ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Διανεμημένα Πρωτόκολλα Ασφαλείας για το Διαδίκτυο των Πραγμάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΓΙΩΡΓΟΣ ΒΛΑΧΟΔΗΜΗΤΡΟΠΟΥΛΟΣ

Επιβλέπων : Συμεών Παπαβασιλείου

Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2018

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Διανεμημένα Πρωτόκολλα Ασφαλείας για το Διαδίκτυο των Πραγμάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΓΙΩΡΓΟΣ ΒΛΑΧΟΔΗΜΗΤΡΟΠΟΥΛΟΣ

Επιβλέπων : Συμεών Παπαβασιλείου
Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 29η Ιουνίου 2018.

……	……..	……...
Συμεών Παπαβασιλείου	Θεοδώρα Βαρβαρίγου	Ιωάννα Ρουσσάκη
Καθηγητής Ε.Μ.Π.	Καθηγήτρια Ε.Μ.Π	Καθηγήτρια Ε.Μ.Π.

Αθήνα, Ιούνιος 2018

Γιώργος Βλαχοδημητρόπουλος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Αποτελεί πραγματικότητα το γεγονός ότι διανύουμε μία μεταβατική περίοδο όσον αφορά τις τεχνολογίες διαδικτύου και τα πρωτόκολλα ασφαλείας των επικοινωνιών. Το υπάρχον status quo είναι υπό ξεκάθαρη αμφισβήτηση. Εμείς, ως μηχανικοί του κλάδου έχουμε την υποχρέωση τόσο απέναντι στο αντικείμενο όσο και απέναντι στους εαυτούς μας να ξεπεράσουμε την ανασφάλεια που προκαλεί η αδράνεια της αλλαγής. Σε αυτό το πλαίσιο αποτελεί ανάγκη η ενασχόληση, με πιο κλινικό βλέμμα, των τεχνολογιών του Διαδικτύου των Πραγμάτων και του Blockchain.

Μπορούμε πλέον να οραματιστούμε ένα όχι και τόσο μακρινό μέλλον στο οποίο κάθε συσκευή θα αποτελεί κόμβο ενός τεράστιου δικτύου ανταλλαγής και αποθήκευσης πληροφοριών, του γνωστού και ως Διαδικτύου των Πραγμάτων (IOT). Η συνδεσιμότητα ως συνέπεια της ύπαρξης αυτού του δικτύου γεννά μια πληθώρα προοπτικών βελτίωσης της εμπειρίας του μέσου ανθρώπου στην επαφή του με όλα τα εργαλεία software και hardware.

Η νέα αυτή πραγματικότητα, ωστόσο, εμφανίζεται με το αντίστοιχο κόστος της αλλαγής. Η ύπαρξη αυτού του δικτύου γεννά ένα πλήθος νέων ζητημάτων όσον αφορά τις δομές αποθήκευσης πληροφορίας και την ασφάλεια. Τα υπάρχοντα πρωτόκολλα δεν αρκούν ώστε να καλύψουν τις νέες ανάγκες. Η ρηξικέλευθη τεχνολογία του Blockchain είναι πολλά υποσχόμενη για να καλύψει τα κομμάτια του puzzle της ασφάλειας που λείπουν.

Το κίνητρο αυτής της διπλωματικής εργασίας υπήρξε , κατά πρώτον, η επισκόπηση του Διαδικτύου των Πραγμάτων και των θεμάτων ασφαλείας που προκύπτουν από την υλοποίησή του και κατά δεύτερον, πώς η νέα τεχνολογία του Blockchain μπορεί να προσφέρει λύσεις σε κάποια από αυτά.

Λέξεις κλειδιά

Διαδίκτυο των Πραγμάτων, IoT, ασφάλεια, δίκτυο, απειλές, blockchain

Abstract

It is a fact that we are in a transition period with regard to Internet technologies and communications security protocols. The existing status quo is clearly under discussion. We, as engineers in the industry, have a duty both to object and to ourselves to overcome the insecurity caused by the inertia of change. In this context, it is necessary to engage, with a more clinical look, on the Internet of Things and Blockchain technologies.

We can now envision a not too distant future in which each device will be a hub of a huge network of information exchange and storage, known as the Internet of Things (IOT). Connectivity as a consequence of the existence of this network generates a wealth of prospects for improving the average man's experience in touching all the software and hardware tools.

This new reality, however, appears with the corresponding cost of change. The existence of this network raises a number of new issues regarding information storage structures and security. Existing protocols are not enough to meet new needs. Blockchain's groundbreaking technology is promising to cover the pieces that are missing from the security puzzle.

The motivation for this diplomatic work was, first of all, the review of the Internet of Things and security issues that emerged from its implementation, and secondly, how Blockchain's new technology can offer solutions to some of them.

Key words

Internet of Things, IoT, security, network, threats, blockchain

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο του προπτυχιακού προγράμματος σπουδών της Σχολής Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου. Μέσω αυτής είχα τη δυνατότητα να διευρύνω τις γνώσεις μου πάνω στο Διαδίκτυο των πραγμάτων καθώς και τη λειτουργία του Blockchain. Το γεγονός αυτό αποτέλεσε το βασικό ερέθισμα για τον επαγγελματικό μου προσανατολισμό. Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου Πρωτονοτάριο Εμμανουήλ, για την δυνατότητα που μου προσέφερε να εργαστώ πάνω στον τομέα της ασφάλειας του διαδικτύου των πραγμάτων, καθώς και για τις πολύτιμες συμβουλές του καθόλη τη διάρκεια των μαθημάτων και της εκπόνησης της διπλωματικής μου εργασίας. Παράλληλα θα ήθελα να ευχαριστήσω τους κ.κ. Συμεών Παπαβασιλείου, Καθηγητή Ε.Μ.Π, την Θεοδώρα Βαρβαρίγου,Καθηγήτρια Ε.Μ.Π, και την Ιωάννα Ρουσσάκη, Καθηγήτρια Ε.Μ.Π, που με τίμησαν με την παρουσία τους στην επιτροπή εξέτασης της διπλωματικής εργασίας. Θα ήθελα να ευχαριστήσω ξεχωριστά και τον κ. Νικόλαο Μπάκαλο, Ε.ΔΙ.Π Ε.Μ.Π. για την πολύτιμη βοήθεια του στην εκπόνηση της συγκεκριμένης εργασίας. Ο χρόνος που αφιέρωσε, η επιστημονική όσο και η πνευματική του στήριξη ήταν ιδιαίτερα σημαντικές κατά τη διάρκεια αυτής της πορείας. Τέλος, με εξίσου μεγάλη θέρμη θέλω να ευχαριστήσω την οικογένεια μου και τους φίλους μου, που ήταν δίπλα μου σε όλη τη διάρκεια της ακαδημαϊκής μου πορείας, ο καθένας με τον ξεχωριστό του τρόπο. Ιδιαιτέρως ευχαριστώ τον πατέρα μου, που ήταν ο λόγος που επέλεξα αυτή τη σχολή και την μητέρα μου, που ήταν ο λόγος που κατάφερα να μπω σε αυτή τη σχολή.

Γεώργιος Κ Βλαχοδημητρόπουλος,

Αθήνα, 29η Ιουνίου 2018

ΠΕΡΙΕΧΟΜΕΝΑ

Σελ.

1 Internet of Things

1.1 Το IoT

Η ραγδαία τεχνολογική εξέλιξη των τελευταίων ετών, σε συνδυασμό με την ευρεία διάδοση του Διαδικτύου, οδήγησε στην ανάπτυξη μιας νέας φιλοσοφίας του Internet of Things (IoT). Στην ουσία πρόκειται για τη δυνατότητα διασύνδεσης ατόμων, μηχανών, οικιακών συσκευών, απλών αντικειμένων και διαδικασιών, ώστε μέσω της μεταξύ τους επικοινωνίας και αλληλεπίδρασης να επιτυγχάνεται αυτοματισμός και ανταλλαγή δεδομένων, με τελική κατάληξη την αξιοποίηση όλων αυτών τόσο σε προσωπικό, σε επιχειρηματικό όσο και σε επαγγελματικό επίπεδο. Πλέον, οι νέες κατευθύνσεις είναι προς απελευθερωμένη δικτύωση από την ανθρώπινη παρέμβαση.

Πριν την αναλυτικότερη παρουσίασή του, κρίνεται σκόπιμο να ξεκαθαρίσουμε ότι ενώ ορισμένοι εξισώνουν τη νέα αυτή τεχνολογία με την επικοινωνία μηχανής με μηχανή (M2M), μια τέτοια ταύτιση δεν είναι σωστή.

Η επικοινωνία μεταξύ συσκευών ορίζεται ως οι τεχνολογίες που επιτρέπουν σε μηχανές, τυπικά (μικρούς) υπολογιστικούς αισθητήρες που εκτελούν ειδικά καθήκοντα (ευφυΐα), να επικοινωνούν ή να αναμεταδίδουν πληροφορίες που απαιτούνται, συνήθως μέσω απλών πρωτοκόλλων αλλά πιο πρόσφατα πάνω από το Πρωτόκολλο Διαδικτύου (IP) μέσω ασύρματης ή ενσύρματης επικοινωνίας, ακόμα και μέσω Υπηρεσίας Σύντομου Μηνύματος (SMS).

Όμως το Διαδίκτυο των Πραγμάτων είναι πολύ περισσότερο από την M2M τεχνολογία. Αφορά την αλληλεπίδραση με τα αντικείμενα γύρω μας, ακόμη και με στατικά μη-έξυπνα αντικείμενα και την αύξηση τέτοιων αλληλεπιδράσεων σε πλαίσια που παρέχονται από τη γεωγραφική θέση, το χρόνο και ούτω καθεξής. Ακόμα και μη-ευφυείς/μη-συνδεδεμένες συσκευές μπορούν να ενταχθούν στο IoT μέσω π.χ. ενός έξυπνου τηλεφώνου που λειτουργεί ως πύλη για το Διαδίκτυο. Έχει να κάνει, για παράδειγμα, με την αλληλεπίδραση μέσω barcode (γραμμικού κώδικα) με το βιβλίο που διαβάζουμε, μέσω NFC (Near Field Communication –Επικοινωνία κοντινού πεδίου) με μια αφίσα, ή με μια διαφήμιση σε εφημερίδα μέσω μικρού κώδικα. Έτσι, η M2M τεχνολογία δεν συνιστά το Διαδίκτυο των Πραγμάτων, αλλά είναι υποσύνολό του.(Ευφροσύνη Θ. Ζώτου, 2012)

1.1.1 Εισαγωγή στο IoT

Το Internet of Things (IoT) είναι το δίκτυο τών πραγμάτων δηλαδή το δίκτυο που αποτελείται από οικιακές συσκευές, φυσικές συσκευές, οχήματα, και άλλα αντικείμενα στα οποία έχουν ενσωματωθεί αισθητήρες, ενεργοποιητές, software, και πρόσβαση στο διαδίκτυο, γεγονός που επιτρέπει την διασύνδεση όλων αυτών των αντικειμένων και την ανταλλαγή δεδομένων μεταξύ τους. Κάθε αντικείμενο είναι μοναδικά αναγνωρισμένο λόγω του δικού του ενσωματωμένου δικτύου αλλά έχει τη δυνατότητα να αλληλεπιδρά μέσα στο υπάρχον δίκτυο. Το Internet of Things είναι μια λέξη-κλειδί για τον όρο "συνδεδεμένες συσκευές", που χρησιμοποιήσαμε τα τελευταία 15 χρόνια για να περιγράψουμε την τάση σύνδεσης των ενσωματωμένων συστημάτων. Προωθείται από την ανάγκη μεταφοράς της χρήσης ενσωματωμένων συσκευών στο επόμενο επίπεδο απόδοσης. Ενεργοποιώντας την απρόσκοπτη επικοινωνία μεταξύ όλων των ενσωματωμένων συσκευών, συλλέγουμε περισσότερα δεδομένα σχετικά με τη συνεχιζόμενη διαδικασία και μπορούμε να επηρεάσουμε τη διαδικασία βελτιστοποίησης. Η υλοποίηση της απρόσκοπτης συνδεσιμότητας ευνοείται από την ευρεία διαθεσιμότητα Ethernet και ασύρματης επικοινωνίας. Ακόμη και οι απαιτήσεις σε πραγματικό χρόνο καλύπτονται από ειδικά βιομηχανικά πρωτόκολλα Ethernet, τα οποία είναι αρκετά γρήγορα ώστε να οδηγούν συστήματα ελέγχου υψηλής συχνότητας με ένα μικρό ποσό ρίσκου.

Οι ειδικοί εκτιμούν ότι μέχρι το 2020 το IoT θα αποτελείται από τουλάχιστον 30 δισεκατομμύρια συσκευές. Επιπλέον υπολογίζεται ότι η αξία της παγκόσμιας αγοράς του IoT θα φτάσει τα 7.1 τρισεκατομμύρια δολάρια μέχρι το 2020.

