρακολούθηση των αποστολών κατά τη μετακίνησή τους στα διεθνή σύνορα και σε όλο τον κόσμο. Ο κλάδος προχωρά επίσης με τη χρήση αυτόνομων οχημάτων στις εργασίες οι οποίες απευθύνονται στην αποθήκευση και την δρομολόγηση των προϊόντων κάθε είδους. Επιπλέον, το IoT έχει αλλάξει τον τρόπο με τον οποίο οι εταιρείες σκέφτονται για τα logistics και, με τη σειρά του, προκάλεσε την άνοδο μιας πιο συνδεδεμένης αλυσίδας εφοδιασμού. Τα δεδομένα που παράγονται από αυτές τις συσκευές μπορούν να χρησιμοποιηθούν για τον εντοπισμό ανωμαλιών ώστε να αποφευχθούν δαπανηρές διακοπές ή καθυστερήσεις στην αλυσίδα εφοδιασμού, να βελτιωθεί η αποδοτικότητα μέσω προγνωστικών αναλύσεων και να ενισχυθεί η ικανοποίηση των πελατών με πληροφορίες σε πραγματικό χρόνο σχετικά με την κατάσταση της παράδοσης.

Ο αριθμός των αισθητήρων που απαιτούνται για τη μετακίνηση και την επεξεργασία όλων αυτών των δεδομένων καταπονεί τα δίκτυα 4G και LTE. Αυτό περιορίζει την ικανότητα της βιομηχανίας να αξιοποιήσει τις προηγμένες τεχνολογίες. Το 5G αίρει αυτόν τον περιορισμό της χωρητικότητας των κυψελών (αναφερόμενοι στα κυψελωτά δίκτυα), δίνοντας στον κλάδο περισσότερες ευκαιρίες για την επέκταση της χρήσης έξυπνων συσκευών.

Μερικές, αναφορικά, από τις τεράστιες ανερχόμενες εξελίξεις στον τομέα των logistics θα αφορούν:

- Αυξημένη ορατότητα της αλυσίδας εφοδιασμού
- Καλύτερη διαχείριση στόλου
- Ακριβής διαχείριση αποθήκης
- Προβλεπτική διαδικασία λήψης αποφάσεων
- Λιγότεροι κίνδυνοι στην αλυσίδα εφοδιασμού

Για να προετοιμαστούν για τα μελλοντικά δίκτυα 5G, οι επιχειρήσεις θα πρέπει να υιοθετήσουν υποδομές δεδομένων που επιτρέπουν γρήγορη, κλιμακούμενη ανάλυση και έξυπνη διαχείριση αποθεμάτων. Η υιοθέτηση του 5G σημαίνει ότι οι επιχειρήσεις πρέπει να υιοθετήσουν υποδομές δεδομένων που υποστηρίζουν ευέλικτες αναλύσεις και έξυπνες πρακτικές διαχείρισης αποθεμάτων.

4.3 Προηγμένη υγειονομική περίθαλψη

Η υγειονομική περίθαλψη είναι ένας άλλος κλάδος που χρησιμοποιεί το 5G για να προωθήσει και να βελτιώσει τις δραστηριότητές του.

Το 5G μπορεί να υποστηρίξει και να βελτιώσει την ανταπόκριση στις κρίσιμες και στις αναφερόμενες ως περιπτώσεις "ζωής και θανάτου" που είναι χαρακτηριστικές στον ιατρικό χώρο. Οι οργανισμοί υγειονομικής περίθαλψης μπορούν να χρησιμοποιήσουν το 5G με πολλούς τρόπους, όπως η ανάλυση, η παρακολούθηση ασθενών, η εξ αποστάσεως διάγνωση και η χειρουργική επέμβαση με τη βοήθεια ειδικά ανεπτυγμένων για τον ιατρικό τομέα ρομπότ.

Η τεχνολογία παρέχει αξιοπιστία και ικανότητα που ανταγωνίζεται τα δίκτυα σταθερής τηλεφωνίας, ενώ επιτρέπει την κινητικότητα εντός των εγκαταστάσεων με τρόπο που δεν μπορούν να παρέχουν τα ενσύρματα δίκτυα. Όπως φαίνεται στην Εικόνα 4.2, ένας ασθενής μπορεί ταυτόχρονα να παρακολουθείται από διάφορους φορείς και να παρέχει σε πραγματικό χρόνο πληροφορίες χρήσιμες για την βελτίωση της υγείας του, την αντιμετώπιση προβλημάτων που μπορεί να προκύψουν κατά την νοσηλεία του και πληροφορίες οι οποίες θα συμβάλουν στην ενημέρωση της πολιτείας σχετικά με επιδημιολογικά και ασφαλιστικά στοιχεία, με σκοπό την αποφυγή μεταγενέστερων προβλημάτων είτε αυτά αφορούν την υγεία του συγκεκριμένου ασθενούς είτε του γενικού πλήθους ανθρώπων.

Εικόνα 4.2: Διάγραμμα παρακολούθησης ασθενούς [7.16]

4.4 Ισχυρότερη στήριξη του εργατικού δυναμικού

Το 5G μπορεί να έχει μεγάλο αντίκτυπο στους εργαζόμενους σε όλους τους εργασιακούς τομείς. Μπορεί να παρέχει υποστήριξη στην απομακρυσμένη εργασία, παρέχοντας μια πολύ ταχύτερη και πιο αξιόπιστη σύνδεση που είναι ικανή να προσφέρει αρκετή ανθεκτικότητα για να υποστηρίξει ακόμη και την απομακρυσμένη εργασία η οποία απαρτίζεται από κρίσιμης σημασίας επιλογές και κινήσεις σε πραγματικό χρόνο. Ομοίως επιτρέπει την απομακρυσμένη συνεργασία με τη χρήση επαυξημένης πραγματικότητας και άλλων παρόμοιων προηγμένων τεχνολογιών. Επιπλέον είναι ικανό να υποστηρίζει την εκπαίδευση προσωπικού η οποία χρησιμοποιεί AR και παρόμοια εργαλεία.

Το 5G υποστηρίζει επίσης προηγμένες πρωτοβουλίες για την ασφάλεια στο χώρο εργασίας. Για παράδειγμα, ένας κατασκευαστής μπορεί να χρησιμοποιήσει ένα σύστημα ανάλυσης βίντεο που υποστηρίζεται από τη συνδεσιμότητα 5G για να αναλύσει και να δράσει σε κρίσιμα ζητήματα ασφάλειας, όπως το μπλοκάρισμα της έναρξης λειτουργίας ενός βαρέως εργαλείου ή εξοπλισμού εάν το σύστημα εντοπίσει έναν εργαζόμενο χωρίς τον απαραίτητο εξοπλισμό ασφαλείας που προϋποθέτει η χρήση του.

5 Συνδυαστικές εφαρμογές των IoT και 5G τεχνολογιών

Οι μαζικές κυψελοειδείς τεχνολογίες IoT χαρακτηρίζονται ως λύση χαμηλού κόστους και χαμηλής κατανάλωσης ενέργειας. Ευδοκιμούν επάνω στη βαθιά και ευρεία κάλυψη σε εσωτερικούς αλλά και εξωτερικούς χώρους. Παρέχουν ασφαλή συνδεσιμότητα και έλεγχο ταυτότητας (authentication), είναι εύκολο να αναπτυχθούν σε οποιαδήποτε τοπολογία δικτύου και έχουν σχεδιαστεί για πλήρη επεκτασιμότητα και αναβαθμίσεις στη χωρητικότητα τους. Με γνώμονα τις συσκευές IoT, το 5G συνδέει περισσότερες συσκευές σε υψηλότερες ταχύτητες και καθιστά πράγματα όπως η καθυστέρηση (lagging) σχεδόν ανύπαρκτα. Ως αποτέλεσμα, το 5G δημιουργεί μια εξαιρετική εμπειρία για τον χρήστη, ανεξάρτητα από την εφαρμογή, τη συσκευή ή την υπηρεσία την οποία πραγματεύεται.

5.1 Εντοπισμός περιουσιακών στοιχείων (Asset tracking)

Η παρακολούθηση περιουσιακών στοιχείων (ή όπως θα αναφέρεται, Asset Tracking) με το IoT δεν είναι κάτι καινούργιο, αλλά η χρήση του 5G για συνδεσιμότητα προσφέρει μοναδικά οφέλη. Παρακάτω παρατίθεται ένας σύντομος κατάλογος περιπτώσεων χρήσης, με βάση τη γενική αρχή ότι μια λύση Asset Tracking στέλνει περιοδικά μικρές ποσότητες δεδομένων από έναν αισθητήρα στο cloud για να αποθηκευτούν, να αναλυθούν και να ληφθούν μέτρα για τη βελτιστοποίηση της χρήσης των περιουσιακών στοιχείων μας:

- Παρακολούθηση ενός μετρητή νερού ή αερίου για τον προσδιορισμό της χρήσης τους στο χρόνο
- Παρακολούθηση της κατάστασης ενός δημοτικού φωτεινού σηματοδότη ή μιας θέσης στάθμευσης
- Παρακολούθηση της θερμοκρασίας και της θέσης ενός κουτιού μπανάνες καθώς ταξιδεύει σε όλο τον κόσμο

Υπάρχουν άπειρες ακόμα υποθέσεις στις οποίες θα μπορεί ο συνδυασμός αυτών των τεχνολογιών να ωφελήσει. Δημιουργείται το ερώτημα, γιατί βλέπουμε μια τόσο μεγάλη διαφορά στις δυνατότητες με την συνεισφορά του 5G; Βασικοί λόγοι είναι οι ακόλουθοι:

- Συμβατότητα προς τα εμπρός (forward compatibility): Τα δίκτυα 4G LTE που είναι διαθέσιμα σήμερα είναι συμβατά προς τα εμπρός με το 5G. Για παράδειγμα, τα δίκτυα CAT-M1 και NB-IoT -γνωστά ως δίκτυα ευρείας περιοχής χαμηλής ισχύος (LPWAN)- είναι οι πρόδρομοι των μαζικών επικοινωνιών τύπου μηχανής 5G (mMTC). Ορισμένο υλικό 4G LTE μπορεί να ενεργοποιηθεί για δυνατότητες 5G με αναβάθμιση υλικολογισμικού.
- Αισθητήρες χαμηλής ισχύος, χαμηλού κόστους: Οι αισθητήρες LPWA έχουν μεγάλη διάρκεια ζωής της μπαταρίας και είναι διαθέσιμοι σε χαμηλό κόστος καθιστώντας τα επιχειρηματικά μοντέλα λειτουργικά.
- Καλύτερη κάλυψη: Οι τεχνολογίες 4G LTE όπως το CAT-M1 και το NB-IoT έχουν καλύτερη ασύρματη κάλυψη μέσα σε κτίρια, υπόγεια και σε αγροτικές περιοχές. Μπορούν να μεταδίδουν δεδομένα σε περισσότερες συσκευές σε συμπυκνωμένη περιοχή από ό,τι άλλες τεχνολογίες κυψελωτής τηλεφωνίας.

Αρχικά θα οριστεί η mMTC ώστε να κατανοηθεί καλύτερα η σημασία αυτής της εξέλιξης. Ο ορισμός στηρίζεται στα λόγια του Dave Dukinfield, CX Product Manager στη Cisco’s CX SP Practice team: «Παροχή συνδεσιμότητας σε μεγάλο αριθμό συσκευών που μεταδίδουν περιοδικά μικρό όγκο κίνησης που συναντάται στα συστήματα IoT επόμενης γενιάς.»

Αυτός μπορεί περεταίρω να αναλυθεί, με εξήγηση των βασικών διαφορών με τα υπάρχοντα συστήματα χωρίς τη χρήση του 5G. Η μαζική επικοινωνία τύπου μηχανής (mMTC), επίσης γνωστή ως μαζική επικοινωνία μηχανής (MMC) ή μαζική επικοινωνία μηχανής με μηχανή (Machine to Machine) είναι ένας τύπος επικοινωνίας μεταξύ μηχανών μέσω ενσύρματων ή ασύρματων δικτύων, όπου η παραγωγή δεδομένων, η ανταλλαγή πληροφοριών και οι λειτουργείες πραγματοποιούνται με ελάχιστη ή καθόλου παρέμβαση από τον άνθρωπο. Αποτελεί υποκατηγορία της επικοινωνίας τύπου μηχανής (MTC). Η mMTC ασχολείται ιδιαίτερα με την ασύρματη συνδεσιμότητα και δικτύωση μεταξύ μαζικών αριθμών (δισεκατομμυρίων) μηχανών και θεωρείται βασική εξέλιξη από το Διαδίκτυο των πραγμάτων IoT στο Διαδίκτυο των πάντων ή αλλιώς IoE.

Επιστρέφοντας στο Asset Tracking, η Cognizant, μια Αμερικανική πολυεθνική εταιρεία παροχής υπηρεσιών τεχνολογίας πληροφοριών και παροχής συμβουλών, σχεδίασε μια προ-διαμορφωμένη, προσαρμόσιμη εφαρμογή παρακολούθησης ψυκτικής αλυσίδας και περιουσιακών στοιχείων, για να επιταχύνει την πρόσβαση σε πολύτιμα δεδομένα αισθητήρων για την έγκαιρη λήψη αποφάσεων. Οραματίστηκαν να παρέχουν στους υπεύθυνους επιχειρήσεων, logistics και εφοδιαστικής αλυσίδας μια προβολή σχεδόν σε πραγματικό χρόνο για την παρακολούθηση ευπαθών και ευαίσθητων στη θερμοκρασία αγαθών, όπως φάρμακα, τρόφιμα και ποτά και αγροτικά προϊόντα. Ο στόχος είναι να παρακολουθούν αυτά τα αγαθά καθώς μετακινούνται από το εργοστάσιο (ή το χωράφι) στην αποθήκη, να διατηρούν αρχεία καταγραφής και να ειδοποιούν για τις διακυμάνσεις της θερμοκρασίας ώστε να διασφαλίζεται η ασφάλεια και η συμμόρφωση τους.

5.2 Επιχειρησιακά κρίσιμες εφαρμογές

Το 5G προσφέρει εξαιρετικά αξιόπιστη χαμηλή καθυστέρηση που επιτρέπει τη διαχείριση κρίσιμων περιπτώσεων ακριβείας για τις επιχειρήσεις, όπου η ασφάλεια αποτελεί ύψιστη προτεραιότητα. Τα δίκτυα χαμηλής καθυστέρησης είναι ιδανικά για τη διοίκηση και τον έλεγχο αυτοματοποιημένων οχημάτων καθοδήγησης (AGV) σε μια αποθήκη, την επικοινωνία σε πραγματικό χρόνο μεταξύ ρομπότ σε ένα έξυπνο εργοστάσιο και το ζωντανό βίντεο με χρήση τεχνητής νοημοσύνης για τον έλεγχο ποιότητας.

Ένας Καναδός κατασκευαστής ρομποτικών λύσεων εφοδιαστικής αλυσίδας σε συνεργασία με έναν καναδικό φορέα εκμετάλλευσης ασύρματων δικτύων για τη δημιουργία μιας ολοκληρωτικής τρισδιάστατης ρομποτικής λύσης, χρησιμοποιώντας ένα ιδιωτικό δίκτυο κινητής τηλεφωνίας βελτιστοποιημένο για χαμηλή καθυστέρηση. Η μοναδική τεχνολογία αυτοματισμού της εταιρείας συμπυκνώνει σειρές και διαδρόμους ραφιών αποθήκης σε ενιαίες, κάθετες δομές αποθήκευσης. Στόλοι ρομποτικών λεωφορείων (shuttles) κινούνται οριζόντια και κάθετα κατά μήκος των αξόνων X, Y και Z εντός αυτών των δομών, ανακτώντας τα εμπορεύματα και παραδίδοντάς τα στην περίμετρο, όπου οι εργαζόμενοι τα διαλέγουν, τα συσκευάζουν και τα αποστέλλουν, όπως απεικονίζεται στην Εικόνα 5.1. Η εταιρεία ισχυρίζεται ότι το αρθρωτό προϊόν της εφοδιαστικής αλυσίδας "όλα σε ένα" (all-in-one) μπορεί να μειώσει τις απαιτούμενες ανάγκες ενός λιανοπωλητή σε χώρο αποθήκης κατά 85%.

Σκεπτόμενοι αυτές τις εξελίξεις στο χώρο των τεχνολογιών του IoT και του 5G δεν μπορούμε παρά να ελπίζουμε στην ανάπτυξη των εργασιακών παραγόντων και την βελτίωση της εργασιακής ποιότητας στις επιχειρήσεις και βιομηχανίες. Όμως, η ικανοποίηση των απαιτήσεων των κρίσιμων αποστολών του IoT απαιτεί μια προσέγγιση παγκόσμιας κλάσης στον σχεδιασμό και τη δοκιμή. Δίνοντας έμφαση στον σχεδιασμό, τη δοκιμή και την ασφάλεια συσκευών, ασύρματων επικοινωνιών, δικτύων και υποδομών IoT, οι λύσεις που μπορούν να αναπτυχθούν θα είναι ικανές να καλύπτουν ολόκληρη τη στοίβα (στρώματα 1-7), από τις συσκευές άκρου (ή συσκευές σημείου εισόδου) έως την απόδοση και την ασφάλεια του δικτύου, καθώς και ολόκληρο τον κύκλο ζωής του προϊόντος, από τα αρχικά στάδια του σχεδιασμού έως την κατασκευή του και πέραν αυτού.

Εικόνα 5.1: Παράδειγμα αυτόματων γερανών για την αποθήκευση τροφίμων [7.19]

5.3 Έξυπνες πόλεις

Με απλά λόγια, οι "έξυπνες πόλεις" (smart cities) χρησιμοποιούν τις αναδυόμενες τεχνολογίες των 5G και IoT για να δημιουργήσουν και να προσφέρουν συνδεδεμένες λύσεις για την ευημερία μιας κοινότητας. Ενώ η καινοτομία της τεχνολογίας 5G δεν θα διευκολύνει από μόνη της την πρόοδο των έξυπνων πόλεων, η νέες υποδομές που βασίζονται στο δίκτυο του 5G διευρύνουν σημαντικά τις δυνατότητες των πόλεων να χρησιμοποιούν

έξυπνες συσκευές, αισθητήρες και δεδομένα για τη βελτίωση των λειτουργιών και των λειτουργιών. Με το 5G να αποτελεί τη νεότερη ασύρματη τεχνολογία, τα πάντα, από έξυπνους αισθητήρες έως αυτοκινούμενα αυτοκίνητα, μπορούν πλέον να επικοινωνούν με εξαιρετικά γρήγορες ταχύτητες με χαμηλή καθυστέρηση και χωρίς να είναι συνδεδεμένα με καλώδιο ethernet, με αποτέλεσμα πιο αποδοτικά συστήματα και πόρους.

5.3.1 Συμβολή του 5G

Λιγότερη καθυστέρηση σημαίνει συμπίεση του χρόνου μεταξύ αποστολής και λήψης του σήματος. Το 5G φέρνει το εύρος τουλάχιστον κάτω από 10 χιλιοστά του δευτερολέπτου (δηλαδή το μισό από το πιο προηγμένο 4G που θα μπορούσε να επιτύχει) και στην καλύτερη περίπτωση γύρω στο 1 χιλιοστό του δευτερολέπτου καθυστερήσεις, που σημαίνει ότι τα δεδομένα θα μεταφέρονται περίπου σε πραγματικό χρόνο. Έχοντας πει αυτά, τί κάνει το 5G τόσο αναγκαίο για την ανάπτυξη και εδραίωση των έξυπνων πόλεων; Παρακάτω θα αναφερθούν καταστάσεις όπου η νέα τεχνολογία κρίνεται ως ζωτικής σημασίας για την δημιουργία και την εξέλιξη των έξυπνων πόλεων:

- Δημόσια ασφάλεια και προστασία. Οι αστυνομικοί και οι αξιωματικοί έκτακτης ανάγκης θα μπορούν να εντοπίζουν και να λαμβάνουν πληροφορίες σε πραγματικό χρόνο σχετικά με ατυχήματα και κλήσεις έκτακτης ανάγκης από έξυπνους αισθητήρες που έχουν τοποθετηθεί σε όλη την πόλη.
- Κινητικότητα. Τα δίκτυα 5G θα παρέχουν ταχύτερη και με μικρότερη καθυστέρηση συνδεσιμότητα για τα συστήματα δημόσιων μεταφορών, διευκολύνοντας την πλοήγηση των αυτόνομων οχημάτων και των ανθρώπων στις πόλεις.
- Διαχείριση της κυκλοφορίας. Ο συνδυασμός των δικτύων 5G και των συσκευών IoT αναμένεται να παρακολουθεί και να διαχειρίζεται έξυπνα τις κυκλοφοριακές ροές, να παρακολουθεί τις οδικές συνθήκες και να μειώνει την κυκλοφοριακή συμφόρηση.
- Ενεργειακή απόδοση. Το 5G δημιουργεί τεράστιες ευκαιρίες για συνδεδεμένες συσκευές εντός κτιρίων και πόλεων που θα βοηθήσουν στην παρακολούθηση και τον έλεγχο της ενέργειας. Αυτό βοηθάει τα κτίρια και τις πόλεις να διαχειρίζονται καλύτερα τον ενεργειακό τους εφοδιασμό, να εξοικονομούν χρήματα και να γίνονται πιο βιώσιμες.