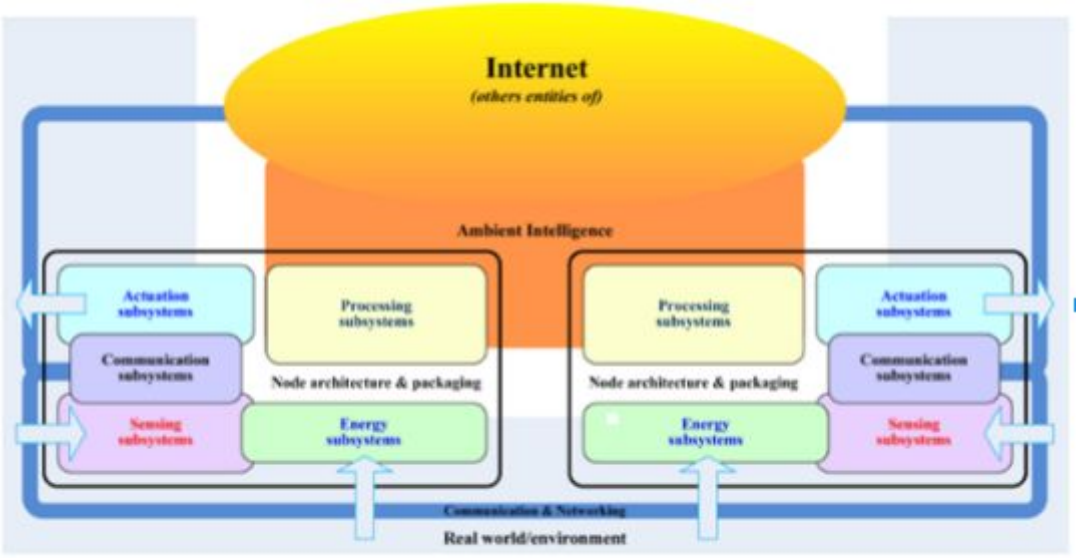
Το IoT επιτρέπει την εξ αποστάσεως μεταχείριση των αντικειμένων που ανήκουν στο δομημένο δίκτυο δίνοντας έτσι τη δυνατότητα την ενσωμάτωση του φυσικού κόσμου στο σύστημα των υπολογιστών. Το γεγονός αυτό αυξάνει την αποδοτικότητα, την ακρίβεια καθώς και τα οικονομικά οφέλη ενώ μειώνεται η ανάγκη ανθρώπινης παρέμβασης. Καθώς το IoT οργανώνεται με ολοένα και περισσότερους αισθητήρες και ενεργοποιητές η τεχνολογία παίρνει μία μορφή πιο γενικευμένη.

Η σημερινή επανάσταση στο Διαδίκτυο, τα κινητά, τα ασύρματα δίκτυα και οι M2M τεχνολογίες μπορούν να θεωρηθούν ως η πρώτη φάση του IoT, η οποία ενεργοποιήθηκε από τις τελευταίες εξελίξεις στα ακόλουθα: αναγνώριση ραδιοσυχνοτήτων (Radio Frequency IdentificationRFID), έξυπνοι αισθητήρες, τεχνολογίες επικοινωνιών, πρωτόκολλα Διαδικτύου και ο αυξανόμενος αριθμός φυσικών αντικειμένων που συνδέονται στο Διαδίκτυο με πρωτόγνωρους ρυθμούς. Το IoT καθιστά ικανά τα φυσικά αντικείμενα να “βλέπουνε”, να “ακούνε”, να

“σκέφτονται”και να εκτελούν εργασίες, έχοντάς τα να μιλούν μεταξύ τους για να μοιράζονται πληροφορίες και να συντονίζουν αποφάσεις. Ουσιαστικά μεταμορφώνει αυτά τα αντικείμενα από κλασικά παραδοσιακά σε έξυπνα. Τα έξυπνα αντικείμενα μαζί με τις “αποστολές”τους αποτελούν τον τομέα ειδικών εφαρμογών (Κάθετες αγορές), ενώ οι πανταχού παρούσες υπολογιστικές και αναλυτικές υπηρεσίες διαμορφώνουν τον τομέα εφαρμογής ανεξάρτητων υπηρεσιών (Οριζόντιες αγορές).

Η παρακάτω εικόνα απεικονίζει την συνολική αντίληψη του IoT, στην οποία κάθε τομέας ειδικών εφαρμογών αλληλεπιδρά με τον τομέα ανεξάρτητων υπηρεσιών, ενώ σε κάθε τομέα, αισθητήρες και ενεργοποιητές επικοινωνούν απευθείας μεταξύ τους.Για παράδειγμα, το έξυπνο σπίτι θα ανοίξει αυτόματα το γκαράζ όταν οι ένοικοι αυτού φτάνουν στο σπίτι, θα ετοιμάζει τον καφέ τους, θα έχει τον έλεγχο του κλίματος-θερμοκρασίας, της τηλεόρασης και άλλων συσκευών. .(Al-Fuqaha et al., 2015)

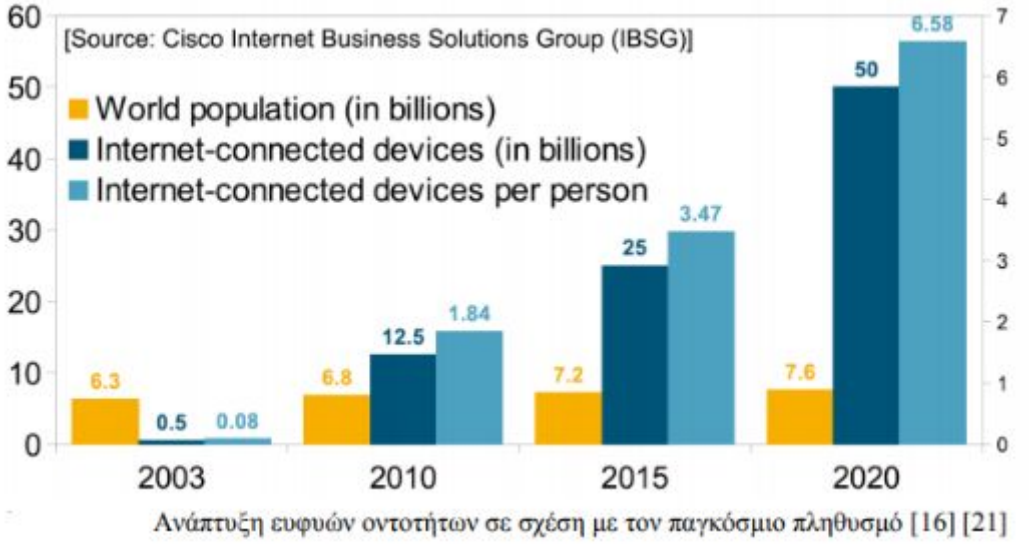
Αυτό το οποίο προτείνει το IoT είναι να ενσωματώσει την τεχνολογία σε καθημερινές συσκευές, όπως οπτικοακουστικούς δέκτες, ανιχνευτές καπνού, οικιακές συσκευές κ.α. και να τις κάνει «Online», επιτρέποντάς τες να επικοινωνούν μεταξύ τους και με άλλες συσκευές ακόμη και αν δεν είχαν αρχικά σχεδιαστεί με αυτή την ικανότητα. Μια άλλη μεγάλη εξελικτική αλλαγή που υπόσχεται το IoT είναι η ενσωμάτωση των δικτύων στα οποία εμπεριέχονται αυτές οι συσκευές, καθιστώντας έτσι κάθε συσκευή άμεσα προσβάσιμη μέσω του Διαδικτύου. Τελικά οι IoT συσκευές θα είναι πανταχού παρούσες και context-awareness, βασικές προϋποθέσεις της περιβάλλουσας νοημοσύνης-Ambient Intelligence. Η περιβάλλουσα νοημοσύνη θα επιτρέπει στα αντικείμενα καθημερινής χρήσης να καταλαβαίνουν το περιβάλλον στο οποίο βρίσκονται, να αλληλεπιδρούν με τους ανθρώπους και να λαμβάνουν αποφάσεις. Κατά συνέπεια, ένας κόσμος γεμάτος έξυπνα αντικείμενα υπόσχεται μεγάλη βελτίωση στις επιχειρηματικές διαδικασίες και τη ζωή των ανθρώπων, αλλά έρχεται επίσης με σοβαρές απειλές και τεχνικές προκλήσεις που πρέπει να ξεπεραστούν.(Whitmore, Agarwal and Da Xu, 2014)



Object connected to Internet of Things and their three main challenging domains: Technologies — Communication — Intelligence [15]

Υπολογίζεται ότι αυτή τη στιγμή υπάρχουν 1.5 δισεκατομμύρια υπολογιστές και πάνω από 1 δισεκατομμύριο κινητά τηλέφωνα, παγκοσμίως με δυνατότητα πρόσβασης στο Διαδίκτυο. Σε αυτές τις δύο κατηγορίες συσκευών θα προστεθεί πολύ μεγάλος αριθμός ευφυών οντοτήτων, ώστε το 2020 υπολογίζεται ότι θα υπάρχουν 50 έως 100 δισεκατομμύρια συσκευές συνδεδεμένες στο Διαδίκτυο παγκοσμίως,

υπερβαίνοντας κάθε προσδοκία ερευνητών και μελετητών. Για να γίνει αντιληπτό το μέγεθος των συσκευών, αξίζει να αναφερθεί μια έρευνα της CISCO (Αμερικανική Εταιρεία Δικτύωσης Υπολογιστών), σύμφωνα με την οποία το 2020 κάθε άνθρωπος στον πλανήτη θα μπορεί να έχει έως και 6 συσκευές συνδεδεμένες ταυτόχρονα στο Διαδίκτυο.(Καλύβας Βασίλειος)(Perera et al., 2014)



Ανάπτυξη ευφυών οντοτήτων σε σχέση με τον παγκόσμιο πληθυσμό [16] [21]

1.1.2 Το όραμα του IoT

Το όραμα του IoT στηρίζεται σε τρεις (3) βασικούς πυλώνες:

1) Τεράστιο εύρος και πλήθος συσκευών. Η επικοινωνία M2M θα περιλαμβάνει τόσο συσκευές χαμηλής τιμής και κατανάλωσης ενέργειας, όσο και συσκευές υψηλών δυνατοτήτων και προδιαγραφών, όπως ευφυή συστήματα όρασης (intelligent vision systems), εξαρτήματα ελέγχου μηχανών (machine control modules), πύλες μετάδοσης δεδομένων σε έξυπνα σπίτια (gateways in smart homes), καθώς και καταναλωτικά ηλεκτρονικά προϊόντα (π.χ.smartphones, tablets, υπολογιστές, smartwatches).

2) Εξαιρετικά επεκτάσιμη συνδεσιμότητα. Αυτή είναι ίσως η σημαντικότερη παράμετρος στην M2M επικοινωνία, καθώς μια συσκευή που δεν είναι συνδεδεμένη στο Διαδίκτυο δεν μπορεί να συνεργαστεί με άλλες. Έτσι, η μεγαλύτερη πρόκληση που αντιμετωπίζουν οι κατασκευαστές δικτύων είναι ο σχεδιασμός και η υλοποίηση μιας χαμηλού κόστους συνδεσιμότητας, μεταξύ του τεράστιου εύρους συσκευών που αναφέρθηκε προηγουμένως, λαμβάνοντας υπόψη τις ιδιαιτερότητες και τις κατασκευαστικές απαιτήσεις τους.

3) Διαχείριση, έλεγχος και πρόσβαση στις συσκευές και τις υπηρεσίες μέσω της τεχνολογίας Cloud. Η ιδέα του IoT δεν αφορά την αυτόνομη λειτουργία κάθε

συσκευής αλλά τη συνεργασία πολλών συσκευών μεταξύ τους. Επομένως, είναι απαραίτητη η ύπαρξη κεντρικών μονάδων διαχείρισης και λήψης αποφάσεων ανά μεγάλα πλήθη διατάξεων ή κόμβων M2M. Προς το παρόν, αυτό είναι εφικτό μόνο μέσω της τεχνολογίας Cloud.

Όσον αφορά στον επιχειρηματικό τομέα, το IoT προσφέρει περισσότερες δυνατότητες στις επιχειρήσεις και εμπλουτίζει τον τομέα υπηρεσιών Cloud, Mobile και Big Data Analytics. Οι έννοιες αυτές αφορούν τις κινητές επικοινωνίες, τις ψηφιακές πληροφορίες, το διαμοιρασμό τους, την ανάλυση και την εξαγωγή συμπερασμάτων. Η στρατηγική των επιχειρήσεων επαναπροσδιορίζεται ώστε να αξιοποιούν στο έπακρο τις δυνατότητες απομακρυσμένου ελέγχου και παρακολούθησης των διαφόρων τμημάτων τους, δυνατότητες που προσφέρουν το IoT και οι M2M επικοινωνίες. Για παράδειγμα, καθίσταται δυνατή η απομακρυσμένη επιτήρηση φορτίων σε φορτηγά πλοία, ο έλεγχος της κατάστασης και του περιεχομένου τους και ο ακριβής προσδιορισμός της εκάστοτε θέσης τους. Έτσι, μια ναυτιλιακή επιχείρηση έχει πλήρη έλεγχο των εμπορευμάτων της κάθε στιγμή και υπό οποιεσδήποτε σχεδόν συνθήκες. (Καλύβας Βασίλειος)

Όπως γίνεται αντιληπτό, το IoT θα έχει μία ευρεία χρήση και στην καθημερινότητα του ανθρώπου. Όμως η χρήση του πρέπει να γίνει με προσοχή καθώς από αυτήν μπορεί να δημιουργηθούν προβλήματα ασφάλειας και ελέγχου. Είναι φανερό ότι η υλοποίηση του IoT δεν μπορεί να γίνει με τα σημερινά επίπεδα ελέγχου και ασφάλειας. Επίσης, μεγάλο ζήτημα για την ανάπτυξη του αποτελεί και η ιδιωτικότητα του ανθρώπου. Έτσι πρέπει να βρεθούν τρόποι για να προστατεύονται οι πληροφορίες από τυχόν αλλοιώσεις και καταστροφές καθώς και από μη εξουσιοδοτημένη χρήση. Επιπλέον, πρέπει να παρέχει αξιόπιστες πληροφορίες, οι οποίες να είναι διαθέσιμες στους χρήστες που τις αναζητούν. Δηλαδή, πρέπει να υπάρξει διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων αλλά και της αδιάλειπτης λειτουργίας του υπολογιστικού συστήματος.

Συμπερασματικά, η εποχή του IoT έρχεται να ταράξει τις ισορροπίες που ισχύουν έως τώρα. Οι τομείς στους οποίους θα εισχωρήσει το IoT θα βελτιώσουν την ποιότητα ζωής των ανθρώπων και θα βοηθήσει πολύ στην εξοικονόμηση ενέργειας, χρόνου και χρήματος. Το μεταβατικό στάδιο είναι αρκετά δύσκολο και για να γίνει το IoT οικείο στον άνθρωπο θα πρέπει να ξεπεραστούν όλοι οι κίνδυνοι και οι φόβοι που δημιουργεί. Όμως από την στιγμή που όλοι αυτοί οι κίνδυνοι ξεπεραστούν, η ζωή του ανθρώπου θα έχει αλλάξει προς το καλύτερο.

Η ιστορία του IoT

Το Διαδίκτυο των Πραγμάτων (IoT) αναφέρεται στην εικονική αναπαράσταση ενός μοναδικά αναγνωρίσιμου αντικειμένου, σε μία διαδικτυακή μορφή, συνδεδεμένο με τεχνολογία Ραδιο- συχνότητας (Radio-Frequency IDentification technology (RFID)). Ο όρος χρησιμοποιήθηκε για πρώτη φορά από τον Kevin Ashton το 1999 με την

σημερινή του έννοια, ενώ υπάρχουν αναφορές στην βιβλιογραφία τουλάχιστον από το 1991. Η έρευνα που γίνεται πάνω στο IoT βρίσκεται ακόμα σε πρώιμο στάδιο, για το λόγο αυτό δεν υπάρχει κάποιος καθολικός ορισμός του όρου. Σύμφωνα με τον ορισμό του Kevin Ashton: "Σήμερα οι υπολογιστές και ως εκ τούτου και το Διαδίκτυο, εξαρτώνται σχεδόν αποκλειστικά από εμάς τους ανθρώπους όσον αφορά τις πληροφορίες. Σχεδόν όλο το σύνολο των περίπου 50 petabytes (1petabyte = 1024 terrabytes) των διαθέσιμων δεδομένων στο Διαδίκτυο δημιουργήθηκαν από τον άνθρωπο, πληκτρολογώντας, εκχωρώντας μια εγγραφή, λαμβάνοντας μια ψηφιακή φωτογραφία ή σαρώνοντας ένα barcode κτλ. Συμβατικά διαγράμματα του Διαδικτύου περιλαμβάνουν διακομιστές (servers), δρομολογητές (routers) κ.ο.κ, αλλά δεν περιλαμβάνουν τους σημαντικότερους δρομολογητές, που είναι οι άνθρωποι. Το πρόβλημα είναι, ότι οι άνθρωποι έχουν περιορισμένο χρόνο, προσοχή και ακρίβεια, κατά συνέπεια δεν είναι πολύ αποτελεσματικοί στην καταγραφή δεδομένων που αφορούν πράγματα του πραγματικού κόσμου. " (Kevin Ashton,1999)

Το IoT σύμφωνα με το IERC ορίζεται ως "μια δυναμική παγκόσμια υποδομή δικτύου με δυνατότητες αυτο-διαμόρφωσης βασιζόμενη σε πρότυπα και διαλειτουργικά πρωτοκόλλα επικοινωνίας, φυσικά και εικονικά "πράγματα", που έχουν ταυτότητα και χαρακτηριστικά και είναι ικανά να χρησιμοποιούν ευφυείς διεπαφές, ενσωματωμένα σε ένα δίκτυο πληροφοριών". Οι λέξεις "Internet" και "Things" σημαίνει ένα διασυνδεδεμένο παγκόσμιο δίκτυο βασισμένο σε αισθητήρες, επικοινωνία, δικτύωση και τεχνολογία επεξεργασίας πληροφοριών, το οποίο μπορεί να είναι η νέα έκδοση της τεχνολογίας πληροφοριών και επικοινωνιών (ICT). Ωστόσο, ο ακριβής ορισμός του IoT είναι ακόμα στη διαδικασία σχηματισμού που υπόκειται στις προοπτικές που λαμβάνονται. (Shancang Li & Li Da Xu &Shanshan Zhao)

Ο ορισμός του IoT σύμφωνα με το IERC [18]

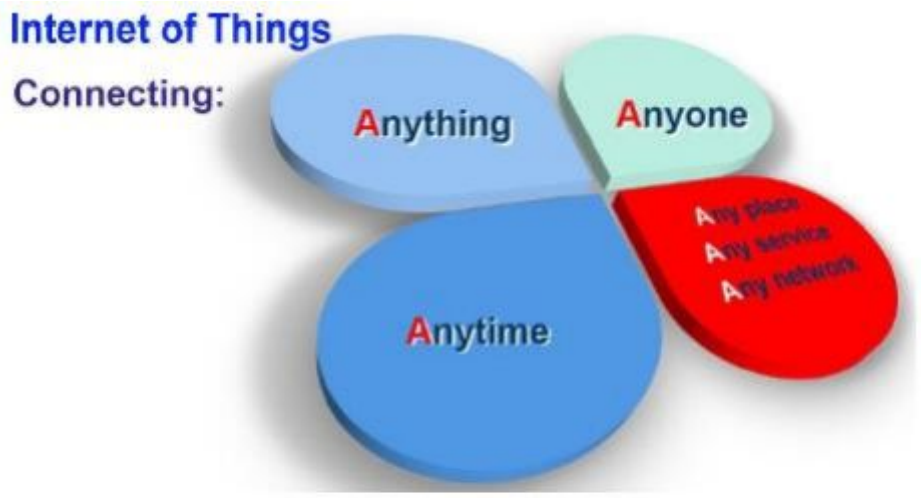
1.1.3 Τα χαρακτηριστικά του IoT

Το Διαδίκτυο των Πραγμάτων έχει τρία σημαντικά χαρακτηριστικά:

- Διασυνδεσιμότητα: Όσον αφορά το IoT, οτιδήποτε μπορεί να είναι διασυνδεδεμένο με την παγκόσμια πληροφοριακή και επικοινωνιακή υποδομή.
- Things-related services: Το IoT είναι ικανό να παρέχει συναφείς υπηρεσίες σύμφωνα με τους περιορισμούς των πραγμάτων, όπως η προστασία της ιδιωτικότητας και η σημασιολογική συνοχή μεταξύ των φυσικών πραγμάτων και των αντίστοιχων εικονικών τους.
- Ετερογένεια: Οι συσκευές στο IoT είναι ετερογενείς, καθώς βασίζονται σε διαφορετικές πλατφόρμες υλικού και δίκτυα. Μπορούν να αλληλεπιδράσουν με άλλες συσκευές ή πλατφόρμες μέσω διαφορετικών δικτύων.
- Δυναμικές αλλαγές: Η κατάσταση των συσκευών αλλάζει δυναμικά, π.χ. μπορεί είναι σε κατάσταση "ύπνου" ή σε λειτουργία, να είναι συνδεδεμένες και / ή αποσυνδεδεμένες. Επιπλέον, ο αριθμός των συσκευών μπορεί να αλλάξει δυναμικά.
- Τεράστιες κλίμακα: Ο αριθμός των συσκευών που πρέπει να είναι διαχειρίσιμες και επικοινωνούν μεταξύ τους, θα είναι τουλάχιστον μία τάξης μεγέθους μεγαλύτερος από τις συσκευές που είναι συνδεδεμένες στο Διαδίκτυο τώρα. Η αναλογία της επικοινωνίας που προκλήθηκε από τις συσκευές σε σύγκριση με την επικοινωνία που προκλήθηκε από τον άνθρωπο, θα μετατοπιστεί σημαντικά προς την επικοινωνία που προκλήθηκε από την συσκευή. Ακόμη πιο κρίσιμη θα είναι η διαχείριση των δεδομένων που παράγονται και η ερμηνεία τους. Αυτό σχετίζεται με την σημασιολογία των δεδομένων, καθώς και με την αποτελεσματική διαχείριση των δεδομένων.

Με βάση την παραπάνω θεώρηση των «πραγμάτων», ένας τεράστιος αριθμός συσκευών και πραγμάτων θα συνδέεται στο Διαδίκτυο, παρέχοντας το καθένα δεδομένα και πληροφορίες και ορισμένα, ακόμα και υπηρεσίες. Το όραμα αυτό

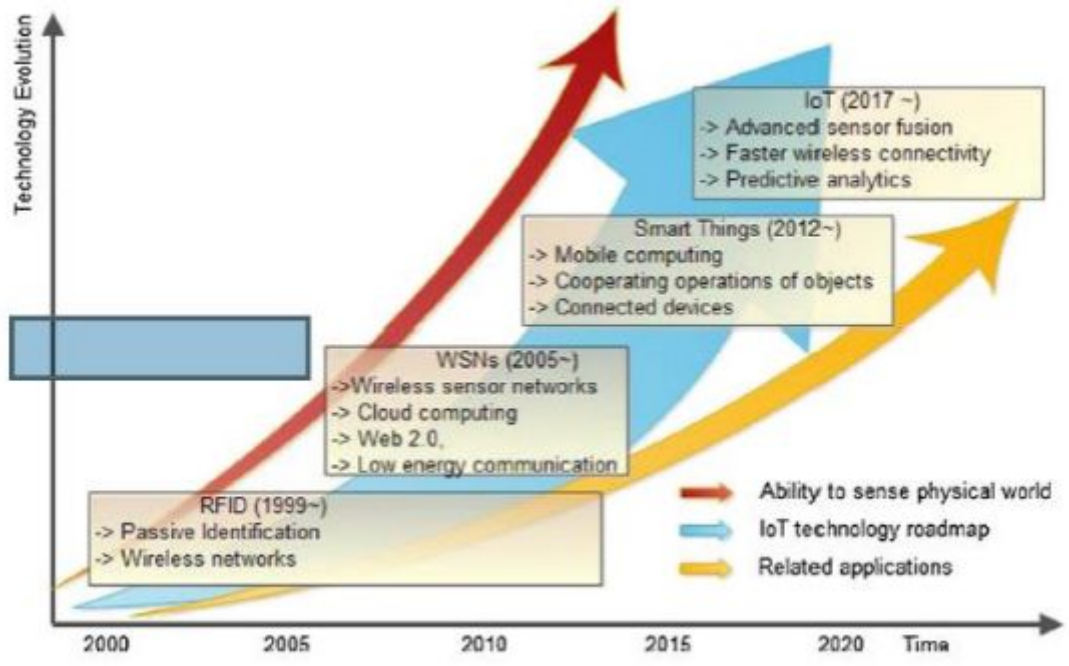
ενισχύει τη συνδεσιμότητα από το «κάθε- στιγμή, σε κάθε-θέση» για «κάθε-έναν» στο «κάθε-στιγμή, σε κάθε-θέση» για «κάθε-τι». Το Διαδίκτυο των Πραγμάτων θα μπορούσε να επιτρέψει στους ανθρώπους και τα πράγματα να είναι συνδεδεμένοι πάντα και παντού, με οτιδήποτε και οποιονδήποτε, ιδανικά χρησιμοποιώντας οποιαδήποτε διαδρομή/δίκτυο και κάθε υπηρεσία. (Εικ. 2.4) Κάθε στιγμή – Κάθε θέση: Μέρα, νύχτα, σε κίνηση, σε εξωτερικούς και εσωτερικούς χώρους, από το Pc ή μακριά από αυτό. Κάθε τι: Ανάμεσα σε PCs, άνθρωπο προς άνθρωπο, άνθρωπο προς πράγματα και πράγμα προς πράγματα.



Internet of Things – 6A connectivity [15]

Στην συνέχεια θα παρουσιάσουμε την εξέλιξη του Διαδικτύου των Πραγμάτων όπως απεικονίζεται παρακάτω (Εικ.2.5) σε διάφορες φάσεις, σε σχέση με την Τεχνολογική εξέλιξη και τον Χρόνο. Το IoT ξεκίνησε όπως προαναφέραμε με τη χρήση της τεχνολογίας RFID, οποία χρησιμοποιείται όλο και περισσότερο στα logistics, στη παραγωγή φαρμακευτικών προϊόντων, στη λιανική και σε διάφορες βιομηχανίες. Επιπλέον, οι αναδυόμενες ασύρματες τεχνολογίες αισθητήρων έχουν επεκτείνει σημαντικά τις ικανότητες των συσκευών αυτών και ως εκ τούτου η αρχική έννοια του IoT επεκτείνετε σε περιβάλλουσα νοημοσύνη-Ambient Intelligence και αυτόνομο έλεγχο. Τέλος, τεχνολογίες όπως ασύρματα δίκτυα αισθητήρων (WSNs), γραμμωτούς κώδικες (barcodes), έξυπνη ανίχνευση, RFID, NFC, χαμηλή κατανάλωση ενέργειας,

ασύρματες επικοινωνίες, cloud computing και ούτω καθεξής, βοηθούν στην εξέλιξη και την πραγματοποίηση του οράματος που ονομάζεται Διαδίκτυο των Πραγμάτων.

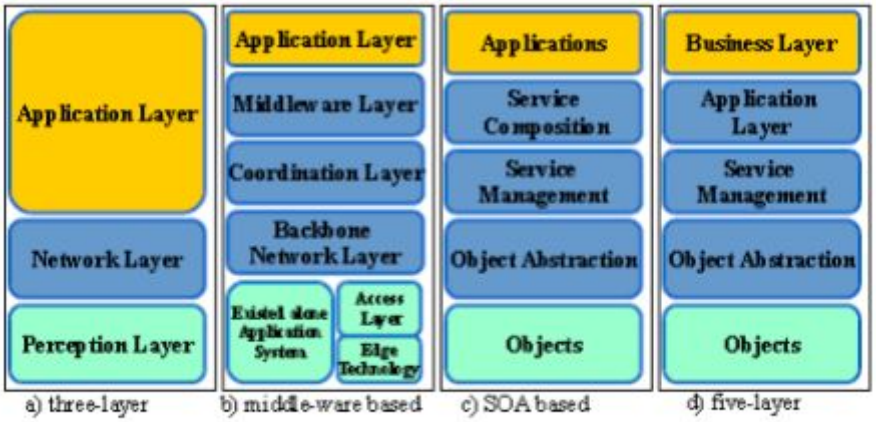


Η εξέλιξη του IoT [18]

1.2 Η Αρχιτεκτονική του IoT

Το IoT θα πρέπει να είναι σε θέση να παρέχει επικοινωνία σε δισεκατομμύρια ή τρισεκατομμύρια ετερόκλητα αντικείμενα μέσω του Διαδικτύου. Έτσι υπάρχει μια κρίσιμη ανάγκη για ευέλικτη πολύ επίπεδη αρχιτεκτονική. Ο συνεχώς αυξανόμενος αριθμός προτεινόμενων αρχιτεκτονικών ακόμα δεν συγκλίνει σε ένα μοντέλο αναφοράς. Εν τω μεταξύ, υπάρχουν ορισμένα έργα όπως IoT-A, το οποίο προσπαθεί να σχεδιάσει μια κοινή αρχιτεκτονική που να βασίζεται στην ανάλυση των αναγκών των ερευνητών και της βιομηχανίας.