Επιπλέον, με τα νέα δίκτυα, η ταχύτητα και η καθυστέρηση δεν χειροτερεύουν ακόμη και με δεκάδες χιλιάδες συνδεδεμένες συσκευές. Συνεπώς, το 5G προσφέρει μεγαλύτερη πυκνότητα συσκευών. Ο συνδυασμός υψηλής πυκνότητας και χαμηλής καθυστέρησης θα μεταμορφώσει τις πόλεις μας. Σήμερα, σε πολυσύχναστα σημεία διακοπών ή σε γήπεδα, η σύνδεση μπορεί μερικές φορές να χειροτερέψει.

Με το 5G δεν θα υφίσταται αυτή η κατάσταση: θα είναι δυνατό να υπάρχει ένας τεράστιος αριθμός (έως και ενός εκατομμυρίου) συνδέσεων ταυτόχρονα για κάθε τετραγωνικό χιλιόμετρο. Αυτό σημαίνει ότι, εκτός από τις προσωπικές συσκευές, όπως τα smartphones, τα tablets οι υπολογιστές, πλέον αντικείμενα και αισθητήρες θα μπορούν να καταγράφουν πληροφορίες και να συνομιλούν μεταξύ τους. Η έμφαση θα δοθεί στην εξαιρετική απλότητα, στη χαμηλή κατανάλωση ενέργειας για να εξασφαλιστεί μεγαλύτερος χρόνος λειτουργίας και στη διάχυτη κάλυψη για την πρόσβαση δύσκολων τοποθεσιών, καθώς και στην αυξημένη πυκνότητα συνδέσεων, ώστε τα δίκτυα να μπορούν να διαχειριστούν τον τεράστιο αριθμό συσκευών που αναπτύσσονται για εφαρμογές IoT. Ως εκ τούτου, το 5G αφαιρεί ουσιαστικά μια από τις αντιστάσεις στην ανάπτυξη του IoT, το οποίο έτσι θα μπορέσει να εκφράσει τις δυνατότητές του όχι μόνο στο οικιακό περιβάλλον αλλά και σε βιομηχανικές εγκαταστάσεις, σε δημόσια κτίρια ή στους δρόμους.

5.3.2 Συμβολή του IoT

Από την άλλη πλευρά έχουν το IoT με τις δικές του ξεχωριστές ικανότητες και λειτουργείες, μαζί με την τεχνολογία 5G, IoT αποτελεί βασική πτυχή για τη δημιουργία μιας πραγματικής, πλήρως λειτουργικής έξυπνης πόλης. Αυτή η τεχνολογία παρέχει στις επιχειρήσεις, τις πόλεις και τους ιδιώτες τη δυνατότητα να παρακολουθούν, να διαχειρίζονται και να ελέγχουν αυτές τις συνδεδεμένες συσκευές, ενώ παράλληλα συλλέγουν δεδομένα, αναλύσεις και πληροφορίες σε πραγματικό χρόνο. Μερικές χρήσεις του όσον αφορά τις έξυπνες πόλεις είναι:

- Διαχείριση ενέργειας
- Διαχείριση της ποιότητας του αέρα
- Παρακολούθηση και διαχείριση της κυκλοφορίας
- Συνδεδεμένες δημόσιες μεταφορές
- Συνδεδεμένοι σηματοδότες και φωτισμοί δρόμου
- Παρακολούθηση καιρού
- Διαχείριση αποβλήτων

Καθώς το IoT γίνεται όλο και πιο διαδεδομένο, τα έξυπνα κτίρια γίνονται όλο και μεγαλύτερο συστατικό των έξυπνων πόλεων. Ενώ οι ιδιοκτήτες και οι διαχειριστές κτιρίων αναζητούσαν πάντα νέους και καλύτερους τρόπους για τη μείωση του κόστους και τη βελτίωση της ενεργειακής απόδοσης, τα παραδοσιακά συστήματα διαχείρισης κτιρίων (BMS) έχουν αρχίσει να ξεπερνιούνται εν μέσω των πρόσφατων τεχνολογικών εξελίξεων. Αυτό διότι τα καλωδιακά δίκτυα στα κτίρια φτάνουν γρήγορα στα όρια των δεδομένων τους, αλλά οδηγούν επίσης σε υψηλότερο κόστος και αυξημένη πολυπλοκότητα. Σήμερα, τα έξυπνα κτίρια μπορούν να αξιοποιήσουν την ασύρματη τεχνολογία, τις συσκευές IoT, τον αυτοματισμό κτιρίων και την ανάλυση δεδομένων για την αξιολόγηση και την παρακολούθηση των διαδικασιών, ενώ παράλληλα λειτουργούν πιο οικονομικά και αποδοτικά.

Μέσω αισθητήρων IoT, αυτοματισμών και απομακρυσμένης διαχείρισης, οι ιδιοκτήτες και οι διαχειριστές κτιρίων μπορούν να αναπτύξουν διάφορες συσκευές σε ολόκληρη την εγκατάσταση για να καταγράφουν δεδομένα και πληροφορίες σε πραγματικό χρόνο σχετικά με τη διαχείριση και τις λειτουργίες του κτιρίου, δίνοντάς τους τη δυνατότητα να έχουν απαράμιλλη ορατότητα στις λειτουργίες του κτιρίου τους. Εξετάζοντας συγκεκριμένα την ενεργειακή απόδοση, οι ιδιοκτήτες και οι διαχειριστές εγκαταστάσεων μπορούν πλέον να δουν ακριβώς πώς και πού χρησιμοποιείται η ενέργεια σε ένα κτίριο. Αναμφισβήτητα, η μεγαλύτερη εφαρμογή της έξυπνης αρχιτεκτονικής και υποδομής είναι τα έξυπνα δίκτυα, τα οποία βοηθούν σημαντικά στην εξοικονόμηση πόρων. Το Άμστερνταμ, για παράδειγμα, πειραματίζεται με την προσφορά οικιακών μονάδων αποθήκευσης ενέργειας και ηλιακών συλλεκτών για τα νοικοκυριά που είναι συνδεδεμένα με το έξυπνο δίκτυο της πόλης. Αυτές οι μπαταρίες συμβάλλουν στη μείωση της πίεσης στο δίκτυο τις ώρες αιχμής, επιτρέποντας στους κατοίκους να αποθηκεύουν ενέργεια κατά τις ώρες εκτός αιχμής. Οι ηλιακοί συλλέκτες επιτρέπουν επίσης στους κατοίκους να πωλούν την πλεονάζουσα ενέργεια από τους συλλέκτες πίσω στο δίκτυο.

Μαζί με την ενεργειακή απόδοση, οι ασύρματοι αισθητήρες IoT μπορούν να παρακολουθούν την υγεία των εγκαταστάσεων και την ποιότητα του αέρα. Καθώς οι άνθρωποι αρχίζουν να επιστρέφουν στο γραφείο μετά την πανδημία, η σημασία της παρακολούθησης της υγείας των εγκαταστάσεων και της ποιότητας του αέρα είναι σημαντική. Από αυτή την άποψη, οι αισθητήρες IoT διασφαλίζουν ότι οι διαχειριστές κτιρίων και οι επιχειρήσεις διατηρούν ένα υγιές περιβάλλον εργασίας μέσω προηγμένων συστημάτων.

Τέλος, η διαχείριση της ασφάλειας του IoT σε κλίμακα είναι απαραίτητη όταν πρόκειται για δεδομένα. Προκειμένου να διαπιστωθεί ότι οι συσκευές και τα δίκτυα IoT παραμένουν ασφαλή και λειτουργικά, η διαχείριση περιουσιακών στοιχείων είναι ζωτικής σημασίας, καθώς παρέχει τακτικές και ουσιαστικές αξιολογήσεις ασφάλειας του IoT.

5.3.3 Συμπέρασμα ανάπτυξης έξυπνων πόλεων

Το 5G και το IoT αποτελούν αμφότερα βασικά στοιχεία για τον μετασχηματισμό του τρόπου σύνδεσης και λειτουργίας των πόλεων. Με τις απεριόριστες δυνατότητες του IoT και τις απίστευτα γρήγορες ταχύτητες και τη χαμηλή καθυστέρηση του 5G, οι τεχνολογίες αυτές απελευθερώνουν κρίσιμες υποδομές για το μέλλον των συνδεδεμένων κοινοτήτων. Χάρη στην εξάπλωση και την υιοθέτηση του 5G και του IoT, το μέλλον των έξυπνων πόλεων θα είναι πιο ευφυές από ποτέ, παρέχοντας ατελείωτες ευκαιρίες στις κοινότητες που αξιοποιούν τη δύναμη της υπολογιστική ακμής, των δεδομένων και των τεχνολογιών από μηχανή σε μηχανή (machine-to-machine technologies). Οι έξυπνες πόλεις είναι η επόμενη μεγάλη εξέλιξη της καθημερινότητας μας και πρόκειται να οδηγήσουν την αστική ζωή στο επόμενο επίπεδο. Ωστόσο, η διασυνδεσιμότητα των έξυπνων πόλεων είναι ταυτόχρονα το μεγαλύτερο πλεονέκτημα και η μεγαλύτερη αδυναμία τους.

5.4 Εμπορικά κέντρα μεγάλης κλίμακας

5.4.1 Λιμένες

Με την ταχεία ψηφιοποίηση του δικτύου μεταφορών και εφοδιαστικής (T&L), η παραδοσιακή σκέψη της αλυσίδας εφοδιασμού -που είναι γραμμική και ανεξάρτητη- δίνει τη θέση της σε ένα διασυνδεδεμένο, ανοικτό σύστημα εφοδιαστικών λειτουργιών: τα δεδομένα ρέουν πλέον από την αρχή ενός λιμένα, μέσω του φορέα εκμετάλλευσης τερματικού σταθμού και στη συνέχεια στη ναυτιλιακή γραμμή με δυναμικό τρόπο σε πραγματικό χρόνο. Στον ευρύτερο τομέα του T&L (Transport and Logistics), οι εταιρείες έχουν αρχίσει να πειραματίζονται με μια σειρά από τεχνολογίες συνδεσιμότητας και δεδομένων. Στο σύνολό τους, οι τεχνολογίες αυτές αποτελούν το IoT, το οποίο αντιπροσωπεύει μια σύγκλιση μεταξύ του φυσικού και του ψηφιακού κόσμου, χρησιμοποιώντας τελικά τα δεδομένα και την τεχνητή νοημοσύνη AI ως πηγή αξίας.

Καθώς η τεχνητή νοημοσύνη τυποποιείται σε όλους τους κλάδους, το να γίνεις ένας οργανισμός που τροφοδοτείται με τεχνητή νοημοσύνη θα είναι πιθανότατα απαραίτητο για την επιβίωση. Αυτό σημαίνει επανεξέταση του τρόπου με τον οποίο οι άνθρωποι και

οι μηχανές αλληλοεπιδρούν σε εργασιακά περιβάλλοντα όπως τα λιμάνια και η ναυτιλία. Η υποστήριξη της συνδεσιμότητας ενός νέου τεχνολογικού οικοσυστήματος είναι μία από τις τρεις πρωταρχικές περιπτώσεις χρήσης του 5G. Οι άλλες δύο είναι η αύξηση της χωρητικότητας (κινητή ευρυζωνικότητα) και η εξαιρετικά υψηλή αξιοπιστία (χαμηλή καθυστέρηση). Ωστόσο, εξακολουθούν να υπάρχουν αρκετά σημεία συμφόρησης που πρέπει να αντιμετωπιστούν πριν από την προβλεπόμενη εδραίωση του 5G. Η αξιοποίηση των τεχνολογιών σε αυτό το πλαίσιο απαιτεί πλήρως ενσωματωμένες τεχνολογίες στον πυρήνα του οργανισμού. Το νέο ανατρεπτικό και καινοτόμο περιβάλλον του σήμερα απαιτεί την κατάκτηση της τέχνης της αλλαγής για τον μετασχηματισμό και τη δημιουργία ουσιαστικού επιχειρηματικού αντίκτυπου.

Το 2020, το Zeebrugge (ανήκει στο δήμο του Brugge στη Δυτική Φλάνδρα της φλαμανδικής περιφέρειας του Βελγίου), ένα από τα πιο πολυσύχναστα λιμάνια του κόσμου, με 45,8 εκατομμύρια τόνους εμπορευμάτων να μεταφορτώνονται ετησίως μέσω των αποβάθρων του, ανακοίνωσε την ολοκλήρωση της πρώτης φάσης ενός ιδιωτικού ασύρματου δικτύου βιομηχανικού επιπέδου 5G για το λιμάνι.

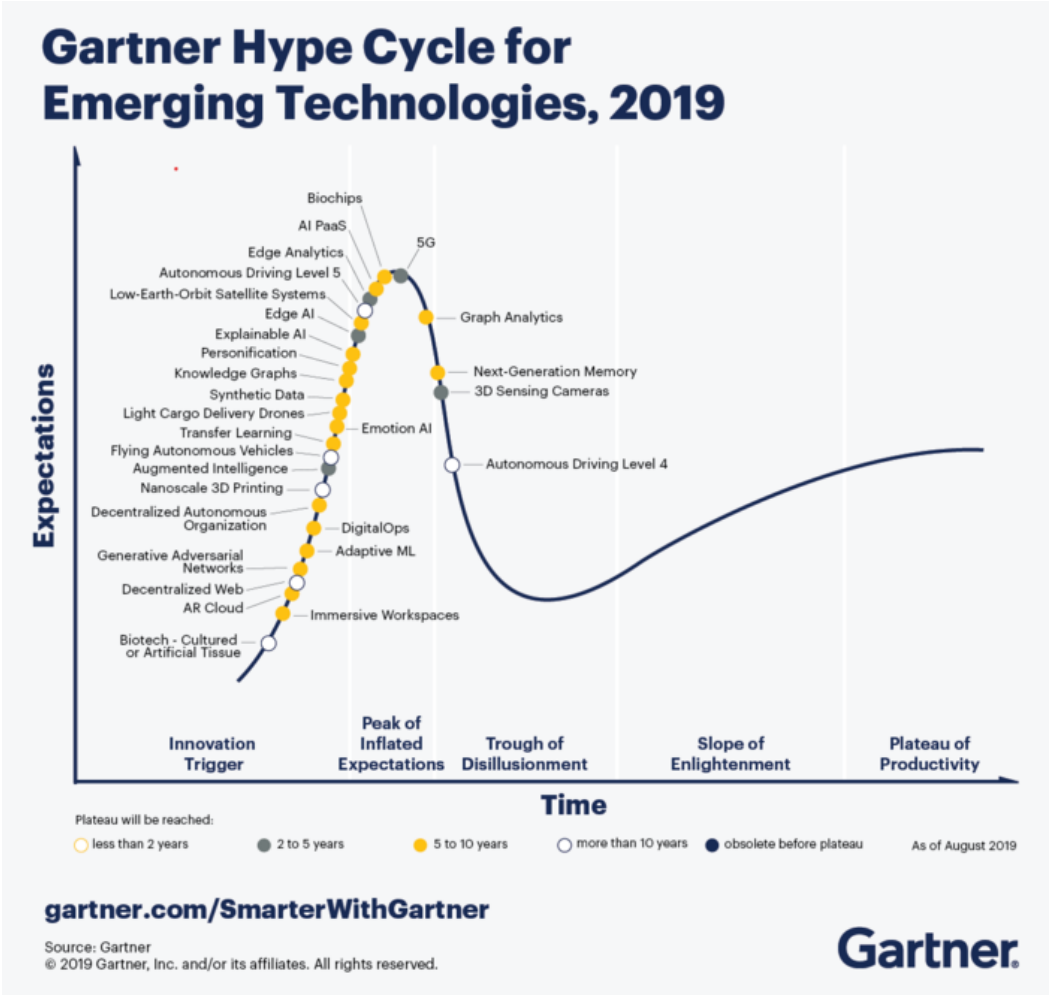
Με την εφαρμογή της πλατφόρμας Nokia Digital Automation Cloud -ιδιωτική πλατφόρμα ασύρματης δικτύωσης και υπολογισμού άκρων υψηλής απόδοσης- το Zeebrugge ελπίζει να βελτιώσει την υλικοτεχνική πρόκληση της διακίνησης και παρακολούθησης σχεδόν ενός εκατομμυρίου τόνων εμπορευμάτων κάθε εβδομάδα. Επιπλέον, η νέα πλατφόρμα θα παρέχει ιδιωτική ασύρματη συνδεσιμότητα σε περισσότερα από 100 τελικά σημεία σε όλες τις εργασιακές λειτουργίες του λιμανιού. Το δίκτυο χρησιμοποιείται τώρα για τη συνδεσιμότητα με ρυμουλκά, ανιχνευτές ατμοσφαιρικής ρύπανσης, κάμερες ασφαλείας και αισθητήρες προκυμαίας. Αυτή η συνεργασία θα επιτρέψει στο Zeebrugge να προσφέρει μια σειρά νέων και βελτιωμένων περιπτώσεων χρήσης 5G και IoT για τη βελτίωση των λειτουργικών επιδόσεων του λιμανιού και θα αναδείξει επίσης το Zeebrugge ως ηγέτη στον μετασχηματισμό και την ψηφιοποίηση των λιμανιών. Λίγους μήνες μετά, τον Ιανουάριο του 2021, ο λιμενικός τερματικός σταθμός 5 (Terminal 5) του λιμανιού του Seattle), ακολούθησε το Zeebrugge για τη χρήση της πλατφόρμας DAC της Nokia, συνεργαζόμενος με την Tideworks Technology, πάροχο τεχνολογίας λειτουργίας τερματικών σταθμών για θαλάσσιες εγκαταστάσεις, για την ανάπτυξη του Nokia Digital Automation Cloud (DAC) στο Terminal 5, το οποίο αποτελεί μέρος της Northwest Seaport Alliance, μιας από τις μεγαλύτερες πύλες εμπορευματοκιβωτίων στη Βόρεια Αμερική.

Το ιδιωτικό ασύρματο δίκτυο LTE/5G θα χρησιμοποιηθεί για την ενίσχυση του Wi-Fi, για βελτιωμένη εφεδρεία και διαθεσιμότητα, και θα υποστηρίζει τις λειτουργίες του λιμένα και τερματικού χωρίς καλώδια, χρησιμοποιώντας επικαλυπτόμενες ζώνες LTE (B53 και B48). Αυτό θα αποτελέσει πολύτιμη προσθήκη στον αυξανόμενο κατάλογο των βιομηχανικών περιπτώσεων χρήσης 5G και IoT της Nokia. Η εισαγωγή ενός ιδιωτικού ασύρματου δικτύου LTE/5G βιομηχανικού επιπέδου θα προσφέρει, σύμφωνα με τις εταιρείες, σημαντικές αυξήσεις στην αποδοτικότητα, την ασφάλεια των εργαζομένων και τις επιδόσεις χειρισμού τερματικών σταθμών, "μειώνοντας την πολυπλοκότητα της ροής του λιμένα".

Ο Matt Young, αντιπρόεδρος του τμήματος US Enterprise Sales της Nokia Cloud and Networking Services δήλωσε "Αυτές οι περιπτώσεις χρήσης καταδεικνύουν τα οφέλη του ιδιωτικού ασύρματου δικτύου σε ένα λιμάνι ή σε έναν διατροπικό τερματικό σταθμό". Το νέο δίκτυο θα παρέχει συνδεσιμότητα σε εσωτερικούς και εξωτερικούς χώρους σε όλες τις λειτουργίες και εργασίες του Terminal 5, τους γερανούς, τα φορτηγά και τους ανελκυστήρες, ενώ το Nokia DAC θα ενσωματωθεί επίσης σε ανθεκτικά tablet και smartphones για εφαρμογές επικοινωνίας και απογραφής.

5.4.2 Αερολιμένες

Τα ενδιαφερόμενα μέρη των αεροδρομίων αναπτύσσουν συχνά οράματα για ψηφιακούς τερματικούς σταθμούς και ψηφιοποίηση των λειτουργιών των αεροδρομίων. Οι νέες τεχνολογίες πληροφορικής και επικοινωνιών -Information and Communications Technologies (ICT)-, όπως η τεχνητή νοημοσύνη (AI), τα δίκτυα 5G και οι αισθητήρες του IoT, βρίσκονται στο αποκορύφωμα των διογκωμένων προσδοκιών σύμφωνα με τον τεχνολογικό κύκλο Hype Cycle της Gartner. Ο κύκλος "hype cycle" της Gartner είναι μια γραφική παρουσίαση που αναπτύχθηκε, χρησιμοποιείται και φέρει την επωνυμία της αμερικανικής εταιρείας ερευνών, παροχής συμβουλών και τεχνολογίας πληροφοριών Gartner, με έδρα το Stanford, για την παρουσίαση της ωριμότητας, της υιοθέτησης και της κοινωνικής εφαρμογής συγκεκριμένων τεχνολογιών, Εικόνα 5.2. Οι πρώτες υλοποιήσεις είναι παρούσες στους οδικούς χάρτες ψηφιοποίησης και στις επενδύσεις ICT στα πιο προηγμένα διεθνή αεροδρόμια ή/και στα έργα κατασκευής αεροδρομίων/τερματικών σταθμών σε όλο τον κόσμο.



Εικόνα 5.2: Hype Cycle της Gartner [7.20]

Τα σύγχρονα αεροδρόμια αγκαλιάζουν τα οφέλη της αυτοματοποίησης και των νέων τεχνολογιών για την επιχειρησιακή αποδοτικότητα, τη μείωση του κόστους συντήρησης, την ικανοποίηση των πελατών και τον προγνωστικό σχεδιασμό της χωρητικότητας. Ωστόσο, οι νέες τεχνολογίες φέρνουν μαζί τους και νέα πιθανά τρωτά σημεία. Ο Ευρωπαϊκός Οργανισμός Ασφάλειας της Αεροπορίας (EASA) εκτιμά ότι κατά μέσο όρο 1.000 επιθέσεις σημειώνονται κάθε μήνα σε συστήματα αερομεταφορών, αποτελώντας έτσι πραγματική απειλή για την ασφάλεια, την προστασία και τη φήμη των αεροδρομίων. Οι κίνδυνοι για την ασφάλεια στον κυβερνοχώρο εξελίσσονται γρήγορα και η ίδια η φύση των κυβερνοεπιθέσεων, που χαρακτηρίζεται από το χαμηλό κόστος τους, τις καθιστά εύκολα προσιτές σε τρομοκρατικές και εγκληματικές οργανώσεις.

Τα δίκτυα 5G θα διαδραματίσουν κεντρικό ρόλο στην επίτευξη του ψηφιακού μετασχηματισμού της οικονομίας και της κοινωνίας της ΕΕ. Πράγματι, τα δίκτυα 5G έχουν τη δυνατότητα να επιτρέψουν και να υποστηρίξουν ένα ευρύ φάσμα εφαρμογών και λει-

τουργιών, που θα επεκτείνονται πολύ πέρα από την παροχή υπηρεσιών κινητών επικοινωνιών μεταξύ τελικών χρηστών. Με τα παγκόσμια έσοδα από το 5G να εκτιμώνται σε 225 δισεκατομμύρια ευρώ το 2025, οι τεχνολογίες και οι υπηρεσίες 5G αποτελούν βασικό πλεονέκτημα για την ανταγωνιστικότητα της Ευρώπης στην παγκόσμια αγορά.

Τα δίκτυα 5G θα παρέχουν πρακτικά πανταχού παρούσα συνδεσιμότητα με εξαιρετικά υψηλό εύρος ζώνης και χαμηλή καθυστέρηση όχι μόνο σε μεμονωμένους χρήστες αλλά και σε συνδεδεμένα αντικείμενα. Χάρη σε αυτά τα τεχνικά χαρακτηριστικά, τα δίκτυα 5G αναμένεται να εξυπηρετήσουν ένα ευρύ φάσμα εφαρμογών και τομέων, κυρίως την αυτόνομη οδήγηση και τη συνδεσιμότητα αισθητήρων IoT. Στα αεροδρόμια, εκτός από τα ιδιωτικά δίκτυα κινητής τηλεφωνίας εντός των τερματικών σταθμών, το 5G θα υποστηρίξει την ευρυζωνική επιχειρησιακή συνδεσιμότητα στις περιοχές του προαυλίου και του διαδρόμου προσγείωσης. Το δυναμικό 5G θα μπορούσε επίσης να υποστηρίξει την αυτοματοποιημένη επίγεια εξυπηρέτηση αεροδρομίων και τις ρομποτικές εγκαταστάσεις του συστήματος διαχείρισης αποσκευών (BHS).

Από τεχνολογικής άποψης, τα δίκτυα 5G θα κάνουν χρήση ορισμένων νέων τεχνικών χαρακτηριστικών, σε σύγκριση με την τρέχουσα κατάσταση στα υφιστάμενα δίκτυα, όπως:

- Η μετάβαση στο λογισμικό και την εικονικοποίηση μέσω των τεχνολογιών "Software Defined Networks" (SDN) και "Network Functions Virtualization (NFV)".
- Το "Network slicing" θα καταστήσει δυνατή την υποστήριξη σε μεγάλο βαθμό του διαχωρισμού διαφορετικών επιπέδων υπηρεσιών στο ίδιο φυσικό δίκτυο.
- 'Mobile Edge Computing', το οποίο επιτρέπει στο δίκτυο να κατευθύνει την κυκλοφορία σε υπολογιστικούς πόρους και υπηρεσίες τρίτων που βρίσκονται κοντά στον τελικό χρήστη, εξασφαλίζοντας έτσι χαμηλούς χρόνους απόκρισης.

Τα προαναφερθέντα τεχνολογικά χαρακτηριστικά ορίζονται παρακάτω:

1. Η τεχνολογία δικτύωσης που καθορίζεται από το λογισμικό -ή Software-defined networking1 (SDN)- είναι μια προσέγγιση στη διαχείριση του δικτύου που επιτρέπει τη δυναμική, προγραμματικά αποδοτική διαμόρφωση του δικτύου με σκοπό τη βελτίωση της απόδοσης και της παρακολούθησης του δικτύου, καθιστώντας την περισσότερο σαν υπολογιστικό νέφος από την παραδοσιακή διαχείριση του δικτύου.

2. Η εικονικοποίηση λειτουργιών δικτύου (NFV) είναι μια έννοια αρχιτεκτονικής δικτύου που αξιοποιεί τις τεχνολογίες εικονικοποίησης της πληροφορικής για την εικονικοποίηση ολόκληρων κατηγοριών λειτουργιών κόμβων δικτύου σε δομικά στοιχεία που μπορούν να συνδεθούν ή να αλυσιδωθούν μεταξύ τους για τη δημιουργία και παροχή υπηρεσιών επικοινωνίας (NFV) -είναι μια έννοια αρχιτεκτονικής δικτύου που αξιοποιεί τις τεχνολογίες εικονικοποίησης της πληροφορικής για την εικονικοποίηση ολόκληρων κατηγοριών λειτουργιών κόμβων δικτύου σε δομικά στοιχεία που μπορούν να συνδεθούν ή να αλυσιδωθούν μεταξύ τους για τη δημιουργία και παροχή υπηρεσιών επικοινωνίας.
3. Το 5G network slicing είναι μια αρχιτεκτονική δικτύου που επιτρέπει την πολυπλεξία εικονικών και ανεξάρτητων λογικών δικτύων στην ίδια φυσική υποδομή δικτύου. Κάθε «φέτα» (slice) δικτύου είναι ένα απομονωμένο δίκτυο από άκρο σε άκρο, προσαρμοσμένο ώστε να ικανοποιεί ποικίλες απαιτήσεις που ζητούνται από μια συγκεκριμένη εφαρμογή.
4. Multi-access edge computing (MEC), ή πρώην γνωστό ως mobile edge computing, είναι μια ορισμένη από το ETSI (European Telecommunications Standards Institute ή Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων) έννοια αρχιτεκτονικής δικτύου που ενεργοποιεί τις δυνατότητες υπολογιστικού νέφους και ενός περιβάλλοντος υπηρεσιών πληροφορικής στην άκρη του κυψελοειδούς δικτύου και, γενικότερα, στην άκρη οποιουδήποτε δικτύου.

Αυτά τα νέα χαρακτηριστικά θα φέρουν πολλές νέες προκλήσεις στον τομέα της ασφάλειας. Ειδικότερα, θα δώσουν πρόσθετη έμφαση στην πολυπλοκότητα της αλυσίδας εφοδιασμού των τηλεπικοινωνιών στην ανάλυση της ασφάλειας, με διάφορους υφιστάμενους ή νέους φορείς, όπως οι ολοκληρωτές (integrators), οι πάροχοι υπηρεσιών ή οι πωλητές λογισμικού, να εμπλέκονται ακόμη περισσότερο στη διαμόρφωση και τη διαχείριση βασικών τμημάτων του δικτύου. Ταυτόχρονα, οι τεχνολογίες και τα πρότυπα 5G θα μπορούσαν να βελτιώσουν την ασφάλεια, σε σύγκριση με τις προηγούμενες γενιές δικτύων κινητής τηλεφωνίας (2/3/4G), λόγω διαφόρων νέων λειτουργιών ασφαλείας, όπως αυστηρότερες διαδικασίες ελέγχου ταυτότητας στη ραδιοδιεπαφή. Ωστόσο, αυτές οι νέες λειτουργίες ασφαλείας δεν θα ενεργοποιηθούν όλες εξ ορισμού στον εξοπλισμό του δικτύου και, ως εκ τούτου, η εφαρμογή τους θα εξαρτηθεί σε μεγάλο βαθμό από τον τρόπο με τον οποίο οι φορείς εκμετάλλευσης αναπτύσσουν και διαχειρίζονται τα δίκτυά τους.

Οι δύο κύριοι εμπλεκόμενοι φορείς έχουν ιδιαίτερη σημασία για την ασφάλεια στον κυβερνοχώρο των δικτύων 5G:

- Οι φορείς εκμετάλλευσης δικτύων κινητής τηλεφωνίας (MNO) έχουν κεντρικό, αποφασιστικό ρόλο που τους δίνει μόχλευση για τη συνολική ασφαλή λειτουργία των δικτύων τους.
- Από την άλλη πλευρά, οι κατασκευαστές τηλεπικοινωνιακού εξοπλισμού είναι υπεύθυνοι για την παροχή του λογισμικού και του υλικού που απαιτείται για τη λειτουργία των δικτύων.

Οι σύγχρονοι φορείς εκμετάλλευσης αεροδρομίων πιθανότατα θα αναθέσουν την υποδομή και τις επενδύσεις 5G σε MNOs και θα βασίζονται στα σχέδια ασφάλειας στον κυβερνοχώρο μέσω πιθανών ελέγχων και δοκιμών διείσδυσης. Στις περιπτώσεις όπου τα εσωτερικά συστήματα κατανεμημένων κεραιών (DAS) αποτελούν μέρος της υποδομής του δικτύου ICT του αεροδρομίου, οι αξιολογήσεις τρωτότητας και οι δοκιμές διείσδυσης θα πρέπει επίσης να περιλαμβάνονται στα σχέδια μετριασμού των κινδύνων στον κυβερνοχώρο των αεροδρομίων σύμφωνα με το πρόγραμμα ISO27001 ISMS.

5.5 Αλλάζοντας τις ζωές των ατόμων με αναπηρίες

5.5.1 Κατανόηση

Κατ' αρχάς, ας κατανοήσουμε τι χαρακτηρίζει νομικά ένα άτομο ως ανάπηρο. Σύμφωνα με τους κανόνες της Κοινωνικής Ασφάλισης, ένα άτομο χαρακτηρίζεται με ειδικές ανάγκες εάν δεν είναι πλέον σε θέση να κάνει την εργασία που έκανε πριν, εάν η Κοινωνική Ασφάλιση αποφασίσει ότι το άτομο δεν μπορεί να προσαρμοστεί σε άλλη εργασία λόγω ιατρικών συνθηκών, και εάν οι ειδικές του ανάγκες έχουν διαρκέσει ή αναμένεται να διαρκέσουν για ένα έτος ή να οδηγήσει στο θάνατο. Η Κοινωνική Ασφάλιση χρησιμοποιεί μια διαδικασία 5 βημάτων για να εκτιμήσει αν ένα άτομο πληροί αυτόν τον "αυστηρό ορισμό των ειδικών αναγκών".

Για παράδειγμα, το να κερδίζει κανείς περισσότερα από 1.000 ευρώ το μήνα ή η ικανότητα προσαρμογής σε άλλες δεξιότητες που θα μπορούσαν να του αποφέρουν απασχόληση αποκλείει γενικά ένα άτομο από τον ισχυρισμό της αναπηρίας. Από την άλλη πλευρά, οι "σοβαρές" παθήσεις που εμπίπτουν στον κατάλογο των ιατρικών παθήσεων της Διοίκησης Κοινωνικής Ασφάλισης ή η αδυναμία να κάνει κάποιος εργασία που έκανε πριν, μπορεί να ενισχύσει τον ισχυρισμό των ειδικών αναγκών του ατόμου. Τα άτομα με

ειδικές ανάγκες έρχονται συνεχώς αντιμέτωπα με εμπόδια. Ο Παγκόσμιος Οργανισμός Υγείας περιγράφει τα εμπόδια ως παράγοντες που περιορίζουν τη λειτουργικότητα. Αυτοί κυμαίνονται από φυσικά εμπόδια μέχρι φραγμούς συμπεριφοράς, από εμπόδια επικοινωνίας μέχρι φραγμούς πολιτικής και πολλά άλλα.

Παγκοσμίως, περίπου ένα δισεκατομμύριο άνθρωποι έχουν ειδικές ανάγκες και το 80% ζουν σε αναπτυσσόμενες χώρες, οι αναδυόμενες τεχνολογίες κινητής τηλεφωνίας θα μπορούσαν να βοηθήσουν τα άτομα με ειδικές ανάγκες να ζουν ανεξάρτητα και να συνεισφέρουν περισσότερο στον εργασιακό χώρο και να βελτιώσουν την ποιότητα ζωής τους στον αναπτυσσόμενο κόσμο. Ζούμε σε μια εποχή όπου ο αριθμός των συνδεδεμένων συσκευών αρχίζει να αυξάνεται. Έτσι, η ύπαρξη ενός ασύρματου συστήματος που μπορεί να διευκολύνει την ανταλλαγή δεδομένων μεταξύ αυτών των διαφορετικών πλατφορμών είναι απαραίτητη για τη μελλοντική τους λειτουργία, αλλά και για τις συσκευές για άτομα με ειδικές ανάγκες.

5.5.2 Κινητικότητα

Η "αναζήτηση διαδρομής" για τα άτομα με ειδικές ανάγκες, η μετακίνηση και η πλοήγηση με μεγαλύτερη ανεξαρτησία είναι ένας τομέας όπου το 5G θα τους ωφελήσει. Οι άνθρωποι χωρίς όραση χρησιμοποιούν πλέον ένα λευκό μπαστούνι ή ένα ζώο εξυπηρέτησης για να μετακινηθούν. Μπορούν να κινούνται ανεξάρτητα μέσω των αναδυόμενων τεχνολογιών κινητής τηλεφωνίας. Η πιθανή ύπαρξη έξυπνων γυαλιών συνδεδεμένων με 5G σε συνδυασμό με ένα smartphone, τα οποία θα τους δίνουν τη δύναμη της τεχνητής νοημοσύνης και θα παρέχουν ηχητική ανατροφοδότηση σε πραγματικό χρόνο για να το βοηθήσουν να πλοηγηθεί σε ένα κατάστημα ή μια πόλη ανεξάρτητα. Με ένα δίκτυο υψηλής ταχύτητας, αυτές οι λύσεις που βασίζονται σε δεδομένα θα οδηγήσουν μόνο σε μεγαλύτερη ανεξαρτησία και αποτελεσματικότητα για τα άτομα με ειδικές ανάγκες. Οι νέες εξελίξεις, όπως η αναγνώριση προσώπου, θα τους λένε για παράδειγμα ποιος πλησιάζει, τα δρομολόγια των λεωφορείων και των τρένων, τα τρόφιμα στα ράφια του καταστήματος που αναγνωρίζονται.

Άρθρο του Ομίλου Thales παρουσιάζει λεπτομερώς μερικές τεχνολογικές εξελίξεις που βασίζονται στο IoT και βοηθούν τα άτομα με ειδικές ανάγκες να ξεπεράσουν τα προβλήματα κινητικότητας. Το Crosswalk -αποτελεί βοηθητική εφαρμογή με έδρα τις Κάτω Χώρες- μπορεί να μεταφορτωθεί σε smartphones, επιτρέπει στους πεζούς με ειδικές ανάγκες να ειδοποιούν τα φανάρια και να ζητούν επιπλέον χρόνο για τη διέλευση. Ο

χρήστης μπορεί να επιλέξει μεταξύ τεσσάρων ειδών ρυθμίσεων ανάλογα με την κινητικότητά του. Αυτό το προϊόν IoT επιδεικνύει εξαιρετική διαλειτουργικότητα, καθώς αλληλοεπιδρά ταυτόχρονα με το GPS και το λογισμικό των φωτεινών σηματοδοτών.

Οι καινοτόμες νέες εξελίξεις στον τομέα αυτό περιλαμβάνουν τις έξυπνες σόλες από την Ducere Technologies, μια ένθετη σόλα που χρησιμοποιεί δονήσεις για να διευκολύνει την πλοήγηση. Άλλες εταιρείες πειραματίζονται επίσης με νέες λύσεις, όπως φορητές συσκευές που λειτουργούν σαν ραντάρ και τεχνολογίες οστικής αγωγιμότητας. Αυτές οι εξελίξεις είναι χρήσιμες για την υπέρβαση των φυσικών εμποδίων που αντιμετωπίζουν τα άτομα με ειδικές ανάγκες, όπως οι σκάλες που μπορεί να εμποδίζουν κάποιον να εισέλθει σε ένα κτίριο, ή τα κράσπεδα που διαφορετικά θα μπορούσαν να εμποδίσουν ένα άτομο με ειδικές ανάγκες να χρησιμοποιήσει το πεζοδρόμιο.

Εξελίξεις όπως αυτές βοηθούν στην άρση των εμποδίων στις μεταφορές που αντιμετωπίζουν τα άτομα με ειδικές ανάγκες, επιτρέποντάς τους να φτάσουν σε κόμβους δημόσιων μεταφορών και καθιστώντας την κινητικότητα πιο προσιτή. Ακόμη, οι εξελίξεις που υποστηρίζονται από το IoT όπως αυτή επιτρέπουν στα άτομα με ειδικές ανάγκες να ξεπεράσουν προσωρινά την τρέχουσα έλλειψη προσαρμοστικών και βοηθητικών υποδομών και πολιτικής, παρέχοντας στα άτομα μια βιώσιμη εναλλακτική λύση.

5.5.3 Ακοή

Η καθυστέρηση αποτελεί πρόβλημα για τα άτομα χωρίς ακοή και το 5G θα βοηθήσει σε αυτό το πρόβλημα. Στις μέρες μας, τα άτομα χωρίς ακοή χρησιμοποιούν τη νοηματική γλώσσα για να επικοινωνήσουν με τους άλλους, μέσω των χειρονομιών και των εκφράσεων του προσώπου τους για να επικοινωνήσουν πολλά νοήματα. Όταν αυτό πραγματοποιείται εξ αποστάσεως, μπορεί να αποτελέσει πρόκληση κατά τη χρήση εφαρμογών βίντεο-συνομιλίας μέσω smartphone, λόγω ορισμένων περιορισμών δεδομένων ή υποδομών για τη μετάδοση δεδομένων στις αναπτυσσόμενες χώρες. Η καθυστέρηση είναι ο δολοφόνος αυτού του φαινομένου. Με το 5G, τα προβλήματα καθυστέρησης ουσιαστικά εξαφανίζονται. Δεν αφορά μόνο τους τα άτομα χωρίς ακοή. Οι ακούοντες βασίζονται σε διερμηνέα, οπότε το 5G θα μπορούσε να διευκολύνει την ευρύτερη ένταξη των ανθρώπων που βασίζονται στη SL (Sing Language) ως γλώσσα τους και να τους επιτρέψει να συμμετέχουν πιο απρόσκοπτα στην κοινωνία μας.

Οι υπηρεσίες 5G βοηθούν επίσης τα άτομα με αναπηρία να ζουν ανεξάρτητα με ένα πιο συνδεδεμένο έξυπνο σπίτι, χρησιμοποιώντας ένα smartphone για τον έλεγχο του περιβάλλοντος, όπως για την ενεργοποίηση και απενεργοποίηση του φωτός, τον έλεγχο της θερμοκρασίας, τη λειτουργία μιας πόρτας κ.λπ. Με αυτά τα δίκτυα υψηλής ταχύτητας, οι υπηρεσίες αυτές θα βελτιωθούν. Οι φορητές συσκευές θα βελτιώσουν τη σωματική υγεία των ατόμων με αναπηρία. Επίσης, τα φορητά κινητά GPS, συνδεδεμένα με smartphone, βοηθούν τους γονείς να εντοπίζουν τους γιους ή τις κόρες με νοητική αναπηρία.

Η ποιότητα ζωής των ατόμων με ειδικές ανάγκες θα βελτιωθεί με τις αναδυόμενες τεχνολογίες:

- Θα ενημερώνονται και θα επικοινωνούν καλύτερα με τον κόσμο.
- Θα ενισχύσει την πρόσβαση στην εκπαίδευση
- Θα παρέχει την ευκαιρία να ζουν και να εργάζονται ανεξάρτητα.