Από το "pool" των προτεινόμενων μοντέλων, το βασικό μοντέλο αρχιτεκτονικής είναι αυτό των τριών επιπέδων (3-layer), αποτελούμενο από τα στρώματα εφαρμογής, δικτύου και αντίληψης. Ωστόσο, στην πρόσφατη βιβλιογραφία, κάποια άλλα μοντέλα έχουν προταθεί που προσθέτουν μια πιο αφηρημένη IoT αρχιτεκτονική. Η Εικ. 2.6 δείχνει μερικές κοινές αρχιτεκτονικές, μεταξύ άλλων και το μοντέλο των πέντε επιπέδων (5-layer) (δεν πρέπει να συγχέεται με τα TCP/IP στρώματα). Στην συνέχεια, παρέχουμε μια σύντομη αναφορά σε αυτό και γιατί επιλέξαμε να το αναλύσουμε.



Η αρχιτεκτονική του IoT [13]

Objects/Perception Layer: Το πρώτο στρώμα, τα Αντικείμενα (συσκευές) ή στρώμα Αντίληψης, αντιπροσωπεύει τους φυσικούς αισθητήρες του IoT, που στοχεύουν στη συλλογή και επεξεργασία πληροφοριών. Αυτό το στρώμα περιλαμβάνει αισθητήρες και ενεργοποιητές, οι οποίοι εκτελούν διάφορες λειτουργίες, όπως η υποβολή ερωτημάτων θέσεως, θερμοκρασίας, βάρους, κίνησης, δόνησης, επιτάχυνσης, υγρασίας, κ.τ.λ. Τυποποιημένοι μηχανισμοί plug-and-play πρέπει να χρησιμοποιούνται από αυτό το επίπεδο για να ρυθμίζονται τα ετερόκλητα αντικείμενα. Το στρώμα Αντίληψης ψηφιοποιεί και μεταφέρει δεδομένα στο Object Abstraction layer μέσω ασφαλών καναλιών.

Object Abstraction layer: Το Object Abstraction layer μεταφέρει τα δεδομένα που παράγονται από το στρώμα Αντίληψης ή Αντικειμένων στο στρώμα Διαχείρισης Υπηρεσιών –Service Management μέσω ασφαλών καναλιών. Τα δεδομένα μπορούν να μεταφερθούν μέσω διαφόρων τεχνολογιών όπως RFID, 3G, GSM, UMTS, Wi-Fi, Bluetooth Low Energy, infrared, ZigBee κ.α. Επιπλέον, άλλες λειτουργίες όπως το cloud computing και οι διαδικασίες διαχείρισης δεδομένων είναι χειρίσιμες σε αυτό το στρώμα.

Service Management Layer: Το στρώμα Διαχείρισης ή Middleware συνδυάζει μια υπηρεσία με τον αιτούντα αυτής, βάση διεύθυνσης ή ονόματος. Αυτό το στρώμα ενεργοποιεί τους IoT προγραμματιστές εφαρμογών να δουλέψουν με ετερογενή αντικείμενα χωρίς να λαμβάνουν υπόψη μια συγκεκριμένη πλατφόρμα υλικών. Επιπλέον, αυτό το στρώμα επεξεργάζεται τα ληφθέντα δεδομένα, παίρνει αποφάσεις και παραδίδει τις απαιτούμενες υπηρεσίες μέσω πρωτοκόλλων ενσύρματων δικτύων.

Application Layer: Το στρώμα Εφαρμογής παρέχει τις υπηρεσίες που ζητούν οι πελάτες. Για παράδειγμα, το στρώμα αυτό μπορεί να παρέχει μετρήσεις θερμοκρασίας και υγρασίας αέρα στον πελάτη που ρωτά για αυτά τα δεδομένα. Η

σημασία αυτού του στρώματος για το IoT είναι ότι έχει τη δυνατότητα να παρέχει έξυπνες υπηρεσίες υψηλής ποιότητας για την κάλυψη των αναγκών των πελατών. Το στρώμα Εφαρμογής καλύπτει πολλές κάθετες αγορές όπως το έξυπνο σπίτι, κτήριο, μεταφορές, Βιομηχανικοί Αυτοματισμοί και την έξυπνη υγειονομική περίθαλψη.

Business Layer: Το Επιχειρησιακό στρώμα (management) διαχειρίζεται τις συνολικές IoT δραστηριότητες και υπηρεσίες του συστήματος. Οι ευθύνες αυτού του επιπέδου είναι να οικοδομήσει ένα επιχειρηματικό μοντέλο, γραφικές παραστάσεις, διαγράμματα ροής κ.λ.π., βάσει των ληφθέντων δεδομένων από το στρώμα Εφαρμογής. Επίσης, αναλύει, σχεδιάζει, υλοποιεί, αξιολογεί, παρακολουθεί, αναπτύσσει συσχετιζόμενα IoT στοιχεία και υποστηρίζει τη διαδικασία λήψης αποφάσεων, με βάση την ανάλυση μεγάλου όγκου δεδομένων (Big Data). Επιπλέον, αυτό το στρώμα συγκρίνει το αποτέλεσμα του κάθε επιπέδου με το αναμενόμενο αποτέλεσμα για την βελτίωση των υπηρεσιών και τη διατήρηση του απόρρητου των χρηστών. (Al-Fuqaha et al., 2015)

Οι αρχιτεκτονικές που δανείζονται τα στρώματα και τις έννοιες τους από στοίβες δικτύου (όπως το μοντέλο των τριών επιπέδων), δεν ανταποκρίνονται σε πραγματικά IoT περιβάλλοντα, δεδομένου ότι, π.χ., το στρώμα «δικτύου» δεν καλύπτει όλες τις υποκείμενες τεχνολογίες οι οποίες μεταφέρουν δεδομένα σε μια IoT πλατφόρμα. Επιπλέον, αυτά τα μοντέλα έχουν σχεδιαστεί για συγκεκριμένους τύπους μέσων επικοινωνίας όπως το WSNs. Το πιο σημαντικό είναι ότι τα στρώματα θα "τρέχουν" σε συσκευές περιορισμένων πόρων. Για το λόγο αυτό, δεν είναι αποδεκτό ένα στρώμα σαν το Service Composition-Σύσταση Υπηρεσίας στην SoA (Service oriented Architecture) αρχιτεκτονική, να καταλαμβάνει ένα μεγάλο κλάσμα του χρόνου και της ενέργειας της συσκευής για να επικοινωνήσει με άλλες συσκευές και να ενσωματώσει τις απαραίτητες υπηρεσίες.

Στο μοντέλο των πέντε στρωμάτων, το στρώμα Εφαρμογών είναι η διασύνδεση με την οποία οι τελικοί χρήστες μπορούν να αλληλεπιδράσουν με μια συσκευή και να θέτουν ερωτήματα. Παρέχει επίσης μια διεπαφή στο στρώμα Επιχειρήσεων, όπου υψηλού επιπέδου ανάλυση και αναφορές μπορούν να παραχθούν. Οι μηχανισμοί ελέγχου της πρόσβασης στα δεδομένα σε επίπεδο Εφαρμογής, γίνεται επίσης σε αυτό το στρώμα. Λαμβάνοντας υπόψη όλα τα παραπάνω από την μια πλευρά και την απλότητα της αρχιτεκτονικής από την άλλη, το μοντέλο των πέντε-στρωμάτων είναι το πιο εφαρμόσιμο για τις IoT εφαρμογές.

Πρέπει να σημειωθεί, ωστόσο, πως επί του παρόντος, δεν υπάρχει κάποια ευρέως αποδεκτή αρχιτεκτονική του Διαδικτύου των Πραγμάτων. Αρκετά άρθρα προτείνουν διάφορες εννοιολογικές αρχιτεκτονικές σχεδίασης, ενώ άλλα προτείνουν κριτήρια για την αξιολόγηση των προτεινόμενων αρχιτεκτονικών, καθώς και μια εννοιολογική αρχιτεκτονική που να ανταποκρίνεται στις απαιτήσεις των έξυπνων αντικειμένων.

1.3 Εφαρμογές IoT

1.3.1 Έξυπνα Εργοστάσια

Έξυπνη παραγωγή και έξυπνα εργοστάσια αποτελούν μία γενική έννοια της παραγωγής που αποσκοπεί στην βελτίωση της παραγωγικής διαδικασίας. Η έξυπνη παραγωγή είναι μία διαδικασία που χρησιμοποιεί έλεγχο από ηλεκτρονικούς υπολογιστές, μοντελοποίηση, big data αλλά και άλλους αυτοματισμούς με στόχο την οργάνωση της παραγωγής.

Η έξυπνη παραγωγή ωφελείται από τις νέες τεχνολογίες στους πάνω στην μεταφορά δεδομένων και επικοινωνία των μηχανών. Εκτιμάται ότι θα αποτελέσει τη νέα βιομηχανική επανάσταση.

Το ινστιτούτο National Institute of Standards and Technology (NIST) ορίζει την έξυπνη παραγωγή ως συστήματα τα οποία είναι πλήρως ολοκληρωμένα συστήματα παραγωγής τα οποία αποκρίνονται σε πραγματικό χρόνο ώστε να ικανοποιούν ανά πάσα στιγμή τις απαιτήσεις και τις συνθήκες που διαμορφώνονται στο εργοστάσιο, στο δίκτυο διανομής αλλά και στην ζήτηση των καταναλωτών.

Ο οργανισμός Smart Manufacturing Leadership Coalition (SMLC) ορίζει την έξυπνη παραγωγή ως την ικανότητα να μπορεί να λύνει υπάρχοντα αλλά και μελλοντικά προβλήματα μέσω μίας ανοιχτής υποδομής η οποία επιτρέπει την εφαρμογή λύσεων ταυτόχρονα με την παραγωγή ενώ παράλληλα παράγει και πλεονάζουσα αξία.

(Manufacturingtomorrow.com, 2018)

Πλέον δεν χρειάζεται κανείς να κοιτάξει από πολύ κοντά την παραγωγή ώστε να καταλάβει ότι ο τρόπος με τον οποίο λειτουργούν σήμερα τα εργοστάσια εξαρτάται άμεσα από την εξέλιξη της τεχνολογίας. Η εφαρμογή των νέων τεχνολογιών κάνει τη διαδικασία της παραγωγής πιο ευφυή και δυναμική επιτρέποντας την ιδέα των έξυπνων εργοστασίων να γίνει πραγματικότητα.

Κατανοώντας το έξυπνο εργοστάσιο

Αρχικά, ο όρος έξυπνο εργοστάσιο αναφέρεται σε ένα περιβάλλον όπου οι μηχανές και ο εξοπλισμός είναι σε θέση να βελτιώσουν τις παραγωγικές διαδικασίες μέσω αυτοματισμού και αυτοβελτίωσης. Τα οφέλη δεν περιορίζονται στην παραγωγή των προϊόντων αλλά και σε διαδικασίες όπως η οργάνωση και διαχείριση της εφοδιαστικής αλυσίδας αλλά και στην εξέλιξη των ίδιων των προϊόντων.

Ωστόσο, η παραγωγή πραγματοποιείται μέσα στους τέσσερις τοίχους του εργοστασίου. Η δομή ενός έξυπνου εργοστασίου μπορεί να περιλαμβάνει συνδιασμό της παραγωγικών, πληροφοριακών και επικοινωνιακών τεχνολογιών με δυνατότητα ενσωμάτωσης σε ολόκληρη την αλυσίδα εφοδιασμού της βιομηχανίας.

Όλα αυτά τα ξεχωριστά μέρη της παραγωγής μπορούν να συνδεθούν μέσω ενός δικτύου Internet of Things (IoT) ή μέσω άλλων προχωρημένων ολοκληρωμένων κυκλωμάτων, τα οποία επιτρέπουν την μέτρηση, την αίσθηση, τον έλεγχο και την επικοινωνία μεταξύ όλων των τμημάτων που συμμετέχουν στην παραγωγή.

Οι αισθητήρες επιτρέπουν το IoT

Κεντρικό κομμάτι ενός έξυπνου εργοστασίου αποτελεί η τεχνολογία που επιτρέπει τη συλλογή δεδομένων. Αυτού του είδους η τεχνολογία σε συνδυασμό με τους έξυπνους αισθητήρες, τα μηχανήματα και τη ρομποτική, συνθέτουν τη γραμμή παραγωγής.

Οι αισθητήρες βοηθούν στην παρακολούθηση συγκεκριμένων διαδικασιών της παραγωγής με αποτέλεσμα να υπάρχει αυξημένη επίγνωση στο τι ακριβώς συμβαίνει σε όλα τα επίπεδα της παραγωγής. Για παράδειγμα, οι αισθητήρες δονήσεων μπορούν άμεσα να ενημερώνουν για το ποια μηχανήματα, ρουλεμάν ή κάποιο άλλο είδος εξοπλισμού χρειάζεται συντήρηση. Αυτού του είδους οι μικρές προειδοποιήσεις αποτρέπουν κινδύνους για προβλήματα που μπορούν να προκαλέσουν ζημιά στην παραγωγή.

Παρόμοια τεχνολογία αισθητήρων με αυτή των SDVs (Self-Driving Vehicles) χρησιμοποιείται και κατά τη διαχείριση των υλικών. Έτσι αυξάνεται η αποδοτικότητα και η ασφάλεια καθώς το προϊόν κινείται μέσα στο εργοστάσιο. Αυτού του είδους η ρομποτική έχει τη δυνατότητα να ανιχνεύει την παρουσία ανθρώπου ή κάποιου άλλου εμποδίου που θα μπορούσε να παρεμποδίσει την ομαλή λειτουργία της παραγωγής. Η δυνατότητα του να μπορείς να αποφεύγεις αυτόματα τέτοιου είδους εμπόδια, αποτελεί τεράστιο πλεονέκτημα καθώς το εργοστάσιο λειτουργεί εύρυθμα.

Η επικοινωνία καθώς και η δυνατότητα χρησιμοποίησης των δεδομένων είναι και ο βασικός λόγος που τοποθετούμε πλέον τον όρο "έξυπνο" μπροστά από το εργοστάσιο. Οι νέες τεχνολογίες που αναδύονται συμβάλλουν αποφασιστικά στο εγχείρημα των έξυπνων εργοστασίων τα οποία από πολλούς θεωρούνται ως η βιομηχανική επανάσταση της εποχής μας.

Ουσιαστικά, είναι η χρήση της ευφυίας στο εργοστάσιο που επιτρέπει ένα δυναμικό παραγωγικό περιβάλλον και τα επιθυμητά αποτελέσματα, μειώνοντας τα κόστος και αυξάνοντας την ποιότητα και την αξιοπιστία.

Πως θα επηρεαστούν οι θέσεις εργασίας στα εργοστάσια?

Καθώς τα έξυπνα εργοστάσια θα αρχίσουν να παρουσιάζονται, ο ρόλος των εργαζομένων θα αρχίσει κι αυτός να αλλάζει. Θα είναι εξελιγμένος σε σχέση με την τωρινή του θέση. Ο εργαζόμενος πλέον θα αναλαμβάνει πιο σύνθετους ρόλους καθώς ο αυτοματισμός της παραγωγής θα καταλάβει τις επαναλαμβανόμενες εργασίες. Έχει αποδειχθεί από έρευνες ότι η εξέλιξη της τεχνολογίας δεν μειώνει τις θέσεις εργασίας απλά αλλάζει ο ρόλος του κάθε εργαζόμενου πλέον.

Συμπερασματικά, η επένδυση ενός έξυπνου εργοστασίου ωφελεί τους παραγωγούς καθώς δημιουργούν ένα πιο ασφαλές και αξιόπιστο εργοστάσιο

Παραδείγματα "έξυπνης" παραγωγής

Caterpilar

Η εταιρία μηχανημάτων και εξοπλισμού **Caterpilar** δημοσίευσε συνεργασία με την Uptake, η οποία είναι μία εταιρία για analytics, με στόχο να βοηθήσει τους πελάτες της πρώτης να έχουν μεγαλύτερη επίγνωση για την κατάσταση των μηχανημάτων τους, να μπορούν δηλαδή να τα παρακολουθούν και να οργανώνουν τον στόλο τους όσο το δυνατόν πιο αποδοτικά. Η εταιρία υποστηρίζει ότι οι πελάτες χρησιμοποιούν την τεχνολογία αυτή για να επιβλέπουν τους στόλους των μηχανημάτων καθώς και ανιχνεύουν τα επίπεδα καυσίμου σε κάθε μηχανή. Βέβαια, υποστηρίζεται ότι η συνεργασία αυτή στοχεύει να ανεβάσει τις υπηρεσίες της Caterpillar στο επόμενο επίπεδο.

Doug Oberhelman, CEO of Caterpillar ισχυρίζεται ότι με την εφαρμογή των νέων τεχνολογιών που φέρνει το IoT δίνεται μία νέα προοπτική στους πελάτες καθώς πλέον ξεφεύγουν από τη λογική ‘repair after failure’ και πλέον έχουν τη δυνατότητα του ‘repair before failure’. Αποτέλεσμα αυτού είναι η μεγιστοποίηση του κέρδους των πελατών μέσω της καλύτερης διαχείρισης του στόλου των μηχανημάτων τους.

(Today's Motor Vehicles, 2018)

Airbus

Η Airbus, μία από τις πιο ισχυρές εταιρίες που ασχολούνται με την κατασκευή και συντήρηση αεροσκαφών χρησιμοποιεί τις τεχνολογίες του IoT σε μεγάλο βαθμό. Όχι μόνο εισάγει τις καινούριες τεχνολογίες του IoT στα προιόντα της (αεροπλάνα) αλλά και στα εργαλεία που χρησιμοποιούν οι εργάτες κατά την παραγωγική διαδικασία.

Για την Airbus, το εργοστάσιο του μέλλοντος περιλαμβάνει έναν εργάτη ο οποίος με τη χρήση ενός tablet ή smart glasses μπορεί να οργανώσει μία συγκεκριμένη εργασία και μετά να τη μεταδόσει σε ένα ρομποτικό εργαλείο το οποίο θα εκτελέσει την εργασία με επιτυχία. Συμφωνα με τον Jean-Bernard Hentz, head of PLM R&T & Innovation at Airbus ICT, με το να συνδέεις τους ανθρώπους και τα εργαλεία που χρησιμοποιούν σε μία πλατφόρμα IoT, όχι μόνο επιταχύνει την παραγωγή αλλά και αυξάνει και την αξιοπιστία.

(Anon, 2018)

(Drinkwater, 2018)

Siemens

Οι Γερμανοί πάντα ήταν στην πρώτη γραμμή σε ότι αφορά την καινοτομία στην παραγωγή, άρα γιατί θα αποτελούσε είδηση ότι χρησιμοποιούν ήδη τις τεχνολογίες του IoT? Σε ένα εργοστάσιο στο Amberg, το γερμανικό πάθος για τεχνολογική καινοτομία είναι προσωποποιημένο, όχι με αυτό που κάνουν αλλά με το πώς το κάνουν.

Το Siemens AG plant αποτελεί μέρος της συνολικής προσπάθειας της γερμανικής κυβέρνησης για την ανάπτυξη πλήρως αυτοματοποιημένων, συνδεδεμένων στο Ίντερνετ έξυπνων εργοστασίων.

Το εργοστάσιο που κατασκευάζει αυτόματα μηχανήματα για την BMW ισχυρίζεται ότι είναι το λιγότερο 75% αυτοματοποιημένο με τους 1150 υπαλλήλους να χρησιμοποιούν υπολογιστές και να παρακολουθούν την παραγωγική διαδικασία. Το γεγονός αυτό έχει αυξήσει την απόδοση και έχει μειώσει τα κόστη κάτι που ωστόσο το περιμέναμε από την γερμανική βιομηχανία.

ρεφ (Think Progress UK, 2018)

1.3.2 Έξυπνα αυτοκίνητα

Τα αυτοκίνητα του μέλλοντος θα είναι ασφαλέστερα και για τους επιβάτες αλλά και για τους πεζούς και θα προσφέρουν ασφαλιστικές υπηρεσίες όπως pay-as-you-go insurance δηλαδή, τα ασφάλιστρα θα υπολογίζονται ανάλογα με τον τρόπο που οδηγεί ο κάθε οδηγός. Συνολικά, τα έξυπνα αυτοκίνητα θα προσφέρουν μία πιο συναρπαστική εμπειρία οδήγησης. Η Hewlett Packard συμβάλλει στην ταχύτερη άφιξη του έξυπνου αυτοκινήτου μέσω του συνδυασμού των τεχνολογιών που προσφέρει.

Στις δύο δεκαετίες πριν λανσαριστεί η τεχνολογία OnStar σε συνεργασία μεταξύ General Motors (GM), Hughes Electronics, και EDS, η ιδέα του έξυπνου αυτοκινήτου που θα είναι συνδεδεμένο σε ένα δίκτυο και θα ανταλλάσει πληροφορίες ήταν εξαιρετικά αμφιλεγόμενη. Πέρα από την κεντρική ιδέα του συνδεδεμένου αυτοκινήτου με πρόσβαση στο internet, ανοίγουν και νέες αγορές, όπως Vehicle-to-Infrastructure(V2I), Vehicle-to-Vehicle(V2V), Vehicle-to-Cloud(V2C), Vehicle-to-Pedestrian(V2P), and Vehicle-to-Everything(V2X).

Μία πρόσφατη έρευνα που διεξήχθει από το κεντρικό τμήμα έρευνας της αυτοκινητοβιομηχανίας τόνισε ότι ένα μέσο αυτοκίνητο τώρα περιέχει 60 μικροεπεξεργαστές και πάνω από 10 εκατομμύρια γραμμές κώδικα ενώ οι αντίστοιχες γραμμές κώδικα για ένα αεροπλάνο τύπου Boeing Dreamliner airplane περιορίζονται στο μισό. Τα αυτοκίνητα έχουν αρχίσει να γίνονται ολοένα και πιο έξυπνα και μέχρι το τέλος του 2018, ένα στα πέντε αυτοκίνητα θα έχει γνώση για την κατάστασή του και θα είναι ικανό να μοιράζεται πληροφορίες σχετικά με την μηχανική του κατάσταση, την τοποθεσία του καθώς και να ενημερώνει για την κατάσταση του χώρου στον οποίο βρίσκεται. Η ικανότητα του αυτοκινήτου να αυτοπροσδιορίζεται σε πραγματικό χρόνο μαζί με την ανάγκη να είναι συνεχώς ενεργό, απαιτεί αξιόπιστη σύνδεση στο διαδίκτυο καθώς και λύσεις τύπου Internet of Things.

Η ευρεία χρήση του 4G LTE αλλά και η επερχόμενη τεχνολογία των 5G δικτύων θα αυξήσουν περαιτέρω τις δυνατότητες των έξυπνων αυτοκινήτων και θα διευκολύνουν γρηγορότερη ταχύτητα μετάδοσης και μεγαλύτερο όγκο δεδομένων. Η εταιρίες επικοινωνιών μπορούν εύκολα να παρέχουν μια τέτοιου είδους σύνδεση στο διαδίκτυο ενώ ταυτόχρονα χρειάζεται και η συμβολή ενός ακόμα εταίρου που θα δίνει λύσεις μέσω της τεχνολογίας του Internet of Things για να ικανοποιεί τις ανάγκες της αυτοβιομηχανίας.

Αυτοκινητοβιομηχανία και IoT

Καθώς ο αριθμός των συνδεδεμένων αυτοκινήτων αυξάνεται, η αυτοκινητοβιομηχανία θα κινηθεί με βάση πέντε άξονες:

1) Ψυχαγωγία: επικοινωνία ήχου, εξατομικευμένη μουσική

2) Πλοήγηση: Ενημέρωση για την κίνηση στους δρόμους, εύρεση ταχύτερης διαδρομής

3) Ασφάλεια: Έξυπνη κλήση SOS (eCall), οδική βοήθεια

4) Αποδοτικός υπολογισμός εξόδων: Υπολογισμός ασφάλιστρων, εξ αποστάσεως μηχανικός έλεγχος, συντήρηση

5) Πληρωμές: Ηλεκτρονικές πληρωμές διοδίων, κράτηση θέσης πάρκινγκ και πληρωμή

Η εξέλιξη των έξυπνων αυτοκινήτων από V2I σε V2V, και αυξανόμενου V2X, δίνει τη δυνατότητα στους κατασκευαστές αυτοκινήτων να διαφοροποιηθούν από τους

ανταγωνιστές τους, βασιζόμενοι στις ηλεκτρονικές υπηρεσίες που παρέχουν στους πελάτες. Στην παρακάτω εικόνα παρουσιάζονται μερικά σημαντικά παραδείγματα:

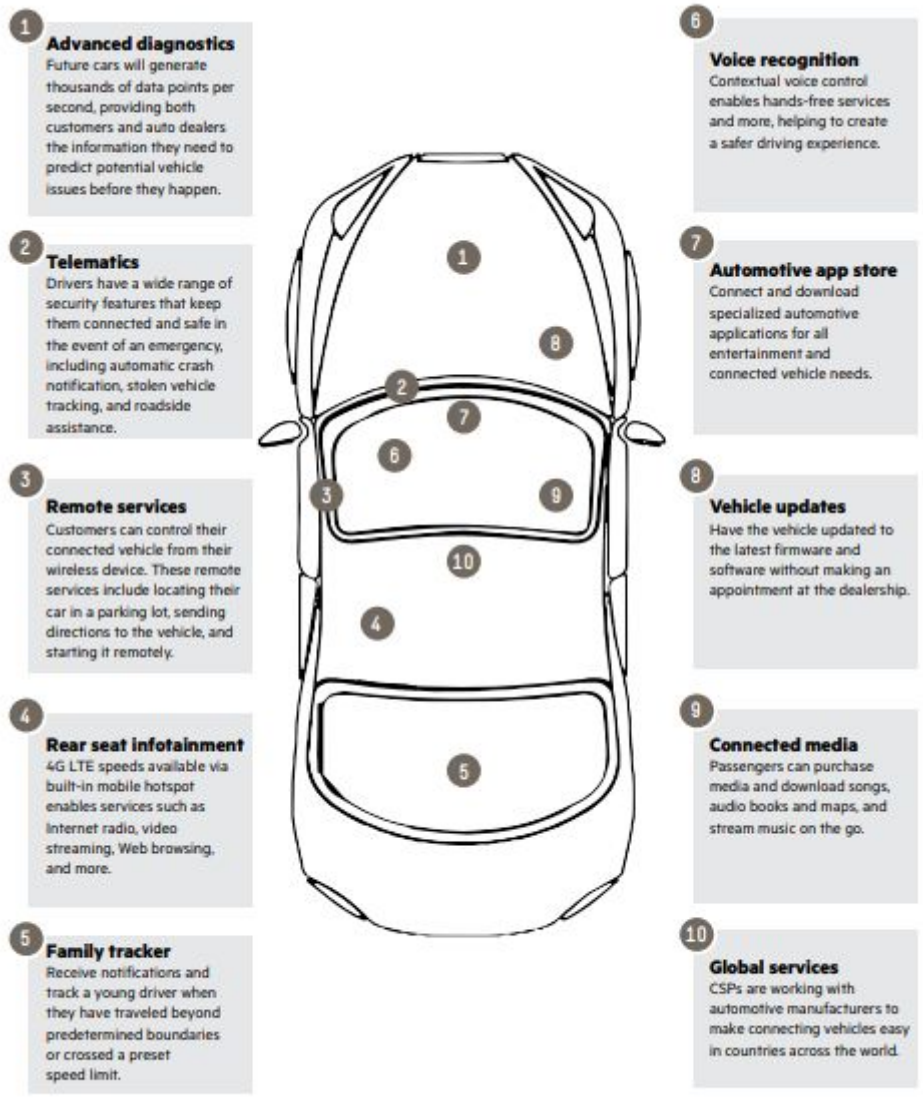


Figure 1. Connectivity differentiation

Παρόλο που τα έξυπνα αυτοκίνητα αυτή τη στιγμή αντιπροσωπεύουν ένα μικρό ποσοστό της ετήσιας αγοράς (10%), εκτιμάται ότι η ζήτηση θα επτά-πλασιαστεί τα επόμενα χρόνια:

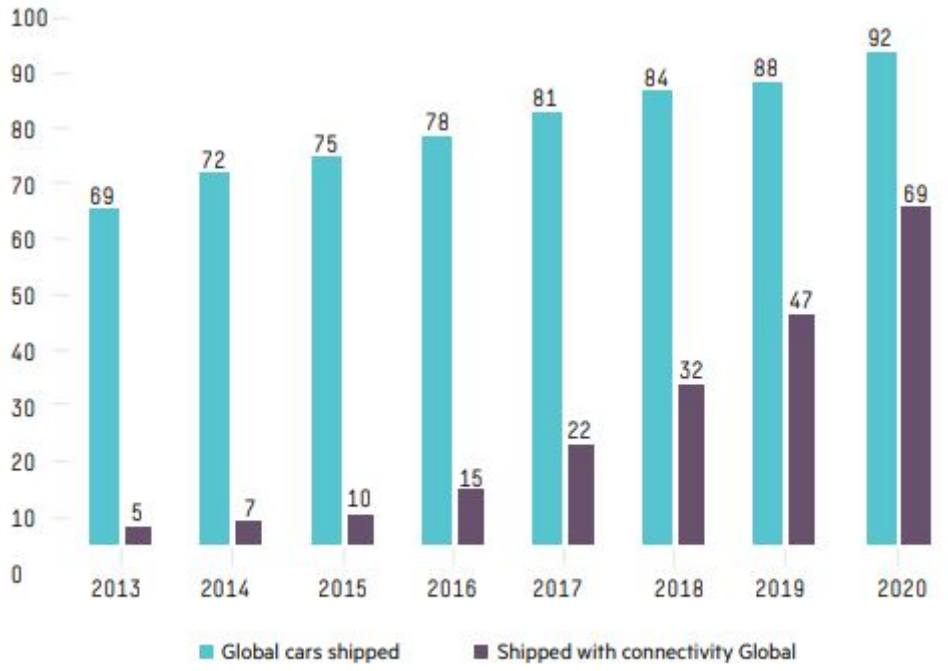


Figure 2. Global connected car growth[1]

Είναι αναμενόμενο λοιπόν ότι η ανάπτυξη αυτών των νέων δυνατοτήτων στα έξυπνα αυτοκίνητα οδηγεί σε αλλαγή τις ροές των εσόδων για τους παραγωγούς των αυτοκινήτων. Εκτιμάται ότι μέχρι το 2020 το 70% όλων των αυτοματοποιημένων ενεργειών των καταναλωτών θα γίνεται ψηφιακά. Τέτοιες ενέργειες μπορεί να είναι η πραγματοποίηση εντολών σε πραγματικό χρόνο από το αυτοκίνητο (για παράδειγμα το να κλείσει από μόνο του ένα ραντεβού για συντήρηση).

Το αυτοκίνητο του μέλλοντος θα είναι και ένα πιο ασφαλές μέρος για όλους. Ιδέες όπως η εφαρμογή της εξυπνάδας του σμήνους (Swarm Intelligence) δίνουν τη δυνατότητα στους οδηγούς να έχουν ενημέρωση σε πραγματικό χρόνο για την κατάσταση του οδοστρώματος καθώς και για τις καιρικές συνθήκες που μπορεί να βρεθούν αντιμέτωποι από άλλα αυτοκίνητα που βρίσκονται σε σχετικά κοντινές αποστάσεις. Για παράδειγμα, ο οδηγός δεν θα ενημερώνεται μόνο για την παρουσία πάγου στο οδόστρωμα αλλά και την ακριβή θέση του στην διαδρομή. Οι επικοινωνίες τύπου V2V και V2X μέσω δυκτίων μεγάλων ταχυτήτων για την μεταφορά δεδομένων καθιστούν ένα τέτοιο πλάνο εφικτό.

Οι δυνατότητες του έξυπνου αυτοκινήτου δεν περιορίζονται μόνο στο να πληρώνει αυτόματα για αγαθά και υπηρεσίες όπως το πετρέλαιο και οι θέσεις parking αλλά περιλαμβάνουν και το θέμα της ασφάλειας. Τα ασφάλιστρα θα υπολογίζονται διαφορετικά καθώς θα λαμβάνεται υπόψιν και ο τρόπος που οδηγεί ο κάθε οδηγός (pay-how-you-drive insurance). Η μέθοδος αυτή θα επιβραβεύει τους καλούς οδηγούς

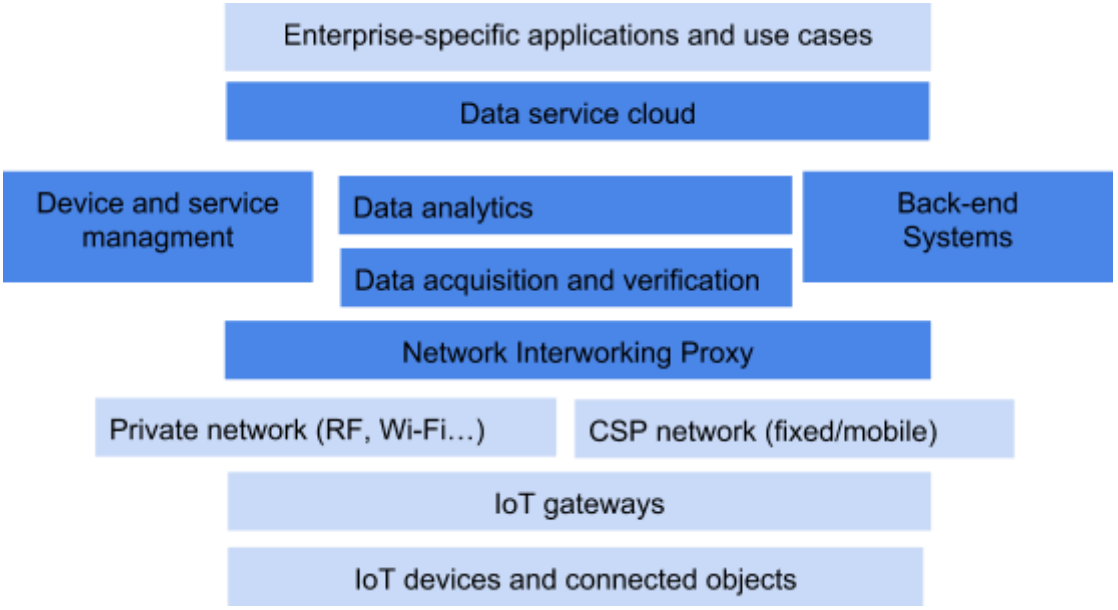
μειώνοντάς τους τα ασφάλιστρα τους. Αντίθετα, οι απρόσεκτοι οδηγοί θα κληθούν να πληρώσουν παραπάνω. Βλέποντας όλες αυτές τις καινοτομίες που φέρνει το έξυπνο αυτοκίνητο είναι προφανές ότι η χρήση αυτών των νέων τεχνολογιών κάνει την οδήγηση μια συναρπαστική εμπειρία.

IoT Platform

Η αρχιτεκτονική για την πλατφόρμα IoT που χρησιμοποιεί η HPE διαμορφωμένη σε επίπεδα παρουσιάζεται παρακάτω. Η πλατφόρμα αυτή δίνει τη δυνατότητα στις εταιρίες CSP (Communication Service Providers) να παρουσιάσουν καινούρια use cases και γρήγορα να πετύχουν επιτυχή αποτελέσματα, τα οποία περιλαμβάνουν:

- ❏ Μειωμένη πολυπλοκότητα λόγω της χρήσης προ-ολοκληρωμένων μοντέλων για την απόκτηση, έλεγχο και ανάλυση δεδομένων
- ❏ Μειωμένος κίνδυνος λόγω της συμμόρφωσης με το oneM2M πρότυπο
- ❏ Γρηγορότερο time-to-value λόγω της χρήσης των μοντέλων τύπου "as-a-Service"

HPE Universal IoT Platform layered architecture:



1.3.3 Τομέας Έξυπνων Υποδομών

Η ενσωμάτωση έξυπνων αντικειμένων σε φυσικές υποδομές μπορεί να βελτιώσει την ευελιξία, την αξιοπιστία και την αποτελεσματικότητα στη λειτουργία των υποδομών. Αυτά τα οφέλη μπορούν να μειώσουν το κόστος και τις απαιτήσεις σε ανθρώπινο δυναμικό, καθώς και να ενισχύσουν την ασφάλεια.

Έξυπνο Σπίτι

Στη σημερινή εποχή, το Έξυπνο Σπίτι αποτελεί αναδυόμενη εφαρμογή και προσφέρει ένα σύστημα διαχείρισης κατοικιών με κύρια χαρακτηριστικά την άνεση, την ευκολία, την εξοικονόμηση ενέργειας και την ασφάλεια. Ο ορισμός του συνδεδεμένου σπιτιού είναι διαφορετικός για διαφορετικούς ανθρώπους. Με απλά λόγια, ένα έξυπνο σπίτι είναι αυτό στο οποίο οι συσκευές έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους καθώς και με το "έξυπνο" περιβάλλον τους. Ένα έξυπνο σπίτι δίνει τη δυνατότητα στον ιδιοκτήτη να προσαρμόζει και να ελέγχει το περιβάλλον του σπιτιού. Το σύστημα θέρμανσης μπορεί να προσαρμοστεί στις προτιμήσεις του ιδιοκτήτη και στον καιρό. Τα φώτα μπορούν να αλλάζουν και να

προσαρμοστούν ανάλογα με την ώρα της ημέρας και της νύχτας. Με την κατάλληλη παρακολούθηση και τα συστήματα συναγερμού, μπορεί να μειωθούν ή να αποφευχθούν περιστατικά διάρρηξης. Το κόστος της ενέργειας μπορεί να μειωθεί, σβήνοντας αυτόματα τις ηλεκτρικές συσκευές όταν αυτές δεν χρησιμοποιούνται. Υπάρχουν πλέον πολλές διαθέσιμες τεχνολογίες IoT για την παρακολούθηση και οικοδόμηση των έξυπνων σπιτιών. Κατασκευαστές καταναλωτικών προϊόντων όπως οι Belkin, Philips, Amazon και Haier έχουν ήδη καθοριστεί ως εξέχουσες εταιρείες στην αγορά αυτή.

Στη συνέχεια, θα περιγραφούν οι κύριες λειτουργίες που προσφέρει το Έξυπνο Σπίτι με σκοπό τη βελτίωση της ποιότητας ζωής του ανθρώπου και τη διευκόλυνση της καθημερινότητάς του: (Καλύβας Βασίλειος)

1.3.4 Έξυπνες Εφαρμογές

Έλεγχος φωτισμού

Οι ένοικοι θα μπορούν να ελέγχουν το φωτισμό της κατοικίας, είτε βρίσκονται εντός είτε εκτός της οικίας. Μέσω κατάλληλου εξοπλισμού και εφαρμογών σε smartphone ή tablet, ο χρήστης θα έχει τη δυνατότητα να ενεργοποιεί και να απενεργοποιεί τα φώτα και να καθορίζει την έντασή τους. Επίσης, ο φωτισμός μπορεί να ρυθμιστεί εκ των προτέρων, ώστε να προσαρμόζεται σε συγκεκριμένες καταστάσεις της ημέρας ή ανάλογα με τη διάθεση του/των ενοίκων. Θα προσφέρεται και η δυνατότητα αυτόματης ενεργοποίησης/απενεργοποίησης όταν ο χρήστης εισέρχεται/εξέρχεται από την οικία, αντίστοιχα.

Έλεγχος Κλιματισμού (HVAC – Heating, Ventilating and Air-Conditioning)

Κατά παρόμοιο τρόπο, ο χρήστης θα μπορεί να ελέγχει το σύστημα θέρμανσης και ψύξης της οικίας, ακόμα και κατά απομακρυσμένο τρόπο μέσω κατάλληλων εφαρμογών. Θα παρέχεται η δυνατότητα αυτόματης ρύθμισης των συστημάτων αυτών για εξοικονόμηση ενέργειας, ανάλογα με τα επίπεδα θερμοκρασίας και υγρασίας εντός της κατοικίας. Επίσης, θα πραγματοποιείται και ανίχνευση πιθανών επιβλαβών αερίων μέσα στο οικιακό περιβάλλον.

Έξυπνη παρακολούθηση

Πρόκειται για πολύ χρήσιμο χαρακτηριστικό του WHA, καθώς δίνεται η δυνατότητα παρακολούθησης, μέσω καμερών συνδεδεμένων στο Διαδίκτυο, της κατάστασης μιας κατοικίας όταν οι ένοικοι απουσιάζουν, ακόμα και όταν βρίσκονται σε διακοπές. Η βασικότερη χρήση του, αφορά την απομακρυσμένη επιτήρηση ατόμων με ειδικές ανάγκες, ανήλικων παιδιών και ηλικιωμένων, ώστε σε περίπτωση έκτακτης ανάγκης, να εντοπιστεί το πρόβλημα και να παρασχεθεί η κατάλληλη βοήθεια είτε από συγγενείς είτε από εξειδικευμένο ιατρικό προσωπικό.