5.5.4 Όραση

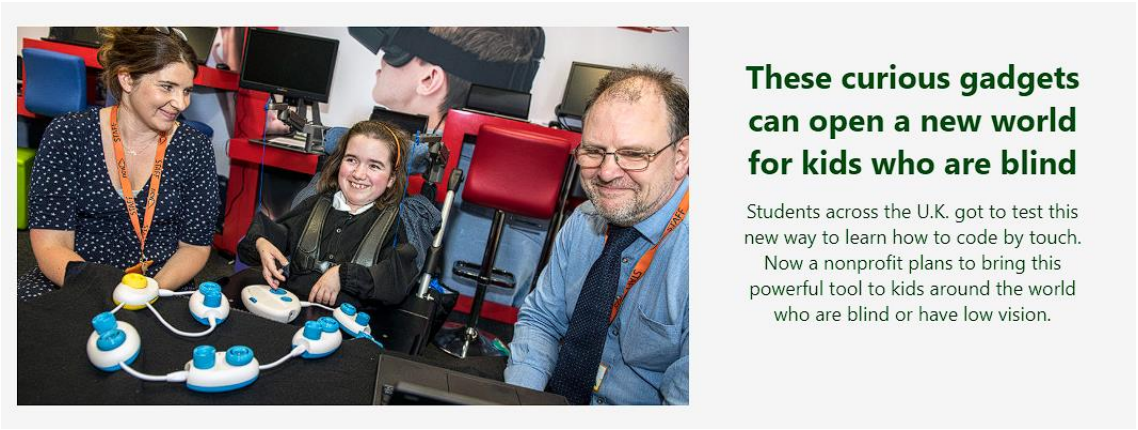
Ο συνδυασμός του IoT και της τεχνητής νοημοσύνης μπορεί να βοηθήσει τα άτομα με ειδικές ανάγκες να διαβάζουν και να κατανοούν καλύτερα το περιβάλλον τους. Αυτό είναι ιδιαίτερα χρήσιμο για όσους έχουν προβλήματα όρασης. Σκεφτείτε την εφαρμογή Seeing AI της Microsoft, η οποία έχει σχεδιαστεί για άτομα με προβλήματα όρασης ώστε να μαθαίνουν για το άμεσο περιβάλλον τους. Η προγραμματισμένη με τεχνητή νοημοσύνη εφαρμογή μπορεί να κατευθύνει τους περιπατητές μακριά από πολυσύχναστες διασταυρώσεις και μπορεί ακόμη και να ενημερώνει τους ανθρώπους για το τι εκφράζουν οι άλλοι γύρω τους με το πρόσωπο.

Μια παρόμοια τεχνολογία που ονομάζεται Cloud Vision API έχει εισαχθεί από την Google για προγραμματιστές για τη δημιουργία εφαρμογών και συσκευών που διαθέτουν χαρακτηριστικά αναγνώρισης και ταξινόμησης. Η τεχνητή "όραση" της εφαρμογής θα βοηθήσει σημαντικά τους χρήστες να κατανοήσουν και να συσχετίσουν τις φυσικές καταστάσεις στο περιβάλλον τους. Η ικανότητα καλύτερης ανάγνωσης του περιβάλλοντος μπορεί να βοηθήσει τα άτομα με ειδικές ανάγκες να ξεπεράσουν τα πολλά εμπόδια επικοινωνίας που αντιμετωπίζουν. Αυτές οι εξελίξεις προωθούν την καλύτερη κατανόηση και μπορούν να είναι πολύ χρήσιμες για τα άτομα με οπτικές, ακουστικές και γνωστικές ειδικές ανάγκες.

Στο Worcester του Ηνωμένου Βασίλειου μια ομάδα μαθητών έχει συγκεντρωθεί στην αίθουσα πληροφορικής του New College Worcester για να επιδείξει τις ικανότητές της στον προγραμματισμό. Αλλά αντί να σκαλίζουν τις οθόνες των tablet ή να πληκτρολογούν σε φορητούς υπολογιστές, ~~αυτοί~~ οι μαθητές παίρνουν πολύχρωμες πλαστικές κάψουλες, τις συνδέουν μεταξύ τους με χοντρά λευκά καλώδια και στη συνέχεια ρυθμίζουν τα κουμπιά και τα κουμπιά της κάψουλας. Αυτά τα φυσικά εξαρτήματα θα χρησιμοποιηθούν για τη δημιουργία προγραμμάτων υπολογιστών που μπορούν να αφηγούνται ιστορίες, να κάνουν μουσική και ακόμη και να λένε αστεία.

Οι μαθητές του New College του Worcester είναι όλοι άτομα χωρίς ή με χαμηλή όραση και ανήκουν σε μια ομάδα μαθητών από όλο το Ηνωμένο Βασίλειο που πέρασαν την προηγούμενη σχολική χρονιά δοκιμάζοντας το Project Torino, ένα ερευνητικό πρόγραμμα που οδήγησε στην ανάπτυξη ενός νέου προϊόντος που ονομάζεται Code Jumper (Εικόνα 5.3). Πρόκειται για μια φυσική γλώσσα προγραμματισμού που έχει σχεδιαστεί για να συμπεριλαμβάνει παιδιά με όλα τα επίπεδα όρασης.

"Αυτό που μου αρέσει στο Project Torino είναι ότι μπορείς πραγματικά να αγγίξεις, με φυσικό τρόπο, το πρόγραμμα", δήλωσε η Βικτόρια, 14 ετών και μαθήτρια στο σχολείο, το οποίο εξυπηρετεί περίπου 80 μαθητές.



Εικόνα 5.3: Χρήση εργαλείου Code Jumper από τους μαθητές [7.21]

Η Microsoft ανακοίνωσε ότι σχεδιάζει να μεταφέρει την έρευνα και την τεχνολογία πίσω από το Code Jumper στο American Printing House for the Blind (APH), ένα μη κερδοσκοπικό ίδρυμα με έδρα το Louisville του Kentucky, το οποίο δημιουργεί και διανέμει προϊόντα και υπηρεσίες για χωρίς ή με χαμηλή όραση. Τα επόμενα πέντε χρόνια, το APH σχεδιάζει να προσφέρει το Code Jumper και το σχετικό πρόγραμμα σπουδών σε μαθητές σε όλο τον κόσμο, με στόχο μαθητές ηλικίας 7 έως 11 ετών.

5.5.5 Απήχηση του IoT και 5G στις ζωές των ανθρώπων

Τα άτομα με αναπηρία υποφέρουν σε μεγάλο βαθμό εξαιτίας των πολλών φυσικών και κοινωνικών εμποδίων που αντιμετωπίζουν. Από την εγκατάλειψη του σχολείου και την αυξημένη βία κατά των παιδιών μέχρι την άνιση απασχόληση και το άνισο εισόδημα, το στίγμα που συνδέεται με τις ειδικές ανάγκες εξακολουθεί να εκδηλώνεται μέσω του κραυγαλέου χάσματος στις διαθέσιμες ευκαιρίες για τα άτομα με ειδικές ανάγκες. Σήμερα, η ψηφιακή εποχή και το IoT μαζί με το 5G προσπαθούν να καταρρίψουν ορισμένα από αυτά τα εμπόδια.

Το IoT με τη μορφή έξυπνων συσκευών είναι πολύ χρήσιμο για να βοηθήσει τα άτομα με ειδικές ανάγκες να γίνουν πιο αυτόνομα. Τα έξυπνα σπίτια, συμπεριλαμβανομένων των συνδεδεμένων ηχείων, ψυγείων, φούρνων και θερμοστατών, βοηθούν τα άτομα με ειδικές ανάγκες να έχουν μεγαλύτερο έλεγχο των καθημερινών τους ενεργειών και μπορούν να προγραμματιστούν ώστε να ανταποκρίνονται στις ανάγκες ενός συγκεκριμένου χρήστη. Η τεχνολογία IoT προβλέπει επίσης wearables όπως τα smartwatches που μεταφράζουν περιεχόμενο, συμπεριλαμβανομένων των emails και των κειμένων, σε γραφή Braille ή διαβάζουν το ίδιο φωναχτά. Βελτιώνοντας την αυτονομία, το IoT βοηθά τα άτομα με ειδικές ανάγκες να ξεπεράσουν τόσο τα κοινωνικά εμπόδια όσο και τους φραγμούς συμπεριφοράς και τους επιτρέπει να βελτιώσουν τη γενική ποιότητα ζωής τους μέσω της παροχής προσβάσιμου και χρήσιμου εξοπλισμού. Με τον καιρό, η ελπίδα είναι ότι η τεχνολογία θα βοηθήσει στην αντιμετώπιση μεγαλύτερου μέρους των προκλήσεων που αντιμετωπίζουν τα άτομα με αναπηρία, με αποτέλεσμα τη βελτίωση της αυτονομίας και την παροχή ίσων ευκαιριών και πρόσβασης.

6 Αδυναμίες στην ασφάλεια

Οι ευπάθειες είναι ελαττώματα σε ένα σύστημα υπολογιστή που αποδυναμώνουν τη συνολική ασφάλεια της συσκευής / συστήματος. Τα τρωτά σημεία μπορεί να είναι αδυναμίες είτε στο ίδιο το υλικό είτε στο λογισμικό που εκτελείται στο υλικό. Οι ευπάθειες μπορούν να αξιοποιηθούν από έναν απειλητικό παράγοντα, όπως ένας εισβολέας, για να υπερβεί τα όρια προνομίων (δηλαδή να εκτελέσει μη εξουσιοδοτημένες ενέργειες) σε ένα σύστημα υπολογιστή. Για να εκμεταλλευτεί μια ευπάθεια, ο επιτιθέμενος πρέπει να διαθέτει τουλάχιστον ένα εφαρμόσιμο εργαλείο ή τεχνική που μπορεί να συνδεθεί με μια αδυναμία του συστήματος. Σε αυτό το πλαίσιο, οι ευπάθειες είναι επίσης γνωστές ως επιφάνεια επίθεσης. Η διαχείριση των τρωτών σημείων είναι μια κυκλική πρακτική που ποικίλλει στη θεωρία αλλά περιέχει κοινές διαδικασίες που περιλαμβάνουν: ανακάλυψη όλων των περιουσιακών στοιχείων, ιεράρχηση των περιουσιακών στοιχείων (ή assets), αξιολόγηση ή εκτέλεση πλήρους σάρωσης τρωτών σημείων, αναφορά των αποτελεσμάτων, αποκατάσταση των τρωτών σημείων, επαλήθευση της αποκατάστασης και επανάληψη. Η πρακτική αυτή αναφέρεται γενικά σε ευπάθειες λογισμικού σε υπολογιστικά συστήματα. Η ευέλικτη διαχείριση τρωτότητας αναφέρεται στην πρόληψη επιθέσεων με τον εντοπισμό όλων των τρωτών σημείων το συντομότερο δυνατό.

6.1 Ευπάθειες στο IoT

Οι συσκευές IoT μπορεί να φαίνονται πολύ μικρές ή εξειδικευμένες για να αποτελέσουν κίνδυνο για τις επιχειρήσεις, αλλά αυτό δεν θα μπορούσε να απέχει περισσότερο από την αλήθεια. Οι συσκευές IoT είναι υπολογιστές γενικής χρήσης που συνδέονται στο δίκτυο και μπορούν να παραβιαστούν και να υποκλαπούν από εγκληματίες, οδηγώντας σε προβλήματα πέρα από την ασφάλεια του IoT. Ακόμη και αν ένας οργανισμός έχει κλειδώσει τις φυσικές συσκευές και έχει θέσει σε ισχύ βασικά μέτρα ασφαλείας IoT, τα συστήματα παραμένουν ευάλωτα. Πολλοί εμπειρογνώμονες κυβερνοασφάλειας ξεχνούν την ασφάλεια των εφαρμογών IoT κατά το σχεδιασμό μιας στρατηγικής ασφάλειας. Η Gartner (εταιρεία που αναφέρθηκε στο κεφάλαιο 5.4.2) εκτιμά ότι μέχρι το 2025 θα υπάρχουν περίπου 25 δισεκατομμύρια συνδέσεις IoT, γεγονός που καθιστά κάθε αισθητήρα IoT, τελικό σημείο, σύνδεση, επίπεδο δικτύου και UI μια ευπάθεια για τις επιχειρήσεις που τα

χρησιμοποιούν. Η ασφάλεια των εφαρμογών IoT παρουσιάζει μια τεράστια περιοχή ευπάθειας και μια περιοχή στην οποία οι οργανισμοί θα πρέπει να εξετάσουν το ενδεχόμενο να κάνουν ίσες επενδύσεις από εδώ και στο εξής. Λαμβάνοντας υπόψιν λοιπόν τα παραπάνω, θα παρατεθούν μερικές βασικές αδυναμίες από τις οποίες απαρτίζονται τα περισσότερα IoT συστήματα σήμερα.

- Μη κρυπτογραφημένη αποθήκευση δεδομένων

Οι συσκευές IoT συλλέγουν τεράστιο όγκο πολύτιμων δεδομένων καθ' όλη τη διάρκεια της ημέρας, μεγάλο μέρος των οποίων αποθηκεύεται στο cloud. Τα δεδομένα αυτά μπορούν να καταστήσουν τις συσκευές IoT στόχο για χάκερς (hackers) και άλλους εγκληματίες του κυβερνοχώρου, γι' αυτό είναι απαραίτητο να αποθηκεύονται με ασφάλεια. Είναι επίσης πολύ σημαντικό κάθε φορά που μεταφέρονται δεδομένα μεταξύ συσκευών να γίνεται με ασφάλεια, ιδανικά με κρυπτογραφημένη σύνδεση. Δυστυχώς, πολλές συσκευές IoT δεν διαθέτουν ακόμη αξιόπιστα τείχη προστασίας και άλλα χαρακτηριστικά ασφαλείας, γεγονός που αφήνει τα δεδομένα αυτά πολύ ευάλωτα. Υπάρχουν επίσης ορισμένα σενάρια στα οποία είναι δύσκολο να εξασφαλιστεί μια ασφαλής σύνδεση μεταξύ των συσκευών - για παράδειγμα, η μεταφορά δεδομένων μεταξύ ενός smartphone και άλλων συσκευών γίνεται συχνά μέσω δημόσιων δικτύων WiFi. Όταν τα δεδομένα δεν αποθηκεύονται σωστά, σας αφήνουν ευάλωτους σε κακόβουλο λογισμικό. Το κακόβουλο λογισμικό μπορεί να επηρεάσει τον τρόπο λειτουργίας των συσκευών σας και, στη χειρότερη περίπτωση, μπορεί ακόμη και να σας αποκλείσει από τις συσκευές σας και να κρατήσει τα δεδομένα σας για λύτρα.

- Μη ασφαλείς οικονομικές πληροφορίες

Ορισμένες συσκευές IoT έχουν πρόσβαση στις οικονομικές πληροφορίες των χρηστών τους. Όταν αυτές οι συσκευές έχουν πρόσβαση σε πράγματα όπως οι πληροφορίες της πιστωτικής σας κάρτας ή οι τραπεζικές σας πληροφορίες, γίνονται γρήγορα στόχος για τους hackers. Αυτό είναι ένα ιδιαίτερα ανησυχητικό πρόβλημα για τις χρηματοπιστωτικές εταιρείες που χρησιμοποιούν συσκευές IoT στην εργασία τους. Καθώς η τεχνολογία IoT και AI επεκτείνεται, δύναται η διαχείριση πολλών διαφορετικών πτυχών μιας επιχείρησής με χρήση αυτών χρησιμοποιώντας αυτά των εργαλείων. Ωστόσο, μπορεί να θέσει σε κίνδυνο τόσο την επιχείρησή όσο και τους πελάτες, εάν αυτές οι συσκευές έχουν πρόσβαση σε μη ασφαλείς χρηματοοικονομικές πληροφορίες.

- Πρόσβαση σε φυσική περιουσία

Ένας άλλος τεράστιος κίνδυνος ασφαλείας που πρέπει να ληφθεί υπόψιν είναι το γεγονός ότι οι συσκευές IoT συχνά συνδέονται με κάποιο τρόπο με φυσική περιουσία. Για παράδειγμα, πολλά σπίτια, επιχειρήσεις και αυτοκίνητα διαθέτουν πλέον κλειδαριές και συστήματα ασφαλείας που είναι συνδεδεμένα με το IoT. Αυτό σημαίνει ότι αν κάποιος παραβιάσει τη συσκευή, θα μπορούσε να έχει πρόσβαση στη φυσική σας περιουσία και να απειλήσει ακόμη και τη φυσική σας ασφάλεια.

- Αδύναμοι κωδικοί πρόσβασης και επαλήθευση ταυτότητας

Ένας ισχυρός κωδικός πρόσβασης είναι απαραίτητος για την προστασία των συσκευών σας. Δυστυχώς, πολλές συσκευές IoT δεν προστατεύονται με κωδικό πρόσβασης. Ακόμη και με συσκευές που προστατεύονται με κωδικό πρόσβασης, πολλοί χρήστες επιλέγουν επιλογές που είναι πολύ απλές και εύκολα προβλέψιμες. Αυτό αφήνει τις συσκευές ~~σας~~ IoT πολύ ευάλωτες στους hacker. Εκτός από τους κωδικούς πρόσβασης, πολλές συσκευές IoT χρησιμοποιούν και άλλες μορφές επαλήθευσης ταυτότητας. Για παράδειγμα, πολλές συσκευές χρησιμοποιούν βιομετρική επαλήθευση όπως δακτυλικά αποτυπώματα ή ακόμη και αναγνώριση προσώπου ως μορφή επαλήθευσης ταυτότητας. Ενώ αυτό μπορεί να είναι πιο ασφαλές από τη χρήση ενός κωδικού πρόσβασης, είναι σημαντικό να βεβαιωθείτε ότι αυτά τα δεδομένα επαλήθευσης ταυτότητας αποθηκεύονται και διαχειρίζονται με ασφάλεια.

- Δίκτυα botnet και κακόβουλες συσκευές IoT

Το IoT επιτρέπει στις ηλεκτρονικές συσκευές να συνδέονται και να μιλούν μεταξύ τους, χωρίς όμως να δημιουργούνται όλες αυτές οι συσκευές με καλές προθέσεις. Οι εγκληματίες του κυβερνοχώρου μπορούν να πάρουν υπάρχουσες συσκευές IoT και να τις χρησιμοποιήσουν για να διεισδύσουν σε ασφαλή δίκτυα. Οι συσκευές IoT είναι επίσης ιδιαίτερα ευάλωτες σε επιθέσεις botnet. Τα botnets είναι δίκτυα συσκευών που χρησιμοποιούνται για την εκτέλεση κακόβουλων bots και τη μεταφορά κακόβουλου λογισμικού. Τα botnets μπορούν να διεισδύσουν σε δίκτυα IoT για να τοποθετήσουν ransomware, spyware ή άλλες μορφές κακόβουλου λογισμικού σε ασφαλείς συσκευές, θέτοντας σε κίνδυνο την οικονομική και προσωπική σας ασφάλεια.

Στον τομέα της ιατροφαρμακευτικής περίθαλψης συγκεκριμένα, οι κρίσιμοι κίνδυνοι για τις ιατρικές συσκευές εξακολουθούν να αφήνουν τα νοσοκομεία και τους ασθενείς τους ευάλωτους σε επιθέσεις στον κυβερνοχώρο και σε ζητήματα ασφάλειας δεδομένων. Παρά το γεγονός ότι οι επενδύσεις των νοσοκομείων στον τομέα της κυβερνοασφάλειας φτάνουν σε υψηλά επίπεδα, οι απειλές ασφαλείας που σχετίζονται με το IoMT (Internet of Medical Things) και τις συσκευές IoT επιτρέπουν επιθέσεις ransomware και άλλες επιθέσεις στον κυβερνοχώρο με πρωτοφανή ρυθμό. Βασισμένη σε δεδομένα από εκατομμύρια συνδεδεμένες συσκευές σε εκατοντάδες νοσοκομεία στις ΗΠΑ και σε όλο τον κόσμο, η ερευνητική έκθεση της Cynerio "State of Healthcare IoT Device Security 2022" παρέχει αριθμούς σχετικά με τις απειλές που θέτουν σε κίνδυνο την ασφάλεια των ασθενών και τα δεδομένα και τι πρέπει να γίνει για αυτές. Μεταξύ των ευρημάτων της έκθεσης είναι και τα κάτωθι αναφερόμενα :

- Πάνω από το 50% των συνδεδεμένων συσκευών σε ένα τυπικό νοσοκομείο παρουσιάζουν κρίσιμους κινδύνους.
- Σχεδόν τα 3/4 των αντλιών ενδοφλέβιας χορήγησης έχουν τρωτά σημεία που θα μπορούσαν να απειλήσουν την ασφάλεια των ασθενών εάν αξιοποιηθούν.
- Πάνω από το 50% των συσκευών στα ογκολογικά, φαρμακολογικά και εργαστηριακά τμήματα λειτουργούν με παλιές εκδόσεις των Windows οι οποίες δεν ενημερώνονται πλέον.
- Ενώ ευπάθειες όπως το Urgent11 και το Ripple20 γίνονται πρωτοσέλιδα, ο πιο συνηθισμένος κίνδυνος για τις συσκευές παραμένει ο ανασφαλής κωδικός πρόσβασης.
- Η αποτελεσματική τμηματοποίηση (segmentation) του δικτύου αντιμετωπίζει πάνω από το 90% των κρίσιμων κινδύνων για τις συσκευές.

Αυτές είναι μόνο μερικές από τις πολλαπλές αδυναμίες που οι ειδικοί καλούνται να αντιμετωπίσουν στον τομέα της ιατροφαρμακευτικής περίθαλψης. Πέρα όμως από τις κακόβουλες επιθέσεις και αδυναμίες, θα πρέπει και εμείς να προσέξουμε και να αντιμετωπίσουμε σωστά αυτές τις συσκευές. Μερικές από τις ερωτήσεις που θα ήταν ορθό να θέσουμε όταν ασχολούμαστε με συσκευές IoT είναι:

Έχει ελεγχθεί το λογισμικό για κοινές ευπάθειες;

Έχουν αφαιρεθεί όλες οι περιττές υπηρεσίες και στοιχεία από το λογισμικό;

Είναι γνωστές ποιες βιβλιοθήκες τρίτων περιλαμβάνονται στο λογισμικό μας;

Παρακολουθούνται αυτές τις βιβλιοθήκες για γνωστές ευπάθειες;

Η ραγδαία ανάπτυξη του IoT αναδεικνύεται σε περαιτέρω πρόκληση για την ασφάλεια. Σύμφωνα με πρόσφατη έρευνα της Wi-SUN Alliance, μόνο ο τομέας των υπηρεσιών κοινής ωφέλειας IoT θα μπορούσε να φτάσει τα 15 δισεκατομμύρια δολάρια μέχρι το 2024. Αυτό υποδεικνύει πως τα συστήματα και τα πρωτόκολλά ασφαλείας θα πρέπει να αναβαθμιστούν στα υπάρχοντα δεδομένα ώστε οι παγκόσμια αγορά να μην κινδυνέψει από κάθε είδους κακόβουλη ενέργεια.

Οι εταιρείες πετρελαίου και φυσικού αερίου, οι οποίες έχουν μακρά ιστορία στη χρήση SCADA (supervisory control and data acquisition, κατηγορία εφαρμογών λογισμικού για τον έλεγχο βιομηχανικών διεργασιών, που συνίσταται στη συλλογή δεδομένων σε πραγματικό χρόνο από απομακρυσμένες τοποθεσίες με σκοπό τον έλεγχο του εξοπλισμού και των συνθηκών) και βιομηχανικών συστημάτων ελέγχου (ICS, industrial control systems) για την αύξηση της αποδοτικότητας, είναι οι πιο πρόθυμες να προσθέσουν το IoT σε αυτό το μείγμα, με το 88% να το θεωρεί προτεραιότητα. Οι επιχειρήσεις κοινής ωφέλειας δεν βρίσκονται πολύ πίσω, με τα τρία τέταρτα όλων των επιχειρήσεων να επενδύουν στο IoT, σύμφωνα με την έρευνα της Wi-SUN. Ο Phil Beecher, πρόεδρος της Wi-SUN Alliance αναφέρει: "Ένας λόγος για το αυξανόμενο ενδιαφέρον για το IoT είναι το γεγονός ότι παίζει σε διάφορους άλλους βασικούς τομείς, όπως η αυτοματοποίηση της πληροφορικής, η ανάλυση μεγάλων δεδομένων και η οργανωτική συνδεσιμότητα". Επιπροσθέτως, τα σημερινά συνδεδεμένα ενεργειακά συστήματα διαφέρουν από εκείνα του παρελθόντος, τα οποία ιστορικά ήταν σε ξεχωριστά δίκτυα: "Έπρεπε να είσαι φυσικά εκεί για να το χακάρεις", αναφέρει ο Ken Munro, εταίρος και ιδρυτής της εταιρείας ασφάλειας διείσδυσης Pen Test Partners.

Ο Karl Lankford, ανώτερος μηχανικός λύσεων στην εταιρεία Bomgar, που ειδικεύεται στην απομακρυσμένη πρόσβαση αναφέρει «Όταν οι λύσεις και οι διαδικασίες IoT τοποθετούνται πάνω σε παλαιά συστήματα, δημιουργείται μια φιλόξενη προοπτική για χάκερς και εχθρικούς παράγοντες». Ο Lankford επισημαίνει ότι «πολλά νέα προϊόντα τίθενται γρήγορα σε χρήση από τους κατασκευαστές, οι οποίοι επιθυμούν να εκμεταλλευτούν τις «αποδοτικότητες» εξοικονόμησης κόστους που μπορεί να προσφέρει το βιομηχανικό διαδίκτυο των πραγμάτων (IIoT, Industrial Internet of Things)». Ο ίδιος προειδοποιεί: «Στη βιασύνη να γίνουν όλα διαδικτυακά, η ασφάλεια μπορεί μερικές φορές να παραβλέπεται και οι επιχειρήσεις πρέπει να διασφαλίσουν ότι κανένας δεν δημιουργεί ή δεν ανοίγει μια κερκόπορτα στο δίκτυο».

6.2 Ευπάθειες στο δίκτυο 5G

Βρισκόμαστε στο μεταίχμιο ενός από τα μεγαλύτερα επιτεύγματα στην ιστορία της τεχνολογίας, το οποίο θα επηρεάσει όλους τους κλάδους, τις επιχειρήσεις, τους καταναλωτές και τους ιδιώτες σε κάθε πτυχή της ψηφιακής και κινητής ικανότητας. Η ανάπτυξη του 5G, εισάγει έναν πλήρη μετασχηματισμό των τηλεπικοινωνιακών δικτύων όπως τα γνωρίζουμε και ανοίγει ένα τεράστιο φάσμα νέων ευκαιριών, υπηρεσιών και δυνατοτήτων. Αυτές οι εξελίξεις παρέχουν συνδεσιμότητα για δισεκατομμύρια χρήστες και συσκευές, επιτρέποντας νέες εφαρμογές που θα προωθήσουν την καινοτομία, νέες αγορές και οικονομική ανάπτυξη σε όλο τον κόσμο. Είναι εκπληκτικό ότι αυτές οι νέες υπηρεσίες προβλέπεται να δημιουργήσουν έσοδα της τάξης ολόκληρης της οικονομίας της Ινδίας. Τα άκρα του δικτύου 5G έχουν σχεδιαστεί για να υποστηρίζουν διάφορες περιπτώσεις χρήσης που θα αποδειχθούν εξαιρετικά σημαντικές για τους οργανισμούς σε όλους τους τομείς, όπως η ανάλυση βίντεο, οι υπηρεσίες εντοπισμού θέσης, IoT, η επαυξημένη πραγματικότητα (AR), η βελτιστοποιημένη διανομή τοπικού περιεχομένου και πολλά άλλα.

Σε αντίθεση με το 3G και το 4G, είναι ενδιαφέρον να σημειωθεί ότι το 5G δεν αναπτύχθηκε αρχικά για να αποτελέσει μια παγκόσμια επαναστατική τεχνολογία. Οι ερευνητές πίστευαν αρχικά ότι το 5G θα εφαρμοζόταν μόνο για ορισμένες περιπτώσεις χρήσης και συγκεκριμένες κάθετες αγορές. Με την πάροδο του χρόνου, κατέστη σαφές ότι η οικονομία του 5G θα μπορούσε να αλλάξει εντελώς τις συνθήκες για όλους και κάθε επιχείρηση, λόγω των υποσχόμενων ταχύτερων ταχυτήτων, του μεγαλύτερου εύρους ζώνης και της βελτιστοποιημένης κινητικότητας. Είναι καλά τεκμηριωμένο ότι το 5G έρχεται με πολλά υποσχόμενες εξελίξεις μεγαλύτερων ταχυτήτων, υψηλότερου εύρους ζώνης, βελτιωμένης συνδεσιμότητας και χαμηλότερης καθυστέρησης, ενώ παράλληλα θα διαχειρίζεται εκατομμύρια έως δισεκατομμύρια συσκευές. Ωστόσο, μαζί με αυτά τα πλεονεκτήματα, το 5G εισάγει επίσης νέες προκλήσεις στον τομέα της ασφάλειας. Είτε πρόκειται για ένα σχολείο, μια παραγωγική μονάδα, έναν οργανισμό υγείας, μια μεγάλη ή μια μικρή επιχείρηση, η εξασφάλιση μιας ταχείας ανάπτυξης του 5G είναι ζωτικής σημασίας για την ευέλικτη ΤΠ (Τεχνολογία Πληροφοριών, ή IT στα αγγλικά, από το “Information Technology”) και την ικανοποίηση των νέων απαιτήσεων των χρηστών. Καθώς όμως η παγκόσμια ζήτηση για την τεχνολογία 5G επεκτείνεται, αυξάνεται και η ανάγκη για ενισχυμένη ασφάλεια. Ενώ το 5G προσφέρει πολλά οφέλη, ενέχει αυξημένο κίνδυνο ασφάλειας. Το 5G όμως δεν αυξάνει μόνο τον αριθμό των συσκευών αλλά και

τους τύπους των συσκευών που πρέπει να προστατευθούν, συμπεριλαμβανομένων των συσκευών IoT, των αισθητήρων, των καμερών, των εικονικών βοηθών κ.λπ. Αυτό διευρύνει την επιφάνεια επίθεσης του δικτύου, με αποτέλεσμα να δημιουργούνται περισσότερα τρωτά σημεία και κενά στο δίκτυο που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι. Τα δίκτυα 5G δημιουργούν ελκυστικούς στόχους για εγκληματίες του κυβερνοχώρου και ξένους αντιπάλους για την αποκάλυψη πολύτιμων πληροφοριών (information) ή ακόμα και επεξεργασμένης πληροφορίας (intelligence) που μπορούν να απειλήσουν την εθνική ασφάλεια και να επηρεάσουν άλλα παγκόσμια συμφέροντα.

Η Ευρωπαϊκή Ένωση σε δημοσίευμα της ανακοίνωσε πως εντοπίστηκαν 60 προκλήσεις στον τομέα ασφάλειας του 5G και ταξινομήθηκαν ονομαστικά σε επτά κατηγορίες:

- Εικονικοποίηση ή εμπορευματοκιβώτιο
- Ενορχήστρωση και διαχείριση
- Διαχείριση και έλεγχος πρόσβασης
- Νέες και παλαιές τεχνολογίες
- Υιοθέτηση ανοικτού κώδικα ή COTS (Commercial-off-the-shelf)
- Αλυσίδα εφοδιασμού
- Νόμιμη υποκλοπή (LI, Lawful Interception)

Η εμπορευματοκιβωτιοποίηση (~~στα αγγλικά~~ Containerization) είναι ένας τύπος εικονικοποίησης στον οποίο όλα τα στοιχεία μιας εφαρμογής συγκεντρώνονται σε μια ενιαία εικόνα εμπορευματοκιβωτίου (container) και μπορούν να εκτελούνται σε απομονωμένο χώρο του χρήστη στο ίδιο κοινό λειτουργικό σύστημα. Τα εμπορευματοκιβώτια είναι ελαφριά, φορητά και ευνοούν σε μεγάλο βαθμό την αυτοματοποίηση.

Μία εξαιρετική έρευνα όσον αφορά τις αδυναμίες του 5G στην εποχή μας παραδίδεται στην συνέχεια, η οποία εισέρχεται και στο επόμενο κεφάλαιο της παρούσας εργασίας το οποίο θα απαρτίζεται από τις κινήσεις που μπορούμε να κάνουμε ώστε να ασφαλίσουμε αυτές τις τεχνολογίες (IoT και 5G) από κάθε είδους κακόβουλη ενέργεια. Την έρευνα αυτή έχουν υλοποιήσει οι Cybersecurity and Infrastructure Security Agency (CISA) και το Department of Defense (DoD), όπου οι συγκεκριμένοι οργανισμοί έχουν κάθε δικαίωμα στην αναφερόμενη έρευνα (πρόσβαση στην έρευνα από τον ακόλουθο σύνδεσμο: 5G Security Evaluation Process Investigation ή, σε περίπτωση που ο συγκεκριμένος σύνδεσμος πάψει να λειτουργεί, μπορείτε να ενημερωθείτε απευθείας από το site της CISA, όσον αφορά την ασφάλεια του 5G αλλά και πολλών άλλων τεχνολογιών, στον σύνδεσμο: https://www.cisa.gov/.

Το πλαίσιο πολιτικής που διέπει το 5G και την ασφάλεια σχετικά με αυτό αποτελείται από υποχρεωτικούς κανόνες δικαίου, οι οποίοι είναι νομικά δεσμευτικοί και εκτελεστοί (π.χ. κανονισμοί), και από μη δεσμευτικούς κανόνες (π.χ. ανακοινώσεις της Επιτροπής). Στην εικόνα 6.1 παρατίθενται τα βασικά έγγραφα πολιτικής και οι βασικοί στόχοι.

Εικόνα 6.1: Έγγραφα πολιτικής και βασικοί στόχοι για την ανάπτυξη και ασφάλεια του 5G [7.27]

Στη σελίδα του Publications Office of the European Union μπορούμε να βρούμε και το ακόλουθο απόσπασμα, ο συγκεκριμένος φορέας παρατίθεται στην Βιβλιογραφία όπως και το άρθρο στο οποίο θα αναφερθούμε παρακάτω, όσον αφορά την ασφάλεια και τον έλεγχο του 5G εντός της Ε.Ε. Όλα τα δικαιώματα όσον αφορά την συγκεκριμένη έκθεση ανήκουν στον προαναφερθέντα φορέα και το απόσπασμα έχει ως εξής:

Εμβέλεια και τρόπος προσέγγισης του ελέγχου

Στο πλαίσιο του εν προκειμένω ελέγχου, εξετάσαμε κατά πόσον η Επιτροπή στήριξε αποτελεσματικά τα κράτη μέλη όσον αφορά:

Την επίτευξη των στόχων της ΕΕ για το 2025 και το 2030 σχετικά με την ανάπτυξη και την έναρξη λειτουργίας των οικείων δικτύων 5G και τη συντονισμένη αντιμετώπιση των ανησυχιών σχετικά με την ασφάλεια του 5G.

Για αμφότερους τους εν λόγω τομείς, εξετάσαμε επίσης τα μέτρα και τις δραστηριότητες των κρατών μελών.

Με τον όρο «ασφάλεια του 5G» αναφερόμαστε στην κυβερνοασφάλεια και στην ασφάλεια του υλικού/λογισμικού. Εξετάσαμε τόσο το ζήτημα της ασφάλειας όσο και της υλοποίησης των δικτύων 5G, για τα οποία το 2020 ήταν καθοριστικό. Σκοπός της παρούσας έκθεσης είναι η παράθεση διαφωτιστικών στοιχείων και η διατύπωση συστάσεων σχετικά με την έγκαιρη ανάπτυξη ασφαλών δικτύων 5G στην ΕΕ.

Ο έλεγχος που διενεργήσαμε καλύπτει την περίοδο από το 2016 έως τον Μάιο του 2021. Στο μέτρο του δυνατού, συμπεριλάβαμε ακόμη πιο πρόσφατα επικαιροποιημένα στοιχεία. Στο πλαίσιο των ελεγκτικών εργασιών μας:

Εξετάσαμε την ενωσιακή νομοθεσία, τις πρωτοβουλίες της Επιτροπής και άλλη συναφή τεκμηρίωση, συνομιλήσαμε με εκπροσώπους της Επιτροπής, της ΕΤΕπ, του Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC), του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), των ενώσεων στον τομέα των τηλεπικοινωνιών, των φορέων εκμετάλλευσης κινητών δικτύων, των προμηθευτών 5G, διεθνών οργανισμών, με εμπειρογνώμονες του τομέα προκειμένου να συλλέξουμε λεπτομερείς πληροφορίες, καθώς και με εκπροσώπους των αρμόδιων αρχών στη Φινλανδία, τη Γερμανία, την Πολωνία και την Ισπανία. Η επιλογή των κρατών μελών βασίστηκε σε κριτήρια όπως το ποσό των ενωσιακών κονδυλίων που διατίθενται σε έργα σχετικά με το 5G, η κατάσταση της ανάπτυξής του, λαμβάνοντας

επίσης υπόψη την εξασφάλιση γεωγραφικής ισορροπίας, υποβάλαμε ερωτηματολόγιο στις ρυθμιστικές αρχές τηλεπικοινωνιών και των 27 κρατών μελών της ΕΕ, προκειμένου να εξετάσουμε από ευρύτερη οπτική τις προκλήσεις που αντιμετωπίζουν τα κράτη μέλη σχετικά με το 5G και τέλος εξετάσαμε δέκα συγχρηματοδοτούμενα από την ΕΕ έργα (ΕΤΣΕ, ΕΤΠΑ και «Ορίζων 2020») σχετικά με το 5G, που επιλέξαμε για ενδεικτικούς σκοπούς.

Βασιστήκαμε επίσης στην πρόσφατη επισκόπηση που πραγματοποιήσαμε σχετικά με την απόκριση της ΕΕ στη στρατηγική κατευθυνόμενων από το κράτος επενδύσεων της Κίνας, καθώς και σε άλλες εκθέσεις μας, παραδείγματος χάριν την έκθεση σχετικά με την ευρυζωνικότητα, την έκθεση σχετικά με την πρωτοβουλία για την ψηφιοποίηση της ευρωπαϊκής βιομηχανίας και την επισκόπηση σχετικά με την ενωσιακή πολιτική για την κυβερνοασφάλεια.

Από τα παραπάνω προκύπτει πως το ζήτημα της εδραίωσης του 5G στην Ευρώπη, αλλά και σε όλο τον κόσμο, δεν είναι απλό. Υπάρχουν πολλές πτυχές που θα πρέπει να εξεταστούν και ποικίλες λεπτομέρειες όσον αφορά την κυβερνοασφάλεια που είναι αναγκαίο να διεκπεραιωθούν ώστε το 5G να μπορέσει να εδραιωθεί ορθά, γρήγορα, και κατά κύριο λόγο, με ασφάλεια

7 Τρόποι ασφάλισης ακεραιότητας

Όσον αφορά την ανάπτυξη, το αποτέλεσμα, το IoT με δυνατότητες 5G παρέχει πολύ μεγάλες προσδοκίες . Ο όγκος των δεδομένων που διανέμονται και επεξεργάζονται από συστήματα IoT που εμπιστεύονται και βασίζονται στη συνδεσιμότητα (connectivity) και στην κάλυψη (coverage) δημιουργεί ορισμένα προβλήματα ασφάλειας. Καθώς η τεχνολογία IoT χρησιμοποιείται άμεσα στην καθημερινή μας ζωή, οι απειλές του σημερινού κυβερνοχώρου μπορεί να γίνουν πιο εμφανείς σε παγκόσμιο επίπεδο. Η παρατεταμένη διάρκεια ζωής των δικτύων, η κάλυψη και η συνδεσιμότητα απαιτούνται για την ασφάλεια των συσκευών δικτύου 5G που βασίζονται στο IoT. Ως αποτέλεσμα αυτών των χαρακτηριστικών, υπάρχουν ελαττώματα που οδηγούν σε παραβιάσεις της ασφάλειας. Επειδή τα σκόπιμα σφάλματα μπορούν γρήγορα να καταστήσουν ολόκληρο το δίκτυο δυσλειτουργικό, είναι πιο δύσκολο να εντοπιστούν από ό,τι οι απροσδόκητες αστοχίες.

7.1 Ασφάλεια IoT συσκευών και συνδέσεων

Τα διασυνδεδεμένα αντικείμενα IoT δεν είναι οι ίδιες συσκευές, αντικείμενα ή υπηρεσίες. Κάθε αντικείμενο έχει διαφορετικό σκοπό, διεπαφή, μηχανισμό λειτουργίας και υποκείμενη τεχνολογία. Δεδομένης αυτής της ποικιλομορφίας, η εφαρμογή μιας ενιαίας δομής και προσέγγισης ασφάλειας για όλα τα αντικείμενα δεν αρκεί για να παρέχει την ασφάλεια που απαιτείται για τα δίκτυα IoT. Οι πρωτοβουλίες για την ασφάλεια του IoT προστατεύουν τις συσκευές IoT που συνδέονται μέσω ενός δικτύου με προληπτικές μεθόδους και αποσκοπούν στην αποτροπή κυβερνοεπιθέσεων μεγάλης κλίμακας που μπορούν να πραγματοποιηθούν μέσω αυτών. Όπως κάθε άλλη υπολογιστική συσκευή, έτσι και οι συσκευές IoT αποτελούν δυνητικά σημεία εισόδου για τους επιτιθέμενους προκειμένου να παραβιάσουν το δίκτυο μιας εταιρείας. Ως εκ τούτου, απαιτούνται ισχυρά μέτρα ασφαλείας για την προστασία τους.