Έξυπνο κλείδωμα και σύστημα αυτόματης ασφάλειας

Η οικιακή ασφάλεια αποτελεί πολύ σημαντικό ζήτημα και, ως εκ τούτου, δεν θα μπορούσε να παραλειφθεί. Όταν ανιχνευθεί απόπειρα παραβίασης ή κακόβουλης επίθεσης εναντίον μιας κατοικίας (π.χ. ρίψη αντικειμένων), το σύστημα αυτόματης ασφάλειας ειδοποιεί αμέσως το χρήστη με την αποστολή e-mail ή SMS στο κινητό του τηλέφωνο. Επιπλέον, υπάρχει η δυνατότητα αυτόματης ασφάλισης της κατοικίας όταν ο ένοικος εξέρχεται από αυτή και αυτόματης απενεργοποίησής της όταν επιστρέφει.

Έλεγχος έξυπνων συσκευών

Στο εσωτερικό των κατοικιών αναμένεται να υπάρχει πλήθος έξυπνων συσκευών, τις οποίες οι ένοικοι θα είναι σε θέση κάθε χρονική στιγμή να διαχειρίζονται από το smartphone, το tablet ή το laptop τους, ακόμα και όταν απουσιάζουν. Ειδικά στην περίπτωση αυτή, θα υπάρχει η δυνατότητα αυτόματης απενεργοποίησης των έξυπνων συσκευών, προς εξοικονόμηση ηλεκτρικής ενέργειας. Τέτοιες συσκευές είναι τα ψυγεία, οι φούρνοι, οι τηλεοράσεις, τα συστήματα θέρμανσης και ψύξης, οι θερμοστάτες, τα συστήματα φωτισμού κτλ.

Έξυπνη καταγραφή μετρήσεων

Ο ένοικος θα έχει την πλήρη γνώση των μετρήσεων της κατανάλωσης ενέργειας στην οικία του. Θα παρέχονται λεπτομερή στοιχεία και γραφήματα σχετικά με τις ώρες λειτουργίας, την ενεργειακή κατανάλωση, το προφίλ χρησιμοποίησης των έξυπνων συσκευών και γενικότερα όλου του εξοπλισμού εντός της οικίας.

Έξυπνη ρύθμιση κατανάλωσης ενέργειας

Έχοντας, όπως αναφέρθηκε προηγουμένως, λεπτομερείς μετρήσεις, ο ένοικος θα είναι πλέον σε θέση να ρυθμίζει τη λειτουργία των έξυπνων συσκευών με στόχο τη μείωση της κατανάλωσης ενέργειας. Θα λαμβάνει αποφάσεις για το ποιες συσκευές θα λειτουργούν, σε ποιες ώρες της ημέρας, για πόσο χρονικό διάστημα, καθώς και αν χρειάζονται αντικατάσταση.

Ένα καλό παράδειγμα αποτελεί η συσκευή **Nest Learning Thermostat**

Nest Learning Thermostat: Είναι μια πραγματικά IoT έξυπνη συσκευή που μαθαίνει την θερμοκρασία που προτιμά ο ιδιοκτήτης μέσα στο σπίτι. Δεν χρειάζεται να ρυθμίζεται η θερμοκρασία του δωματίου/σπιτιού κάθε φορά, ούτε να προγραμματίζεται ο θερμοστάτης, διότι είναι πλέον αυτοπρογραμματιζόμενος, δηλαδή μαθαίνει από τον ιδιοκτήτη και προγραμματίζει τον εαυτό του (autoSchedule). Δεν ζεσταίνει ή κρυώνει ένα άδειο σπίτι, απλά προσαρμόζει (κλείνει ή μειώνει) την θερμοκρασία αφού αδειάσει αυτό (auto-Away). Διαθέτει απομακρυσμένο έλεγχο και μαζί με την Nest εφαρμογή μπορεί κανείς να αλλάξει την θερμοκρασία του σπιτιού, να δει το ιστορικό της ενέργειας και να πάρει ειδοποίηση εάν το σπίτι είναι πολύ ζεστό ή κρύο. Τέλος σε ενημερώνει αν έχει επιλεγεί μια θερμοκρασία που κάνει οικονομία ενέργειας .

(Internet Of Things Wiki, 2018)

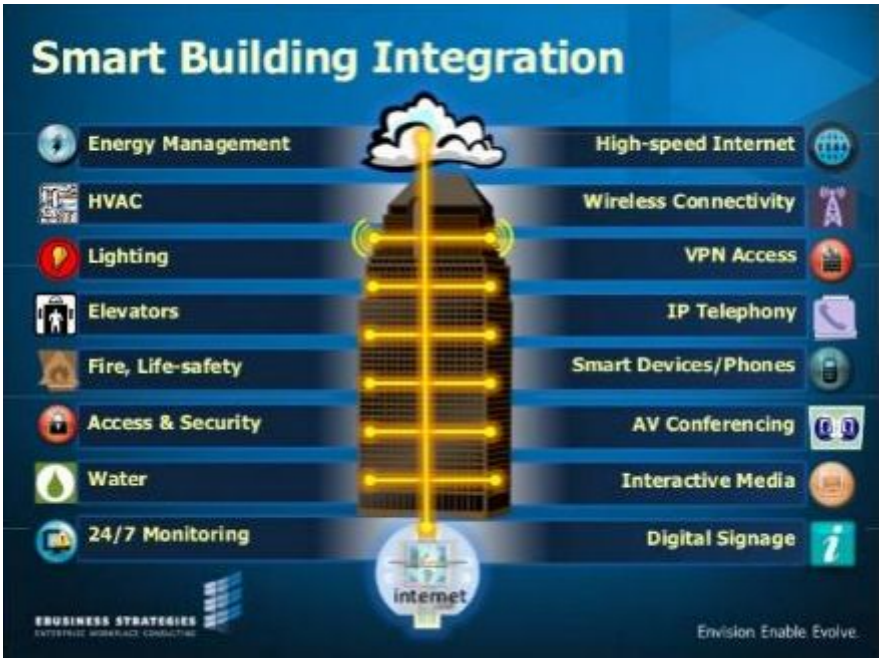
1.3.5 Έξυπνα κτίρια

Τα έξυπνα κτίρια έχουν περιβαλλοντική συνείδηση, προσαρμοστικότητα στις κλιματολογικές συνθήκες, σέβονται και φροντίζουν την υγεία του χρήστη. Για να χαρακτηρισθεί ένα κτίριο ως «Έξυπνο» πρέπει να καλύπτονται τουλάχιστον οι εξής περιοχές λειτουργίας:

Ι)Αποδοτικότητα συστήματος ενέργειας (έλεγχος και εξοικονόμηση ενέργειας, έλεγχος κλιματισμού, θέρμανσης και εξαερισμού, ασύρματοι διακόπτες, σύστημα αδιάλειπτης παροχής ενέργειας)

ΙΙ)Συστήματα ασφάλειας τόσο για το κτίριο, όσο και για τη ζωή των ανθρώπων που βρίσκονται σε αυτό (ασφάλεια, πυρασφάλεια, αυτοματισμός, παρακολούθηση κατάστασης υγείας – health status monitoring) και

ΙΙΙ)Συστήματα τηλεπικοινωνιών (συστήματα επικοινωνίας δεδομένων, εικόνας, ήχου)



Ένα Έξυπνο Κτίριο παρέχει τις παραπάνω δυνατότητες χρησιμοποιώντας:[10]

Αυτοματοποιημένα συστήματα ελέγχου για θέρμανση, εξαερισμό, ψύξη (συστήματα HVAC). Για παράδειγμα ο κλιματισμός και η θέρμανση τίθενται σε λειτουργία ανάλογα με την εξωτερική θερμοκρασία. Με αυτό τον τρόπο επιτυγχάνεται μείωση κατανάλωσης ενέργειας, τουλάχιστον κατά το ήμισυ, σε σύγκριση με τα συμβατικά κτίρια.

Έλεγχος και εξοικονόμηση ενέργειας μέσα από «αισθητήρια» συστήματα, όπως ευφυής θερμοστάτες, οι οποίοι μετά από μερικές ημέρες μαθαίνουν το πρόγραμμα των ανθρώπων που βρίσκονται στο κτίριο και στην συνέχεια το εφαρμόζουν μόνοι τους. Επιπλέον, μπορείς με την βοήθεια μιας εφαρμογής και ενός έξυπνου τηλεφώνου, να συνδεθείς σ' έναν θερμοστάτη και να δεις το ιστορικό ενέργειας, πόση ενέργεια αποθηκεύεται ώστε να έχεις τον απομακρυσμένο έλεγχό του. Τέλος, η

έξυπνη διαχείριση ενέργειας, δεν περιλαμβάνει μόνο πρακτικές και μόνιμα μέτρα εξοικονόμησης ενέργειας (ή καθημερινά μέτρα εφαρμοζόμενα απ' τους καταναλωτές), αλλά και δυναμικές παραμέτρους όπως αμφίδρομη επικοινωνία επιμέρους χώρων – κτιρίου και αντίστοιχη επικοινωνία του κτιρίου με το δίκτυο στο οποίο είναι συνδεδεμένο.

Έλεγχος εσωτερικού κλίματος

Μέτρηση και έλεγχο της θερμοκρασίας, του CO2, του φρέσκου αέρα και του φωτισμού. Ενδεικτικά αναφέρονται, η αυξομείωση της έντασης του φωτισμού ανάλογα με την φωτεινότητα του χώρου, η δυνατότητα σεναρίων φωτισμού, ο έλεγχος κίνησης ή στην περίπτωση που η εξωτερική θερμοκρασία αρχίζει να αυξάνεται, το έξυπνο κτίριο θέτει αυτομάτως σε λειτουργία τα κλιματιστικά.

Πυρανίχνευση

Σύστημα με αισθητήρες μέτρησης καπνού και μονοξειδίου του άνθρακα, δίνοντας έτσι έγκαιρες προειδοποιήσεις, ενεργοποιώντας συναγερμούς και μιλώντας με ανθρώπινη φωνή λέγοντάς σου που βρίσκεται ο καπνός ή αν τα επίπεδα του μονοξειδίου του άνθρακα αυξάνονται.

Ανίχνευση κίνησης

Αισθητήρες κίνησης, οι οποίοι μπορούν να χρησιμοποιούν τόσο στο τομέα της ασφάλειας όσο και στην ανίχνευση παρουσίας μέσα στο κτίριο, όπου παραδείγματος χάριν εάν είναι Σαββατοκύριακο και το κτίριο είναι άδειο, μπορεί να κλείνει αυτόματα η παροχή του νερού, να απενεργοποιούνται όλα τα φώτα και συγκεκριμένες πρίζες ή να λειτουργούν μόνο στον χώρο/χώρους που εντοπίζονται άνθρωποι.

Εντοπισμός ύπαρξης πλημμύρας

Ανίχνευση υγρού π.χ. σε κέντρα δεδομένων, αποθήκες και ευαίσθητα οικόπεδα για την αποφυγή βλαβών και διάβρωσης.

Τέχνη και Προϊόντα Συντήρησης

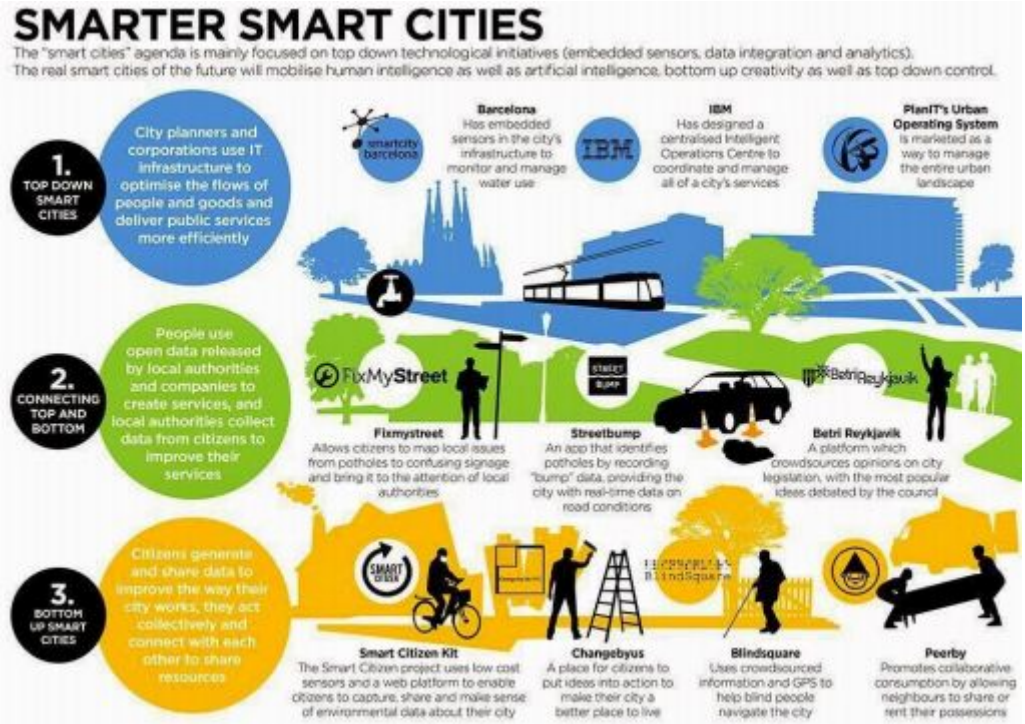
Παρακολούθηση των εσωτερικών συνθηκών στα μουσεία και στις αποθήκες τέχνης. Στο μουσείο ανάλογα με τα εκθέματα, στη κάθε αίθουσα, μπορεί το κτήριο να ρυθμίζει τις συνθήκες στην αίθουσα ώστε να προσομοιώνονται με τα εκθέματα.