Οι συσκευές IoT μπορούν να συνδεθούν σε ένα δίκτυο ή στο διαδίκτυο για να ανταλλάσσουν δεδομένα με άλλα συνδεδεμένα αντικείμενα ή κέντρα. Οι συσκευές αυτές δεν περιορίζονται μόνο σε έξυπνες τηλεοράσεις ή έξυπνα ρολόγια. Οι εκτυπωτές, τα πλυντήρια ρούχων, τα κλιματιστικά, οι έξυπνοι αισθητήρες και άλλα βιομηχανικά μηχανήματα

που συνδέονται σε δίκτυα αποτελούν επίσης συσκευές IoT. Ο τρόπος με τον οποίο εφαρμόζεται σήμερα το IoT απαιτεί από τα ιδρύματα και τους οργανισμούς να διαθέτουν οικοσυστήματα που αποτελούνται από πολλές διαφορετικές συσκευές. Είναι ζωτικής σημασίας να χρησιμοποιηθεί ένας συνδυασμός λύσεων, στρατηγικών και τεχνικών ασφάλειας του IoT αντί των παραδοσιακών προσεγγίσεων για τη διασφάλιση της ασφάλειας αυτού του οικοσυστήματος. Γεμάτες ευπάθειες και προσφέροντας μια επιφάνεια επίθεσης ώριμη για παραβιάσεις ασφαλείας, οι συσκευές IoT αποτελούν ελκυστικούς στόχους για τους εγκληματίες του κυβερνοχώρου. Είτε επιχειρήσεις, οργανισμοί, φορείς ή ακόμη και το ίδιο μας το σπίτι τα οποίες μόλις ξεκινούν με την υιοθέτηση του IoT είτε εκείνα που επιθυμούν να επεκτείνουν τα καθιερωμένα τους δίκτυα IoT, όλα αντιμετωπίζουν παρόμοιες προκλήσεις όσον αφορά τη διαχείριση, την παρακολούθηση και την ασφάλεια των συνδεδεμένων περιβαλλόντων IoT.

7.1.1 Τρόποι ασφάλισης υλικού και λογισμικού

Για την επιτυχή διασφάλιση των συσκευών IoT, υπάρχουν μερικά πράγματα που πρέπει να ληφθούν υπόψη για την ασφάλεια και την ορθή λειτουργεία αυτών των συσκευών.

- Ανακάλυψη συσκευών για πλήρη ορατότητα

Το πρώτο πράγμα που χρειάζεται να κάνει ένας φορέας είναι να αποκτήσει ορατότητα στον ακριβή αριθμό των συσκευών IoT που είναι συνδεδεμένες στο δίκτυό του. Χρειάζεται να ανακαλυφθούν ποιοι τύποι συσκευών είναι συνδεδεμένοι στο δίκτυό και να διατηρηθεί μια λεπτομερής, ενημερωμένη απογραφή όλων των συνδεδεμένων περιουσιακών στοιχείων IoT, ιδανικά με μια ειδική λύση ασφάλειας (προγράμματα τα οποία είναι δημιουργημένα για αυτό τον συγκεκριμένο σκοπό) IoT για να διασφαλιστεί ότι όλες οι συσκευές έχουν εντοπιστεί. Χρειάζεται η επωνυμία του κατασκευαστή και το αναγνωριστικό μοντέλου, τον σειριακό αριθμό, τις εκδόσεις υλικού, λογισμικού και υλικολογισμικού, καθώς και πληροφορίες σχετικά με τα υποκείμενα λειτουργικά συστήματα και τη διαμόρφωση που εφαρμόζεται σε κάθε συσκευή. Απαιτείται το προφίλ κινδύνου κάθε συσκευής και τη συμπεριφορά της σε σχέση με άλλες συνδεδεμένες συσκευές στο δίκτυο. Αυτά τα προφίλ βοηθούν στην τμηματοποίηση και στη δημιουργία πολιτικής τείχους προστασίας επόμενης γενιάς. Χρειάζεται να διατηρείται ο χάρτης περιουσιακών στοιχείων επίκαιρο με κάθε νέα συσκευή IoT που συνδέεται στο δίκτυο.

- Εφαρμογή τμηματοποίησης δικτύου για ισχυρότερη άμυνα

Ο επιθυμητός στόχος ασφάλειας με την τμηματοποίηση δικτύου είναι η μείωση της επιφάνειας επίθεσης. Η τμηματοποίηση δικτύου διαιρεί ένα δίκτυο σε δύο ή περισσότερα υποτμήματα για να επιτρέπει τον λεπτομερή έλεγχο της πλευρικής κίνησης (lateral movement) της κυκλοφορίας μεταξύ συσκευών και φόρτων εργασίας. Σε ένα μη τμηματοποιημένο δίκτυο, όταν ένας μεγάλος αριθμός τελικών σημείων επικοινωνεί απευθείας μεταξύ τους χωρίς να υπάρχει διαμερισματοποίηση, υπάρχει μεγαλύτερη πιθανότητα ένα μεμονωμένο συμβάν παραβίασης να εξαπλωθεί πλευρικά και να μετατραπεί σε μόλυνση. Αντίθετα, όσο περισσότερο τμηματοποιημένο είναι ένα δίκτυο, τόσο πιο δύσκολο είναι για τους hackers να θέσουν σε κίνδυνο μια συσκευή ως μοναδικό σημείο συμβιβασμού για την εισχώρηση exploits ή ransomware πλευρικά. Οι φορείς χρειάζεται να χρησιμοποιούν διαμορφώσεις εικονικών τοπικών δικτύων (VLAN) και πολιτικές τείχους προστασίας νέας γενιάς για την υλοποίηση τμημάτων δικτύου που κρατούν τις συσκευές IoT χωριστά από τα περιουσιακά στοιχεία IT. Με αυτόν τον τρόπο, και οι δύο ομάδες μπορούν να προστατευτούν από την πιθανότητα πλευρικής εκμετάλλευσης (lateral exploit). Μία ολοκληρωμένη ενσωμάτωση μεταξύ της λύσης ασφάλειας IoT και του τείχους προστασίας επόμενης γενιάς (Next-Generation Firewall, NGFW), θα προσθέσει τις λειτουργείες του IoT υπό την προστασία αυτής της συγχώνευσης και θα μειώσει τόσο το χρόνο όσο και την προσπάθεια για τη δημιουργία πολιτικών ασφαλείας.

- Υιοθέτηση πρακτικών ασφαλούς κωδικού πρόσβασης

Οι κακές πρακτικές ασφάλειας κωδικών πρόσβασης συνεχίζουν να τροφοδοτούν τις επιθέσεις που σχετίζονται με τους κωδικούς πρόσβασης σε συσκευές IoT. Ως εκ τούτου, η διατήρηση ισχυρής ασφάλειας κωδικών πρόσβασης είναι ζωτικής σημασίας για την ασφάλεια των τελικών σημείων IoT. Πολλές συσκευές IoT διατίθενται με αδύναμους προκαθορισμένους κωδικούς πρόσβασης που είναι εύκολο να βρεθούν στο διαδίκτυο. Μόλις μια συσκευή IoT συνδεθεί για πρώτη φορά στο δίκτυό σας, αποτελεί βέλτιστη πρακτική η αλλαγή του προκαθορισμένου κωδικού πρόσβασής της με έναν ασφαλή, πιο σύνθετο. Ο νέος κωδικός πρόσβασης θα πρέπει να είναι δύσκολα προβλέψιμος, μοναδικός για κάθε ασφαλιζόμενη συσκευή και σύμφωνος με τις πολιτικές και τις πρακτικές διαχείρισης κωδικών πρόσβασης της ομάδας ασφαλείας σας για θέματα πληροφορικής. Είναι θεμιτό στην ενασχόληση με ευαίσθητές συσκευές τεχνολογίας να ζητείται η συμβουλή ειδικών πριν από κάθε εγκατάσταση και ενημέρωση αυτών.

- Ενίσχυση και ενημέρωση το υλικολογισμικού όταν είναι διαθέσιμο

Ενώ τα περισσότερα συστήματα IT είναι σε θέση να επιδιορθώνουν τα κενά ασφαλείας μέσω τακτικών ενημερώσεων, οι περισσότερες συσκευές IoT δεν έχουν σχεδιαστεί με αυτή τη δυνατότητα, οπότε τα κενά ασφαλείας τους παραμένουν εκεί επ' αόριστον. Στην περίπτωση συσκευών IoT με ιδιαίτερα μεγάλη διάρκεια ζωής, υπάρχει συχνά και ο κίνδυνος να διακόψει ο κατασκευαστής την υποστήριξη. Όταν εγκαθίσταται μια νέα συσκευή IoT, θα πρέπει να κατεβαίνουν τυχόν νέες διορθώσεις ασφαλείας για γνωστές ευπάθειες. Είναι σημαντικό να διασφαλίζεται πως οι συσκευές επιδιορθώνονται τακτικά με τις τελευταίες ενημερώσεις, γι' αυτό χρειάζεται η συνεργασία με τους προμηθευτές των συσκευών IoT για την καθιέρωση μιας επαναλαμβανόμενης στρατηγικής διαχείρισης επιδιορθώσεων και αναβάθμισης υλικολογισμικού. Για την αποφυγή απώλειας δεδομένων, χρειάζεται να προστίθενται λογισμικά στην ασφάλεια με ειδικές ικανότητες πρόληψης απειλών από αρχεία και ιστό (dedicated IoT-aware file and web threat prevention), τα οποία έχουν πλήρη επίγνωση των IoT συσκευών, καθώς και δυνατότητες εικονικής επιδιόρθωσης (virtual patching capabilities) για την μέγιστη πρόληψη εισβολών.

- Διαρκής και ενεργή παρακολούθηση των συσκευών IoT

Η παρακολούθηση σε πραγματικό χρόνο, η υποβολή εκθέσεων και η ειδοποίηση σε περιπτώσεις κινδύνου είναι ζωτικής σημασίας για τους οργανισμούς, φορείς και ιδιωτικούς χώρους, προκειμένου να διαχειριστούν τους κινδύνους IoT. Ωστόσο, δεδομένου ότι οι παραδοσιακές λύσεις ασφάλειας τελικών σημείων απαιτούν πράκτορες λογισμικού (software agents) όπου οι συσκευές IoT δεν είναι σχεδιασμένες να λαμβάνουν, αυτές οι παραδοσιακές λύσεις δεν μπορούν να προστατεύσουν τα περιουσιακά στοιχεία IoT στην σημερινή εποχή. Χρειάζεται η δοκιμή μιας καλύτερης και πιο αποδοτικής προσέγγισης. Η εφαρμογή μια λύσης παρακολούθησης σε πραγματικό χρόνο (real-time monitoring solution, προγράμματα κατασκευασμένα παρακολουθούν και να αναλύουν συσκευές σε πραγματικό χρόνο) αναλύει συνεχώς τη συμπεριφορά όλων των συνδεδεμένων στο δίκτυο τερματικών σημείων IoT, ενσωματώνοντας απρόσκοπτα και ομαλά την υπάρχουσα στάση ασφαλείας αλλά και με την επένδυση ενός τείχους προστασίας επόμενης γενιάς. Με αυτό τον τρόπο οι υπηρεσίες υπεύθυνες για την ασφάλειας θα έχουν πλήρη επίγνωση των χαρακτηριστικών μεταξύ τους και θα είναι σε θέση να παράγουν ένα σύστημα πολύ πιο ικανό να προστατεύσει την ιδιοκτησία.

- Ενεργοποίηση ελέγχου ταυτότητας πολλαπλών παραγόντων

Με τη χρήση του net banking (ή E-banking), είναι πλέον γνωστό τι είναι ο έλεγχος ταυτότητας πολλαπλών παραγόντων. Ο έλεγχος ταυτότητας πολλαπλών, συνήθως δύο, παραγόντων (2FA) είναι ένα πρόσθετο επίπεδο ασφάλειας πέρα από έναν απλό κωδικό πρόσβασης. Με τον έλεγχο ταυτότητας δύο παραγόντων, κάθε φορά που κάποιος προσπαθεί να συνδεθεί στη συσκευή IoT, πρέπει να παρέχει πρόσθετη απόδειξη της ταυτότητάς του. Αυτή η απόδειξη μπορεί να έχει τη μορφή ενός pin (κωδικού) μιας χρήσης (OTP, one-time password) ή ενός κωδικού επαλήθευσης που αποστέλλεται στο τηλέφωνό ή στη διεύθυνση ηλεκτρονικού ταχυδρομείου και επιβεβαιώνει ότι το άτομο που συνδέεται είναι όντως ο κάτοχος της συσκευής. Οι περισσότερες έξυπνες συσκευές διαθέτουν εξ ορισμού τη λειτουργία ελέγχου ταυτότητας πολλαπλών παραγόντων, αλλά υπάρχουν ορισμένες συσκευές που δεν την διαθέτουν. Σε αυτή την περίπτωση, μπορεί-να ενεργοποιηθεί το 2FA χρησιμοποιώντας εφαρμογές τρίτων, όπως το Google Authenticator. Ακόμα και αν η συσκευή IoT διαθέτει έλεγχο ταυτότητας δύο παραγόντων με τη σχετιζόμενη με αυτή εφαρμογή για κινητά, η ύπαρξη ενός επιπλέον επιπέδου ασφάλειας μέσω μιας αξιόπιστης υπηρεσίας τρίτων (third-party service) μπορεί να δώσει περαιτέρω ηρεμία και αίσθηση σιγουριάς.

- Απενεργοποίηση λειτουργιών που δεν χρησιμοποιούνται

Πολλές συσκευές IoT δίνουν τη δυνατότητα ελέγχου από οπουδήποτε. Αν όμως γίνετε χρήση μόνο της οικιακής σύνδεσης Wi-Fi, χρειάζεται να απενεργοποιηθεί η απομακρυσμένη πρόσβαση. Ομοίως, τα έξυπνα ηχεία διαθέτουν συνδεσιμότητα Bluetooth εκτός από Wi-Fi. Οι έξυπνες τηλεοράσεις διαθέτουν φωνητικό έλεγχο, αλλά αυτή η λειτουργία συχνά μένει αχρησιμοποίητη, ακόμη και σε νοικοκυριά με φωνητικό έλεγχο, όπου οι έξυπνοι βοηθοί όπως ο Google Assistant, η Siri ή η Alexa κυριαρχούν. Ένα ενεργό μικρόφωνο, αν παραβιαστεί, μπορεί επίσης να χρησιμοποιηθεί για να κατασκοπεύσει συνομιλίες. Επιπλέον, λειτουργείες που δεν χρησιμοποιούντα, ή ακόμη και συσκευές μη συντηρημένες και ενημερωμένες λόγω μη χρήσης τους, μπορούν δυνητικά να αποτελέσουν σημεία εισόδου λόγω του ότι και το λογισμικό τους δεν είναι ενημερωμένο ώστε να αντιμετωπίσει την νέες απειλές. Έτσι, η απενεργοποίηση των λειτουργιών και συσκευών έχει να κάνει με τον αποκλεισμό όσο το δυνατόν περισσότερων από αυτά τα πολλαπλά σημεία εισόδου.

- Αποφυγή χρήσης του Universal Plug and Play

Ενώ το Universal Plug and Play (UPnP) έχει τις χρήσεις του, μπορεί να καταστήσει τους εκτυπωτές, τους δρομολογητές, τις κάμερες και τις συσκευές IoT ευάλωτους σε επιθέσεις στον κυβερνοχώρο. Η αρχή πίσω από το σχεδιασμό του UPnP είναι να διευκολύνει τη δικτύωση συσκευών χωρίς πρόσθετες ρυθμίσεις και να τις βοηθήσει να ανακαλύπτουν αυτόματα η μία την άλλη και να εγκαθιστούν λειτουργικές υπηρεσίες δικτύου. Ωστόσο, αυτό ωφελεί περισσότερο από οτιδήποτε άλλο τους hackers, καθώς μπορούν να ανακαλύψουν όλες τις συσκευές IoT πέρα από το τοπικό ~~σας~~ δίκτυο. Ως εκ τούτου, είναι επιθυμητή η πλήρης απενεργοποίηση του UPnP.

7.1.2 Ασφάλεια δρομολογητή (Router)

Ο δρομολογητής Wi-Fi είναι η πύλη προς το έξυπνο σπίτι σας και δεν είναι επιθυμητή η παραβίαση του. Η δημιουργία ενός ασφαλούς έξυπνου σπιτιού ξεκινά από το δρομολογητή. Είναι αυτό που συνδέει όλες τις συσκευές IoT ~~σας~~ και τις καθιστά τόσο ευάλωτες. Υπάρχουν βέλτιστες πρακτικές για τη δημιουργία ασφαλούς δρομολογητή:

1. Αλλαγή προεπιλεγόμενου ονόματος δρομολογητή

   Εάν κάποιοι ανακαλύψουν τη μάρκα και το μοντέλο του δρομολογητή, μπορεί να αναζητήσουν την προεπιλεγμένη σύνδεση και τον κωδικό πρόσβασης και να αποκτήσουν εύκολη πρόσβαση στο έξυπνο οικιακό δίκτυο. Συνίσταται η αλλαγή σε ένα ασυνήθιστο όνομα που δεν σχετίζεται με προσωπικά δεδομένα ή τη διεύθυνσή της οικίας. Η δημιουργική φαντασία βοηθά στο νέο όνομα του δρομολογητή σας.

~~2.~~ Ορισμός μοναδικού κωδικού πρόσβασης

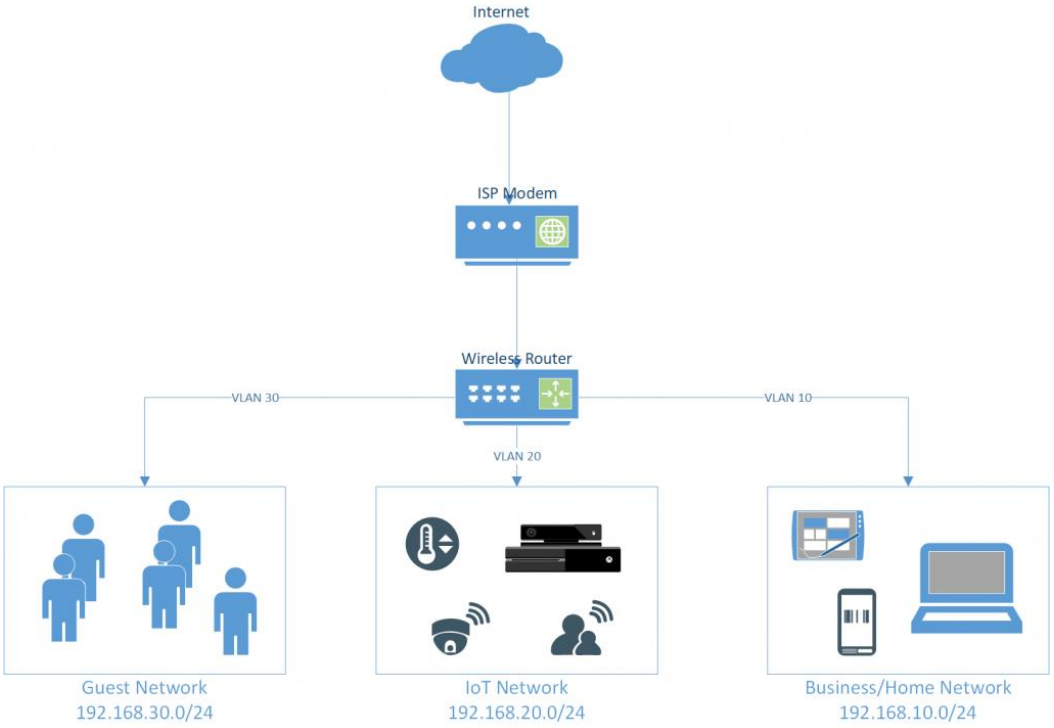
   Παρόμοια με το όνομα του δρομολογητή, απαιτείται ο ορισμός του κωδικού πρόσβασης του δρομολογητή σε κάτι πραγματικά μοναδικό. Συνίσταται η χρήση σύνθετων κωδικών πρόσβασης που αποτελούνται από γράμματα, αριθμούς και σύμβολα. Ακόμη, επιθυμητή είναι η χρήση γεννήτριας τυχαίων κωδικών πρόσβασης (password generator) για τη δημιουργία ενός σχεδόν αδιαπέραστου κωδικού πρόσβασης.

3. Χρήση τοy υψηλότερου επίπεδου κρυπτογράφησης

   Επιθυμητή είναι η επιλογή του υψηλότερου επίπεδου κρυπτογράφησης, το οποίο επί του παρόντος στις περισσότερες συσκευές είναι το WPA2 (το WPA3 εδραιώνεται σταδιακά). Εάν ο δρομολογητής ~~σας~~ υποστηρίζει μόνο τα πρωτόκολλα WPA ή WEP, ίσως να είναι αναγκαία μια αναβάθμιση. Οι οικιακοί δρομολογητές αποτελούν πρωταρχικούς στόχους IoT για τους hackers. Έτσι, ένας ασφαλής δρομολογητής μεταφράζεται σε ένα ουσιαστικά πιο ασφαλές έξυπνο σπίτι. Εάν αναφερόμαστε σε κάποιο οργανισμό, εταιρεία ή φορέα, είναι θεμιτό έως απολύτως αναγκαία η αναβάθμιση του δρομολογητή σε έναν επαγγελματικών προδιαγραφών, με πολύ πιο ευέλικτες δυνατότητες και ασφαλή περιβάλλοντα.

4. Δημιουργία ξεχωριστού δικτύου Wi-Fi για συσκευές IoT

   Πολλοί σύγχρονοι δρομολογητές σας παρέχουν τη δυνατότητα δημιουργίας δικτύου επισκεπτών (ή δευτερεύον δίκτυο). Δημιουργώντας ένα ξεχωριστό δίκτυο αφιερωμένο στις συσκευές IoT, προστατεύεται το κύριο δίκτυό από απειλές IoT. Αυτό σημαίνει ότι συγγενείς, φίλοι και επισκέπτες μπορούν να συνδεθούν σε ένα δίκτυο που δεν σχετίζεται με τις συσκευές IoT. Έτσι, το τοπικό έξυπνο οικιακό δίκτυο είναι προσβάσιμο μόνο από τον κάτοχο και τους οικείους του. Καθώς η τοποθέτηση των συσκευών IoT σε διαφορετικό δίκτυο τις κρατάει αποκομμένες, αν οι hackers καταφέρουν να περάσουν, δεν μπορούν να έχουν πρόσβαση σε καμία από τις πιο σημαντικές συσκευές, όπως ο φορητός υπολογιστής ή το smartphone. Ο Ofer Maor, ηγέτης στην κυβερνοασφάλεια και μέλος του διοικητικού συμβουλίου του Ιδρύματος OWASP, αναφέρει: "Διαχειρίζομαι το σπίτι μου σε πολλαπλά τμήματα δικτύου. Υπάρχει το δίκτυο του "γραφείου" μου με τους φορητούς υπολογιστές, το NAS και όλα τα σημαντικά ευαίσθητα μέρη του σπιτιού μου. Υπάρχει το δίκτυο 'Home IoT' του σπιτιού μου, στο οποίο βρίσκονται οι περισσότερες συσκευές IoT. Αυτό περιορίζει την παραβίαση - αν μια από τις συσκευές IoT μου παραβιαστεί, ο hacker είναι ικανός να εισχωρήσει από αυτήν σε άλλες συσκευές IoT, αλλά δεν θα μπορέσει να φτάσει στο φορητό υπολογιστή μου ή στα ευαίσθητα δεδομένα μου". Ένα απλό παράδειγμα για το πως λειτουργούν τα πολλαπλά δίκτυα απεικονίζεται στην Εικόνα 7.1, και αυτός είναι ένας θεμιτός τρόπος διαχείρισης πολλαπλών συσκευών.



Εικόνα 7.1: Δίκτυο χωρισμένο σε τμήματα [7.28]

Το συγκεκριμένο δίκτυο έχει διασπαστεί σε 3 υπό-δίκτυα, το δίκτυο “VLAN10”, “VLAN20” και “VLAN30”, όπου αντίστοιχα διαχειρίζονται τις συσκευές εργασίας και σπιτιού, της συσκευές του IoT και τέλος των επισκεπτών.

Είτε οι εκκολαπτόμενοι νόμοι για τον κυβερνοχώρο είναι κατάλληλοι για να αντιμετωπίσουν τους προληπτικούς εγκληματίες του κυβερνοχώρου παγκοσμίως είτε όχι, η ζήτηση για προϊόντα ασφαλείας IoT αυξάνεται διαρκώς σε μια αγορά που ωριμάζει. Δημοσιεύματα ειδήσεων ενημερώνουν ότι η αγορά ασφάλειας IoT της Βόρειας Αμερικής αναμένεται να αυξηθεί κατά περίπου 25% ετησίως και η ανάπτυξη θα οδηγηθεί από τη συνεχώς αυξανόμενη ζήτηση για λύσεις ασφάλειας συσκευών IoT, επιχειρηματικές εφαρμογές που βασίζονται στο cloud και άλλες παρόμοιες απαιτήσεις. Δεν θα είναι υπερβολή να αναφερθεί πως σε άλλα μέρη του κόσμου θα αυξηθεί ραγδαία η ζήτηση για λύσεις ασφάλειας IoT, ανάλογα με την αυξανόμενη χρήση συσκευών και δικτύων IoT.

7.2 Ασφάλεια δικτύου 5G

Το 5G έχει σχεδιάσει ελέγχους ασφαλείας για την αντιμετώπιση πολλών από τις απειλές που αντιμετωπίζουν τα σημερινά δίκτυα 4G/3G/2G. Αυτοί οι έλεγχοι περιλαμβάνουν νέες δυνατότητες αμοιβαίου ελέγχου ταυτότητας (mutual authentication), ενισχυμένη προστασία της ταυτότητας του συνδρομητή και πρόσθετους μηχανισμούς ασφαλείας. Το 5G προσφέρει στον κλάδο της κινητής τηλεφωνίας μια άνευ προηγουμένου ευκαιρία για την αναβάθμιση των επιπέδων ασφάλειας του δικτύου και των υπηρεσιών. Το 5G παρέχει προληπτικά μέτρα για τον περιορισμό των επιπτώσεων σε γνωστές απειλές, αλλά η υιοθέτηση νέων τεχνολογιών δικτύου εισάγει πιθανές νέες απειλές που πρέπει να διαχειριστεί ο κλάδος.

7.2.1 Προστασία συνδρομητών και συσκευών

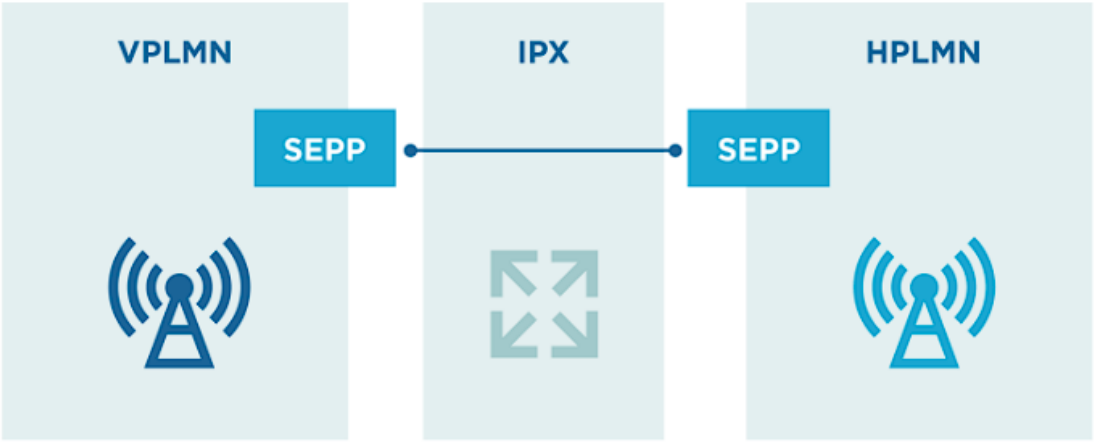
Το 5G βελτιώνει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων των χρηστών και των συσκευών. Σε αντίθεση με τις προηγούμενες γενιές συστημάτων κινητής τηλεφωνίας το 5G:

- Προστατεύει την εμπιστευτικότητα των μηνυμάτων μεταξύ της συσκευής και του δικτύου, του αρχικού στρώματος μη πρόσβασης (non-access stratum, NAS). Ως αποτέλεσμα, δεν είναι πλέον δυνατή η ανίχνευση του εξοπλισμού χρήστη (user equipment, UE) με τη χρήση των σημερινών μεθοδολογιών επίθεσης μέσω της ραδιοδιεπαφής· προστατεύει από επιθέσεις man in the middle (MITM) και επιθέσεις ψεύτικου σταθμού βάσης (Stingray/IMSI catcher).
- Εισάγει έναν μηχανισμό προστασίας που ονομάζεται home control. Αυτό σημαίνει ότι ο τελικός έλεγχος ταυτότητας της συσκευής (device authentication) σε ένα δίκτυο επίσκεψης (visited network) ολοκληρώνεται αφού το δίκτυο προέλευσης (home network) έχει ελέγξει την κατάσταση ελέγχου ταυτότητας της συσκευής στο δίκτυο επίσκεψης. Αυτή η βελτίωση θα αποτρέψει διάφορους τύπους απάτης μέσω της περιαγωγής (roaming fraud) που στο παρελθόν παρεμπόδιζαν τους φορείς εκμετάλλευσης, και θα υποστηρίξει τους φορείς εκμετάλλευσης ώστε να επιτυγχάνουν σωστή πιστοποίηση της ταυτότητας των συσκευών στις υπηρεσίες.

- Υποστηρίζει ενοποιημένο έλεγχο ταυτότητας σε άλλους τύπους δικτύων πρόσβασης, π.χ. WLAN, επιτρέποντας στα δίκτυα 5G να διαχειρίζονται συνδέσεις που προηγουμένως ήταν μη διαχειρίσιμες και μη ασφαλείς. Αυτό περιλαμβάνει τη δυνατότητα εκτέλεσης εκ νέου πιστοποίησης ταυτότητας του UE όταν αυτό μετακινείται μεταξύ διαφορετικών δικτύων πρόσβασης ή εξυπηρέτησης.
- Εισάγει τον έλεγχο ακεραιότητας του επιπέδου χρήστη, διασφαλίζοντας ότι η κυκλοφορία του χρήστη δεν τροποποιείται κατά τη διάρκεια της διαμετακόμισης.
- Ενισχύει την προστασία της ιδιωτικότητας με τη χρήση ζευγών δημόσιων/ιδιωτικών κλειδιών (anchor keys ή κλειδιά άγκυρας) για την απόκρυψη της ταυτότητας του συνδρομητή και την εξαγωγή κλειδιών που χρησιμοποιούνται σε όλη την αρχιτεκτονική της υπηρεσίας.

7.2.2 Ακεραιότητα δεδομένων σηματοδοσίας

Το 5G εισάγει ένα νέο στοιχείο αρχιτεκτονικής δικτύου: τον μεσάζοντα προστασίας ακραίων σημείων ασφαλείας (Security Edge Protection Proxy). Το SEPP προστατεύει την άκρη του οικιακού δικτύου, ενεργώντας ως πύλη ασφαλείας στις διασυνδέσεις μεταξύ οικιακού δικτύου και των δικτύων επίσκεψης, όπως απεικονίζεται στην Εικόνα 7.2.



Εικόνα 7.2: Η αρχιτεκτονική του SEPP [7.30]

Το SEPP έχει σχεδιαστεί για να:

- Παρέχει ασφάλεια επιπέδου εφαρμογής και προστασία από επιθέσεις υποκλοπής και αναπαραγωγής (eavesdropping and replay attacks).
- Παρέχετε από άκρο σε άκρο έλεγχο ταυτότητας, προστασία ακεραιότητας και εμπιστευτικότητας μέσω υπογραφών και κρυπτογράφησης όλων των μηνυμάτων περιαγωγής HTTP/2.

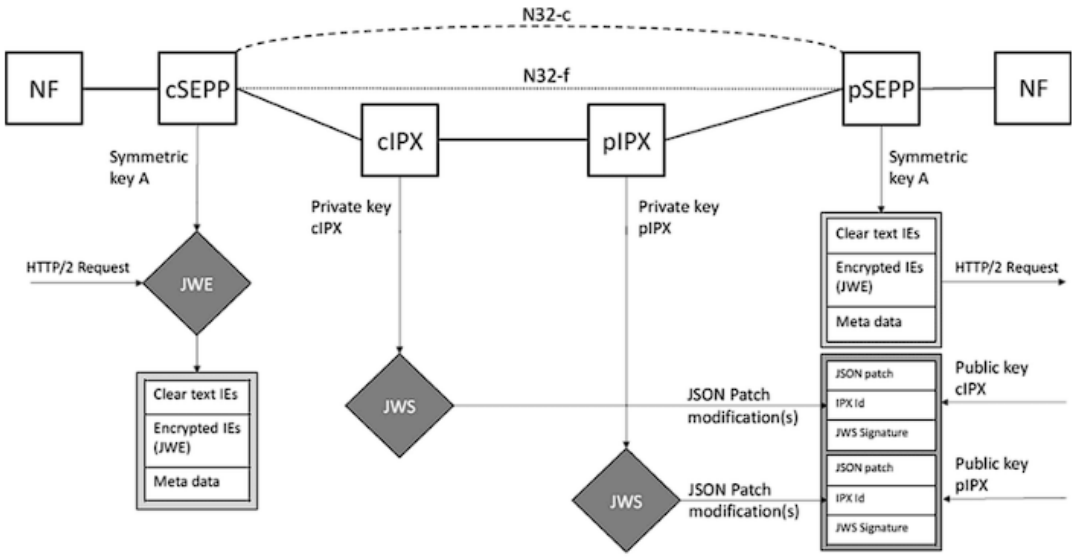
- Προσφέρει μηχανισμούς διαχείρισης κλειδιών για τον καθορισμό των απαιτούμενων κρυπτογραφικών κλειδιών ενώ παράλληλα εκτελεί τις διαδικασίες διαπραγμάτευσης των δυνατοτήτων ασφαλείας.
- Εκτελεί φιλτράρισμα και αστυνόμευση μηνυμάτων, απόκρυψη τοπολογίας και επικύρωση αντικειμένων JSON· συμπεριλαμβανομένου του ελέγχου πληροφοριών σε πολλαπλά επίπεδα με πληροφορίες διευθύνσεων στο επίπεδο IP.

Παράλληλα, εισάγει ενισχυμένη ασφάλεια των υπηρεσιών διεθνούς περιαγωγής για να ξεπεραστούν οι υφιστάμενοι κίνδυνοι ασφαλείας που συνδέονται με τη χρήση SS7 και Diameter. Αυτή η εισαγωγή ενός αποκλειστικού κόμβου ασφαλείας στα πρότυπα 5G αποτελεί σημαντική βελτίωση σε σχέση με τις υφιστάμενες πρακτικές στα δίκτυα 4G/3G/2G που χρησιμοποιούν SS7 και Diameter. Το Diameter χρησιμοποιείται σε μεγάλο βαθμό στις τελευταίες εκδόσεις του 3GPP (3rd Generation Partnership Project) για υπηρεσίες AAA (Authentication, Authorization and Accounting), ενώ το SS7 χρησιμοποιήθηκε αρχικά στα δίκτυα PSTN (public switched telephone network) και GSM (Global System for Mobile communication) για ψηφιακή σηματοδοσία μεταξύ διαφορετικών κόμβων για τη διαχείριση κλήσεων και άλλων υπηρεσιών.

Επιπλέον πολλά πρωτόκολλα πληροφορικής θα συμβάλουν στην εξέλιξη και την εδραίωση του 5G. Πολλά από αυτά είναι ήδη βασικά στοιχεία του διαδικτύου σήμερα και άλλα θα τα γνωρίσουμε για πρώτη φορά, μιας και δημιουργήθηκαν συγκεκριμένα για αυτό το σκοπό. Ιστορικά, τα δίκτυα φορέων εκμετάλλευσης χρησιμοποιούσαν κυρίως ιδιόκτητα πρωτόκολλα για τη διαχείριση του δικτύου. Το 5GC (5G Core) κινείται προς μια στοίβα πρωτοκόλλων βασισμένη σε IP, επιτρέποντας τη διαλειτουργικότητα με μεγαλύτερο αριθμό υπηρεσιών και τεχνολογιών στο μέλλον. Τα ακόλουθα πρωτόκολλα, σχήματα και διαδικασίες θα υιοθετηθούν στο 5GC:

- HTTP/2 μέσω N32 (διεπαφή προώθησης μεταξύ των SEPP), αντικαθιστώντας το Diameter μέσω του σημείου αναφοράς S6a (Το S6a είναι μια διεπαφή που σχετίζεται με την κινητή τηλεφωνία LTE 4G μεταξύ της MME και του HSS και χρησιμοποιείται για την πιστοποίηση ταυτότητας, την τοποθεσία και τις πληροφορίες υπηρεσίας σχετικά με τον συνδρομητή). Ένα πλήρες παράδειγμα τέτοιων διασυνδέσεων δίνεται στην Εικόνα 7.3, το οποίο παράδειγμα μπορείτε να δείτε και να διαβάσετε επεξηγηματικά στην σελίδα η οποία δίνεται στην δικτυογραφία [7.31] και [7.32].

- TLS (Transport Layer Security) ως πρόσθετο επίπεδο προστασίας που παρέχει κρυπτογραφημένη επικοινωνία μεταξύ όλων των λειτουργιών δικτύου (network function, NF) εντός ενός δημόσιου δικτύου κινητής τηλεφωνίας (public land mobile network, PLMN).
- TCP (Transmission Control Protocol) ως πρωτόκολλο επιπέδου μεταφοράς σε αντικατάσταση του πρωτοκόλλου μεταφοράς SCTP (Stream Control Transmission Protocol).
- Πλαίσιο RESTful (Representational state transfer) με OpenAPI 3.0.0+ (Το OpenAPI είναι μια διεπαφή προγραμματισμού εφαρμογών που διατίθεται δημόσια στους προγραμματιστές λογισμικού. Τα ανοικτά API δημοσιεύονται στο διαδίκτυο και διαμοιράζονται ελεύθερα, επιτρέποντας στον ιδιοκτήτη μιας υπηρεσίας με πρόσβαση στο δίκτυο να παρέχει καθολική πρόσβαση στους καταναλωτές) ως γλώσσα ορισμού διεπαφών (Interface Definition Language, IDL).



Εικόνα 7.3: Διασυνδέσεις μεταξύ προηγουμένων αναφερόμενων τεχνολογιών [7.31]

Καθώς αυτά τα πρωτόκολλα χρησιμοποιούνται στον ευρύτερο κλάδο της πληροφορικής, η χρήση τους θα είναι πιθανών να:

- Οδηγήσει σε ένα σύντομο χρονικό διάστημα μεταξύ ευπάθειας και εκμετάλλευσης και σε μεγαλύτερο αντίκτυπο των ευπαθειών που εντοπίζονται σε αυτά τα πρωτόκολλα.

- Επέκταση της δυνητικής ομάδας επιτιθέμενων. Τα δίκτυα τα οποία έχουν ως πύρινα τα 4G και ιδίως τα δίκτυα 3G επωφελούνται από το γεγονός ότι οι επιτιθέμενοι έχουν μικρή εμπειρία με τα ιδιόκτητα πρότυπα που χρησιμοποιούνται σε αυτά.

Τα συστήματα αναφοράς ευπαθειών, όπως το πρόγραμμα συντονισμένης αποκάλυψης ευπαθειών (Coordinated Vulnerability Disclosure, CVD) του GSMA (Global System for Mobile Communications), θα πρέπει να διαχειριστούν το αυξημένο πεδίο εφαρμογής αυτών των πρωτοκόλλων. Μόλις εντοπιστούν, ο χρόνος για την επιδιόρθωση των σχετικών ευπαθειών θα πρέπει να είναι σύντομος.

7.2.3 Τεχνολογίες που αξιοποιούνται από το 5G

Το 5G καθώς εγκαθιστάτε στη ζωή μας θα αναπτύξει παράλληλα πολλά υπάρχοντα στοιχεία τα οποία είναι ήδη σε χρήση. Παρακάτω θα αναφερθούν μερικά από αυτά. Το κείμενο είναι ένα συνονθύλευμα πληροφοριών συγκεντρωμένες από τις σελίδες [7.30] και [7.32], δύο εξαιρετικές πηγές για εμβάθυνση επάνω στο 5G. Οι τεχνολογίες αυτές παρατίθενται ως εξής:

1. Εικονικοποίηση (Virtualization), η αρχιτεκτονική του δικτύου 5GC θα βασίζεται σε υπηρεσίες, πράγμα που σημαίνει ότι οι λειτουργίες του κεντρικού δικτύου μπορούν να εκτελούνται μέσω λειτουργιών εκτός του δικτύου φορέα εκμετάλλευσης, π.χ. μέσω του νέφους. Πρόκειται για μια σημαντική στροφή από τους καθιερωμένους ελέγχους ασφαλείας του κεντρικού δικτύου, ωστόσο προσφέρει στον φορέα εκμετάλλευσης την ευκαιρία να αξιοποιήσει τεχνολογίες εικονικοποίησης. Με αυτή την ευκαιρία έρχονται νέοι φορείς απειλών που πρέπει να αντιμετωπιστούν. Θα πρέπει να εξεταστούν οι παραδοσιακοί έλεγχοι εικονικοποίησης, συμπεριλαμβανομένης της απομόνωσης μισθωτών και πόρων (tenant - ο μισθωτής είναι η πιο θεμελιώδης κατασκευή ενός περιβάλλοντος SaaS. Ως πάροχος SaaS που κατασκευάζει μια εφαρμογή, κάνετε την εφαρμογή αυτή διαθέσιμη στους πελάτες σας. Οι πελάτες που εγγράφονται για να χρησιμοποιήσουν το περιβάλλον σας αντιπροσωπεύονται ως ενοικιαστές του συστήματός σας - and resource isolation). Οι κατάλληλοι έλεγχοι απομόνωσης μειώνουν τον κίνδυνο διαρροής δεδομένων και τον αντίκτυπο των επιδημιών κακόβουλου λογισμικού που γνωρίζουν την εικονικοποίηση.

Οι ευπάθειες σε επίπεδο μικροεπεξεργαστή (Microprocessor), π.χ. Spectre και Meltdown (ευπάθειες των σύγχρονων υπολογιστών προκαλούν διαρροή κωδικών πρόσβασης και ευαίσθητων δεδομένων), έχουν επισημάνει ότι η απομόνωση των μισθωτών σε ένα εικονικό περιβάλλον δεν είναι εγγυημένη, καθώς οι μισθωτές θα πρέπει να στεγάζονται μαζί με βάση τις απαιτήσεις ασφαλείας, π.χ. μην στεγάζετε μισθωτές χαμηλότερου επιπέδου ασφαλείας με μισθωτές υψηλού επιπέδου ασφαλείας.

Η εμπορευματοκιβωτιοποίηση είναι μια τεχνολογία εικονικοποίησης σε επίπεδο λειτουργικού συστήματος που κερδίζει συνεχώς έδαφος. Το λειτουργικό σύστημα του κεντρικού υπολογιστή περιορίζει την πρόσβαση του εμπορευματοκιβωτίου σε φυσικούς πόρους, όπως η CPU, ο αποθηκευτικός χώρος και η μνήμη, έτσι ώστε ένα μεμονωμένο εμπορευματοκιβώτιο να μην μπορεί να καταναλώσει όλους τους φυσικούς πόρους ενός κεντρικού υπολογιστή. Ως εκ τούτου, μειώνεται ο αντίκτυπος των επιθέσεων διαθεσιμότητας κατά της πλατφόρμας. Τα εμπορευματοκιβώτια συχνά εκτελούνται ως root και ως εκ τούτου είναι δυνατή η διαφυγή από το εμπορευματοκιβώτιο και η πρόσβαση στο υποκείμενο σύστημα αρχείων. Η δικτύωση καθορισμένη από λογισμικό (Software defined networking, SDN) παρέχει στους φορείς εκμετάλλευσης την ευκαιρία να εικονικοποιήσουν τις ροές του δικτύου τους, οδηγώντας σε απλούστευση του υλικού.

Όλες οι τεχνολογίες εικονικοποίησης επιτρέπουν την τμηματοποίηση του δικτύου και την απομόνωση των πόρων, διασφαλίζοντας την ασφάλεια και μειώνοντας τον αντίκτυπο των επιτυχημένων επιθέσεων. Η διαμόρφωση αυτών των υπηρεσιών θα πρέπει να πραγματοποιείται με το ήθος της ασφάλειας κατά το σχεδιασμό, ώστε να διασφαλίζεται ότι η προσφερόμενη προστασία δεν ακυρώνεται από κακές διαδικασίες διαχείρισης και ενορχήστρωσης (management and orchestration processes, MANO). Το κεντρικό σύστημα ελέγχου, συχνά ο hypervisor, λειτουργεί ως εγκέφαλος των εικονικοποιημένων τεχνολογιών. Ως εκ τούτου, η προστασία αυτής της υποκείμενης τεχνολογίας θα πρέπει να είναι υψηλή. Θα πρέπει να ολοκληρωθεί ειδική μοντελοποίηση απειλών για επιθέσεις και ευπάθειες που σχετίζονται με την εικονικοποίηση ώστε να είμαστε προετοιμασμένοι για κάθε είδους απειλή, μιας και η εικονικοποίηση επρόκειτο να γίνει μια από τις βάσεις του 5G σήμερα.

2. Υπηρεσίες Cloud (Cloud Services), βασιζόμενο σε εικονικές υπηρεσίες, το νέφος αποτελεί βασικό παράγοντα για το 5G, η αρχιτεκτονική του 5G έχει σχεδιαστεί ώστε να είναι εγγενής στο νέφος, καθώς προσφέρει ελαστικότητα και επεκτασιμότητα. Η χρήση της τεχνολογίας νέφους μπορεί να περιπλέξει την αλυσίδα εφοδιασμού και την αλυσίδα ευθύνης. Σύμφωνα με το Mobile World Live, το 5G επιτρέπει στους φορείς εκμετάλλευσης να εκθέτουν πλούσιες υπηρεσίες μέσω του Cloud και των Restful API. Θα πρέπει να ακολουθούνται ασφαλείς πρακτικές κωδικοποίησης, ώστε να διασφαλίζεται ότι τα δεδομένα δεν διαρρέουν και ότι ο κώδικας δεν μπορεί να χρησιμοποιηθεί για την εκμετάλλευση του παρόχου cloud ή του δικτύου του φορέα εκμετάλλευσης.

3. Τεμαχισμός δικτύου (Network Slicing), η τμηματοποίηση του δικτύου επιτρέπει στον φορέα εκμετάλλευσης να προσαρμόζει τη συμπεριφορά του δικτύου, προσαρμόζοντας (τμηματοποιώντας) το δίκτυο για την εξυπηρέτηση συγκεκριμένων περιπτώσεων χρήσης χρησιμοποιώντας το ίδιο υλικό. Η GSMA έχει ορίσει 35 χαρακτηριστικά που χαρακτηρίζουν μια φέτα δικτύου στο Μόνιμο Έγγραφο Αναφοράς (Permanent Reference Document, PRD, NG.116).

   Το μοντέλο ασφάλειας για κάθε φέτα (slice) θα πρέπει να προσαρμόζεται στην περίπτωση χρήσης. Μπορούν να προβλεφθούν διαφορετικά επίπεδα απομόνωσης που εκτείνονται από έναν μόνο κόμβο του κεντρικού δικτύου έως την πλήρως αποκλειστική ραδιοπρόσβαση (radio access). Κάθε τύπος απομόνωσης πρέπει να ενσωματωθεί στη φάση σχεδιασμού. Για παράδειγμα, ένα slice δικτύου για απομακρυσμένες χειρουργικές επεμβάσεις πρέπει να εξετάζει τη συνεχή αμοιβαία ταυτοποίηση και εξουσιοδότηση για να σταματήσει τις απειλές MITM (man-in-the-middle), αλλά ένα slice για τη διαχείριση περιεχομένου AR/VR δεν θα απαιτεί το ίδιο επίπεδο ασφάλειας.

4. Κινητό IoT (Mobile IoT), αν και το IoT είναι ήδη διαδεδομένο στα δίκτυα 2G/3G/4G, ο αριθμός των συνδέσεων IoT αναμένεται να αυξηθεί εκθετικά στο 5G. Το μεγαλύτερο δεν σημαίνει ότι οι έλεγχοι ασφαλείας πρέπει να αλλάξουν σημαντικά, ωστόσο πρέπει να κλιμακωθούν. Το IoT πρέπει να κωδικοποιείται, να αναπτύσσεται και να διαχειρίζεται με ασφάλεια καθ' όλη τη διάρκεια του κύκλου ζωής του.

Οι περισσότερες υπηρεσίες IoT μοιράζονται μια κοινή αρχιτεκτονική και ως εκ τούτου οι επιθέσεις που θα δεχθεί κάθε υπηρεσία είναι πιθανό να εντάσσονται σε τρία κοινά σενάρια επιθέσεων:

- Επιθέσεις στις συσκευές (τελικά σημεία) μέσω των εφαρμογών που εκτελούνται στη συσκευή, απομακρυσμένες επιθέσεις από το διαδίκτυο και φυσικές επιθέσεις.
- Επιθέσεις στις πλατφόρμες υπηρεσιών (π.χ. το νέφος)
- Επιθέσεις στις ζεύξεις επικοινωνίας (π.χ. κινητή τηλεφωνία, WLAN, διεπαφή αέρα BLE - BLE air interface - κ.λπ.)

Στο εξερχόμενο σκέλος, οι συσκευές IoT αξιοποιούνται όλο και περισσότερο για την εξαπόλυση επιθέσεων DDoS (Distributed Denial-of-Service), καθώς κάθε συσκευή δημιουργεί κάποια μορφή δεδομένων, γεγονός που σε συνδυασμό με τον όγκο των συσκευών οδηγεί σε σημαντικές επιθέσεις με βάση τον όγκο.

5. eSIM: η eSIM εξαλείφει την ανάγκη για αφαιρούμενη κάρτα SIM στην κινητή συσκευή, ενώ τα δεδομένα της κάρτας αυτής προετοιμάζονται σε μια απομακρυσμένη πλατφόρμα παροχής SIM (SM-DP+, Subscription Management Root-Discovery Service και χρησιμοποιείται για τη σύνδεση των συσκευών των καταναλωτών eSIM με ένα δίκτυο κινητής τηλεφωνίας της επιλογής του χρήστη) και στη συνέχεια μεταφορτώνονται με τη μορφή προφίλ eSIM μέσω HTTPS σε ένα ασφαλές στοιχείο (eUICC, embedded universal integrated circuit card, το λογισμικό που επιτρέπει την απομακρυσμένη παροχή SIM πολλαπλών προφίλ δικτύου.) που είναι μόνιμα ενσωματωμένο στην κινητή συσκευή.

   Αυτό το eUICC, που αναγνωρίζεται από ένα παγκοσμίως μοναδικό EID (Electronic IDentification), είναι σε θέση να αποθηκεύσει πολλά προφίλ, και όταν ένα προφίλ είναι ενεργοποιημένο, τα δεδομένα στο εν λόγω προφίλ χρησιμοποιούνται για την ταυτοποίηση και τον έλεγχο ταυτότητας του συνδρομητή στο δίκτυο κινητής τηλεφωνίας με τον ίδιο τρόπο που θα το έκανε μια αφαιρούμενη κάρτα SIM. Το σύστημα χρησιμοποιεί πιστοποιητικά υποδομής δημόσιου κλειδιού (Public Key Infrastructure, PKI) που επιτρέπουν στο SM-DP+ και στο eUICC να πιστοποιούν αμοιβαία ο ένας τον άλλον. Όλα τα κλειδιά παράγονται με Perfect Forward Secrecy (PFS). Στην κρυπτογραφία, η μυστικότητα προς τα εμπρός (forward secrecy), επίσης γνωστή ως τέλεια μυστικότητα προς τα εμπρός

(perfect forward secrecy), είναι ένα χαρακτηριστικό συγκεκριμένων πρωτοκόλλων συμφωνίας κλειδιών που παρέχει διαβεβαιώσεις ότι τα κλειδιά συνόδου (session keys) δεν θα παραβιαστούν ακόμη και αν παραβιαστούν τα μακροπρόθεσμα μυστικά που χρησιμοποιούνται στην ανταλλαγή αυτών των κλειδιών συνόδου. Η διαχείριση των προφίλ eSIM στο eUICC πραγματοποιείται από τον τελικό χρήστη στην περίπτωση χρήσης από καταναλωτές ή από μια απομακρυσμένη πλατφόρμα παροχής sim στην περίπτωση χρήσης M2M/IoT.

6. Τεχνητή νοημοσύνη (Artificial Intelligence AI), αν και πρόκειται για έναν όρο ομπρέλα (umbrella term, ένας όρος που χρησιμοποιείται για να καλύψει μια ευρεία κατηγορία πραγμάτων και όχι ένα συγκεκριμένο αντικείμενο) για πολλές τεχνολογίες, η τεχνητή νοημοσύνη αναμένεται να χρησιμοποιηθεί ευρέως στα δίκτυα 5G και θα ωφελήσει την ασφάλεια. Οι φορείς εκμετάλλευσης θα πρέπει να αξιοποιήσουν τη μηχανική μάθηση (ML) και τη βαθιά μάθηση (DL) για την αυτοματοποίηση της ανίχνευσης απειλών και απάτης. Η χρήση του AI είναι ιδιαίτερα σημαντική όταν λαμβάνεται υπόψη ο όγκος των δεδομένων που θα παράγουν τα δίκτυα 5G. Η τεχνητή νοημοσύνη θα ενισχύσει τον μετριασμό προηγούμενων άγνωστων επιθέσεων σε πραγματικό χρόνο. Το AI μπορεί να χρησιμοποιηθεί για την τροφοδοσία δικτύων αυτοθεραπείας, όπου το σύστημα είναι σε θέση να εντοπίζει προβλήματα και να αναλαμβάνει αυτοματοποιημένη δράση για την παροχή της διόρθωσης. Ωστόσο, αυτή η τεχνολογία είναι επίσης διαθέσιμη στον επιτιθέμενο και αναμένονται επιθέσεις με βάση του AI.

Σκοπός του 5G είναι να ανοίξει το δίκτυο σε ένα ευρύτερο σύνολο υπηρεσιών και να επιτρέψει στους φορείς εκμετάλλευσης κινητής τηλεφωνίας να στηρίξουν αυτές τις υπηρεσίες. Είναι μια ευκαιρία για την προστασία των υπηρεσιών και των καταναλωτών από πολλές από τις σημερινές απειλές. Το 5G έρχεται με πολλούς ενσωματωμένους ελέγχους ασφαλείας εκ κατασκευής, οι οποίοι αναπτύχθηκαν για να ενισχύσουν την προστασία τόσο των μεμονωμένων καταναλωτών όσο και των δικτύων κινητής τηλεφωνίας. Η πρόοδος της τεχνολογίας και η χρήση νέων αρχιτεκτονικών και χαρακτηριστικών, όπως η τμηματοποίηση του δικτύου, η εικονικοποίηση και το νέφος, θα εισάγουν νέες απειλές που απαιτούν την εφαρμογή νέων τύπων ελέγχων.

8 Συμπεράσματα

Στη συγκεκριμένη εργασία αναφέρθηκαν νέες εξελίξεις οι οποίες πλημμυρίζουν τον κόσμο καθημερινά, καθώς και τα δεδομένα τα οποία υπήρχαν πριν από αυτές, και κυρίως δόθηκε έμφαση στις αδυναμίες και τους κινδύνους οι οποίοι θα αποτελέσουν σημαντικά σημεία στα οποία χρειάζεται να αναπτυχθεί ιδιαίτερη προσοχή. Επιπλέον σχολιάστηκαν τα βήματα που μπορούν να ακολουθηθούν έτσι ώστε οι χρήστες αλλά και οι δημιουργοί αυτών των νέων, επαναστατικών τεχνολογιών να αναπτύξουν ασφαλή περιβάλλοντα.

Η κυριότερη δυσκολία που αντιμετωπίσθηκε, ήταν το γεγονός πως κατά τη διάρκεια της δημιουργίας αυτής της εργασίας τα δεδομένα, στον τομέα αυτών των τεχνολογιών, μεταβάλλονταν συνεχώς, με νέες εξελίξεις και νέες προσθέσεις που εμφανίζονταν κατά τη συγγραφή. Με τον αυτόν τρόπο, η παραγωγή έπρεπε να γίνεται έτσι ώστε ενώ εξελίσσεται η εργασία παράλληλα να προστίθενται νέα δεδομένα στα ήδη υπάρχοντα «ολοκληρωμένα» κεφάλαια τα οποία είχαν δημιουργηθεί, ή ακόμη και να αφαιρούνται στοιχεία τα οποία δεν ήταν πλέον σε ισχύ. Η υιοθέτηση μίας τεχνικής όπως αυτή που περιγράφεται αποδείχθηκε εξαιρετικά κουραστική μιας και η ταυτόχρονη ενημέρωση σχετικά με τα θέματα για τα οποία αναπτύσσονται αλλά και για αυτά τα οποία είχαν ήδη διατυπωθεί μείωσε σε έναν αξιοπρεπή βαθμό την παραγωγικότητα.

Όσον αφορά τον συγγραφέα, εάν είχε την δυνατότητα να ξεκινήσει ξανά σήμερα, πιθανότατα δεν θα άλλαζε πολλά, εάν όμως ξεκινούσε σε λίγους μήνες από τώρα, ίσως να επέλεγε το 6G ως βασικό νέο δίκτυο, μιας και αυτή τη στιγμή που ολοκληρώνεται αυτή η εργασία, έχει ξεκινήσει η μελέτη με σκοπό τη δημιουργία του τον επόμενο καιρό. Με τον ρυθμό που βαίνουν τα δεδομένα σήμερα, είναι σίγουρο πως δεν θα αργήσει η στιγμή στην οποία τα κινητά θα αναγράφουν στο εικονίδιο του σήματος τους χαρακτήρες “6G”.

Ήταν μια εξαιρετική εμπειρία (ελπίζω εσείς, ως αναγνώστες να έχετε την ίδια εντύπωση) η οποία προσέφερε γνώσεις και κυρίως όπλισε με ότι είναι αναγκαίο να γνωρίζει ο μέσος άνθρωπος ώστε στο μέλλον να μπορεί να αντιμετωπίσει αλλά κατά κόρων να προφυλαχτεί από κινδύνους οι οποίοι ελλοχεύουν σε κάθε γωνιά του διαδικτύου. Είναι σίγουρο πως και οι αναγνώστες αυτής της εργασίας θα καταφέρουν εξίσου δυναμικά να προφυλαχτούν απέναντι στους ανερχόμενους κινδύνους.

Βιβλιογραφία - Δικτυογραφία

[1] Αναγνωστόπουλος: Από το διαθέσιμο αρχείο του πανεπιστημίου Αθηνών, παρμένες πληροφορίες, κείμενο και η Εικόνα 2.2

[2] Brainbridge, “From 1G to 5G: A Brief History of the Evolution of Mobile Standards”

[3] Πρωτότυπο κείμενο περί IoT του Peter T. Lewis: “The Internet of Things, or IoT, is the integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such devices.”

[4] Πρωτότυπο κείμενο περί IoT και 5G του Matt Young: “These use cases illustrate the benefits of private wireless in a port or intermodal terminal operation”

[5] Πληροφορίες και λεπτομέρειες χρήσης τεχνολογιών του IoT και 5G στους αερολιμένες | Άρθρο στην σελίδα ACI Insights του Μιχάλης Σενή (Michalis Senis) Ηλεκτρολόγου Μηχανικού και Μηχανικού Πληροφορικής με πολυετή εμπειρία στην έναρξη και λειτουργία συστημάτων ICT αεροδρομίων.

[6] Πληροφορίες και λεπτομέρειες χρήσης τεχνολογιών του IoT και 5G για την αναβάθμιση της ποιότητας ζωής ανθρώπων με αναπηρίες | Άρθρο του Aqeel Qureshi, ιδρυτή και CEO της Techbility, στη σελίδα Disability Insider.

[7] Σύνδεσμοι για αναφορές τεχνολογιών, εικόνων ή ορισμών που υπάρχουν στο κείμενο (ταξινομημένες με σειρά αναφοράς στο κείμενο) διαθέσιμες στην αντιπροσωπευτική τους σελίδα, εάν αυτή υπάρχει, ειδάλλως στο Wikipedia:

[7.1] CBCF | https://www.cbcfinc.org/

[7.2] Auto-ID Labs | https://www.autoidlabs.org/

[7.3] GSM | https://en.wikipedia.org/wiki/GSM

[7.4] M2MI | https://www.m2mi.com/

[7.5] NYU WIRELESS | https://wireless.engineering.nyu.edu/

[7.6] Εικόνα 2.1 | https://www.researchgate.net/

[7.7] Διάχυτος υπολογισμός - Ubiquitous computing | https://en.wikipedia.org/wiki/Ubiquitous_computing

[7.8] Μηχανική Μάθηση - Machine Learning | https://en.wikipedia.org/wiki/Machine_learning

[7.9] Υπολογιστικό νέφος - Cloud Computing | https://en.wikipedia.org/wiki/Cloud_computing

[7.10] Αναφορές και λεπτομέρειες για τις εφαρμογές του IoT | https://studiousguy.com/

[7.11] Εικόνα 3.1 | https://www.eco-sense.info/

[7.12] LoRaWAN network & Εικόνα 3.2| https://lora-alliance.org/

[7.13] Ρομπότ στη γεωργία | https://www.cropin.com/

[7.14] Αναφορές και λεπτομέρειες για τις εφαρμογές του 5G | https://www.techtarget.com/

[7.15] Εικόνα 4.1 | https://www.edn.com/

[7.16] Εικόνα 4.2 | https://stlpartners.com/

[7.17] Αναφορές και ιδέες για χρήσης του IoT με 5G | https://cloudblogs.microsoft.com/

[7.18] https://www.5gradar.com/ https://www.porttechnology.org/

[7.19] Εικόνα 5.1 | https://www.interlakemecalux.com/

[7.20] Εικόνα 5.2 | https://www.gartner.com/

[7.21] Εικόνα 5.3 και λεπτομέρειες τεχνολογιών για ανθρώπους με αναπηρίες | https://news.microsoft.com/

[7.22] Έρευνα αδυναμίας νοσοκομείων στο IoT | https://www.cynerio.com/

[7.23] Στατιστικά περί IoT στον τομέα των Utilities | https://internetofbusiness.com/

[7.24] Πληροφορίες σχετικά με τις αδυναμίες του 5G | https://www.networkcomputing.com/

[7.25] Πληροφορίες σχετικά με τις αδυναμίες του 5G σύμφωνα με την Ε.Ε. | https://www.enisa.europa.eu/

[7.26] Έρευνα των CISA και DoD για την αδυναμίες και τρόπους αντιμετώπισης αυτών όσον αφορά το 5G | https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

[7.27] Πληροφορίες και κείμενο από το Γραφείο Εκδόσεων της Ε.Ε. (Publications Office of the European Union) όπως και η εικόνα 6.2 | https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/el/index.html#chapter1

[7.28] Εικόνα 7.1 | https://pelaxa.com/cat/blog/random-thoughts/

[7.29] Πληροφορίες και κείμενο για τους τρόπους ασφάλισης του IoT | https://www.techtarget.com/ https://www.computer.org/ https://www.kelltontech.com/

[7.30] Εικόνα 7.2 και πληροφορίες σχετικά με την ασφάλεια του 5G | https://www.gsma.com/

[7.31] Εικόνα 7.3 και πληροφορίες για αυτή | https://www.researchgate.net/

[7.32] Πληροφορίες για το N32 | https://docs.oracle.com/