Συστήματα ήχου/εικόνας, Η/Υ, επικοινωνίες, αυτοματισμοί γραφείου, ανελκυστήρες, διαφυγή σε περίπτωση κινδύνου και τέλος μείωση των αποβλήτων είναι μερικά ακόμα από τα χαρακτηριστικά των έξυπνων κτιρίων.

Για να γίνουν όλα τα παραπάνω σωστά και συντονισμένα, τα κτίρια χρειάζονται έναν "εγκέφαλο", ένα σύστημα κεντρικής διαχείρισης, που να ελέγχει έξυπνα τα διάφορα υποσυστήματα. Με την ενοποίηση των υποσυστημάτων, τα δεδομένα συντονίζονται και μετατρέπονται σε πληροφορίες που βοηθούν στη λήψη αποφάσεων και ενεργειών, οι οποίες ενισχύουν την απόδοση, την άνεση και την ευεξία των ενοίκων και των ιδιοκτητών του κτιρίου.

1.3.6 Έξυπνες Πόλεις

"Έξυπνη πόλη" ονομάζεται εκείνη η πόλη που αξιοποιεί σύγχρονες τεχνολογίες, με στόχο, αφενός να βελτιώσει την καθημερινότητα των πολιτών της, παρέχοντας όσο το δυνατόν καλύτερη ποιότητα ζωής, αφετέρου να ενισχύσει τη συμμετοχή τους στη λήψη αποφάσεων για θέματα που τους αφορούν. Αυτό στην πράξη μεταφράζεται σε υπηρεσίες ηλεκτρονικής διακυβέρνησης, δημόσια δεδομένα ανοικτά στους πολίτες, ώστε και οι βασικές υπηρεσίες μιας πόλης να καταστούν περισσότερο προσβάσιμες και οι πολίτες να συνεισφέρουν στον εντοπισμό αλλά και στην επίλυση προβλημάτων, σε ευρυζωνικές συνδέσεις στο διαδίκτυο, αξιοποίηση φιλικών προς το περιβάλλον ΤΠΕ, έξυπνη παρακολούθηση, έξυπνο πάρκινγκ, υποδομές υγείας, έξυπνα φώτα, διαχείριση σκουπιδιών, έξυπνοι δρόμοι, ασφαλέστερη και αυτοματοποιημένη μεταφορά, έξυπνα συστήματα διαχείρισης ενέργειας και περιβαλλοντικής παρακολούθησης. Όλα τα ανωτέρω είναι παραδείγματα του Διαδικτύου των Πραγμάτων για τις έξυπνες πόλεις.



Στη συνέχεια, θα αναλυθούν κάποιες λειτουργίες που προσφέρουν οι Έξυπνες πόλεις (IERC Cluster Book, 2014)

Έξυπνο πάρκινγκ

Παρακολούθηση σε πραγματικό χρόνο της διαθεσιμότητας χώρων στάθμευσης στην πόλη, επιτρέποντας έτσι στους κατοίκους να εντοπίζουν και να δεσμεύουν την πλησιέστερη διαθέσιμη θέση παρκινγκ. Μερικά από τα οφέλη είναι, η μείωση της κυκλοφοριακής συμφόρησης και η αύξηση των εσόδων από την δυναμική τιμολόγηση του πάρκινγκ.

Διαχείριση σκουπιδιών

Ανίχνευση του επιπέδου των σκουπιδιών για τη βελτιστοποίηση των δρομολογίων συλλογής των απορριμμάτων. Κάδοι απορριμμάτων και ανακύκλωσης με ετικέτες RFID, επιτρέπουν στο προσωπικό υγιεινής, να δουν πότε άδειασε τελευταία φορά ο κάδος. Ίσως ένα πρόγραμμα "Pay as you Throw" να μειώσει τα σκουπίδια και να εντείνει τις προσπάθειες της ανακύκλωσης.

Έξυπνο σύστημα μεταφορών

Έξυπνοι δρόμοι και αυτοκινητόδρομοι με προειδοποιητικά μηνύματα και εκτροπές ανάλογα με κλιματολογικές συνθήκες και απροσδόκητα γεγονότα όπως ατυχήματα ή κυκλοφοριακή συμφόρηση. Φανάρια με ενσωματωμένους αισθητήρες βίντεο, που

μπορούν να προσαρμόσουν τα πράσινα και τα κόκκινα, ανάλογα με το που είναι τα αυτοκίνητα και την ώρα της ημέρας, μειώνοντας έτσι την κυκλοφοριακή συμφόρηση και την αιθαλομίχλη, δεδομένου ότι τα οχήματα στο ρελαντί στα κόκκινα φανάρια καίνε έως και 17% από τα καύσιμα που καταναλώνονται σε αστικές περιοχές, Σαν αποτέλεσμα θα έχουμε λιγότερη κατανάλωση καυσίμων, άρα και μείωση της ατμοσφαιρικής ρύπανσης.

Έξυπνος τουρισμός

Smartphone εφαρμογές που υποστηρίζονται από τους QR κώδικες και ετικέτες NFC παρέχουν ενδιαφέρουσες και χρήσιμες τουριστικές πληροφορίες σε όλη την πόλη. Οι πληροφορίες θα μπορούσαν να περιλαμβάνουν μουσεία, πινακοθήκες, βιβλιοθήκες, τουριστικά αξιοθέατα, γραφεία τουρισμού, τα μνημεία, τα καταστήματα, λεωφορεία, ταξί, κήπους, κλπ

Δύο «έξυπνες» εφαρμογές στάθμευσης και φωτισμού θα εγκατασταθούν στην Χαλκίδα, την πρώτη πόλη στην Ελλάδα, υποστηριζόμενα από μία ενιαία πλατφόρμα έξυπνης πόλης. Οι δυο εφαρμογές αυτές, θα συμβάλλουν στην αποσυμφόρηση της κυκλοφορίας και στη μείωση κατανάλωσης ενέργειας στην πόλη της Χαλκίδας. Σύμφωνα με ανακοίνωση του Ομίλου ΟΤΕ, σε ότι αφορά την εφαρμογή "Smart Parking" στο πλαίσιο του έργου θα εγκατασταθούν, σε κεντρικό σημείο της Χαλκίδας, ειδικοί αισθητήρες έξυπνης στάθμευσης, οι οποίοι μέσω εφαρμογής στο κινητό, που αναπτύχθηκε από την OTS, θα ενημερώνουν τους οδηγούς που βρίσκονται ελεύθερες θέσεις στάθμευσης και πως θα φτάσουν εκεί.

(Νέα, κατάλογος για Αλληλέγγυα, Κοινωνική Οικονομία enallaktikos.gr, 2018)

Το Τελ Αβίβ αντιμετωπίζει τη κίνηση στους πιο πολυσύχναστους δρόμους, εξασφαλίζοντας μία λωρίδα κυκλοφορίας για λεωφορεία και ταξί, επιτρέποντας όμως στους ανυπόμονους οδηγούς ή σ' αυτούς με τις βαθιές τσέπες να χρησιμοποιούν την ορισθείσα λωρίδα, με το ανάλογο αντίτιμο. Αισθητήρες στην άσφαλτο παίρνουν τον αριθμό της πινακίδας του αυτοκινήτου και χρεώνεται αυτόματα στην πιστωτική κάρτα του ιδιοκτήτη ένα ποσό, που ποικίλλει ανάλογα με το πόση κυκλοφοριακή συμφόρηση παρουσιάζει ο δρόμος.

Πηγή(The Globe and Mail, 2018)

1.3.7 Τομέας Ενέργειας

Το Έξυπνο δίκτυο (Smart Grid) ενσωματώνει δυνατότητες επικοινωνίας με τα δίκτυα κοινής ωφέλειας (π.χ. ηλεκτρική ενέργεια, φυσικό αέριο, νερό) και τις υποδομές, για την αυτοματοποίηση της παρακολούθησης και του ελέγχου. Βασικές εφαρμογές

έξυπνων δικτύων είναι οι έξυπνοι μετρητές, η αυτοματοποίηση του δικτύου διανομής, η ανταπόκριση στην ζήτηση, η διάγνωση εξοπλισμού καθώς και η παρακολούθηση και ο έλεγχος της κατάστασης του δικτύου ευρείας περιοχής. Το έξυπνο δίκτυο μπορεί ανά πάσα στιγμή να γνωρίζει τις μεταβλητές της κατάστασής του, να βελτιώνει τον εντοπισμό, την απόκριση ακόμα και την πρόβλεψη σφαλμάτων και καταστροφών, μειώνοντας έτσι τις απώλειες που προκαλούνται από αυτά και τους χρόνους διακοπών παροχής ενέργειας.

(Geng Wu et al., 2011) Τα κύρια σενάρια εφαρμογής του IoT στα έξυπνα δίκτυα είναι:

- (Ευφροσύνη Θ. Ζώτου, 2012) Στον τομέα της παραγωγής ενέργειας, το IoT μπορεί να χρησιμοποιηθεί για την παρακολούθηση της μονάδας, των κατανεμημένων σταθμών ηλεκτροπαραγωγής, της περιοχής των σταθμών παραγωγής, των ρύπων και των εκπομπών αερίων, της ενεργειακής κατανάλωσης, του υλικού του άνθρακα, της αιολικής μονάδας παραγωγής, των φωτοβολταϊκών σταθμών παραγωγής, της παραγωγής ηλεκτρικής ενέργειας από βιομάζα, της αποθήκευσης ενέργειας, της διασύνδεσης ηλεκτρικής ενέργειας κτλ.

- Το IoT επίσης χρησιμοποιείται ευρέως για την παρακολούθηση των γραμμών μεταφοράς, την προστασία των πύργων, τους έξυπνους υποσταθμούς, την αυτοματοποίηση της διανομής, την παρακολούθηση της κατάστασης διανομής και για τη διαχείριση της λειτουργίας και του εξοπλισμού.

- Το IoT χρησιμοποιείται κυρίως για τους έξυπνους μετρητές και τη μέτρηση κατανάλωσης ενέργειας, τη σύγκλιση του πολύ-δικτύου, τα ηλεκτρικά οχήματα και τη φόρτισή τους, την παρακολούθηση και διαχείριση της ενεργειακής απόδοσης και για τη διαχείριση ζήτησης, η οποία αποτελεί σημαντική εξοικονόμηση στην κατανάλωση πόρων όταν η παροχή ταιριάζει δυναμικά με τη ζήτηση.

Έξυπνα συστήματα καταμέτρησης (Smart metering)

Μεταξύ των έξυπνων συστημάτων καταμέτρησης πρώτος έρχεται ο μετρητής κατανάλωσης ηλεκτρικής ενέργειας. Εκτός από το να καταγράφει πόσες kWh έχουν καταναλωθεί από την ηλεκτρική εγκατάσταση, θα πρέπει να μπορεί να δίδει και άλλες πληροφορίες όπως οι δυνατότητες άμεσης τηλεανάγνωσης της κατανάλωσης αλλά και δημιουργίας στατιστικών χρήσης και αξιοποίησής τους από το εσωτερικό του κτιρίου. Η πλέον ενδιαφέρουσα δυνατότητα που δίδεται στον καταναλωτή είναι το να μπορεί να ελέγχει κάθε στιγμή την κατανάλωσή του, άρα και το κόστος της ενέργειας που καταναλώνει από το εσωτερικό της κατοικίας του. Οι πληροφορίες αυτές μπορούν να μεταδίδονται από το μετρητή προς την κατοικία είτε μέσω του δικτύου (της παροχής) ή ασύρματα με την τεχνική KNX-RF. Ο καταναλωτής θα μπορεί (αν θέλει βέβαια) να λαμβάνει τις πληροφορίες για την ενέργεια που

καταναλώνει μέσω του υπολογιστή του (με ειδικό modem) ή μέσω ενός ειδικού panel. Αντίστοιχες εξελίξεις προβλέπονται για τους μετρητές κατανάλωσης νερού και αερίου.

Έξυπνες ΑΠΕ

Με την χρήση των τεχνολογιών του έξυπνου δικτύου διευκολύνεται η ενσωμάτωση ενός μεγάλου εύρους κατανεμημένων πηγών παραγωγής, από ανανεώσιμες πηγές ενέργειας, όπως φωτοβολταϊκά και ανεμογεννήτριες, μέχρι μικρής κλίμακας συστήματα συμπαραγωγής ηλεκτρικής και θερμικής ενέργειας, καθώς και συστημάτων αποθήκευσης ενέργειας. Μέσα από τη χρήση εξελιγμένων εργαλείων μοντελοποίησης και ανάλυσης των συστημάτων, υποστήριξης αποφάσεων, πρόβλεψης καιρού και πρόβλεψης κατάστασης φορτίου μέσω μηχανικής μάθησης, η εισαγωγή των πηγών αυτών στο δίκτυο θα μπορεί να γίνει με πολύ μεγαλύτερη ευκολία σε σύγκριση με το δίκτυο του παρελθόντος.(Παντισκα Λεονάρδος,2016)

- Φωτοβολταϊκές εγκαταστάσεις: Παρακολούθηση και βελτιστοποίηση της απόδοσης στον τομέα της ηλιακής ενέργειας.
- Ανεμογεννήτριες: Παρακολούθηση και ανάλυση της ροής της ενέργειας από ανεμογεννήτριες και αμφίδρομη επικοινωνία με τους ευφυείς μετρητές των καταναλωτών για την ανάλυση καταναλωτικών προτύπων.

Έξυπνοι καταναλωτές

Στα συστήματα του έξυπνου δικτύου, ο ρόλος των καταναλωτών αλλάζει και πλέον από παθητικοί χρήστες γίνονται ενεργοί συμμετέχοντες στη διαχείριση της ενέργειάς τους. Με τη χρήση εξελιγμένου υλικού, όπως έξυπνοι μετρητές και έξυπνες συσκευές, λογισμικού και τεχνολογιών επικοινωνίας, οι καταναλωτές έχουν μια πληθώρα πληροφοριών στη διάθεσή τους, οι οποίες τους βοηθούν στο να παίρνουν αποφάσεις και κάνουν δυνατή την εφαρμογή ενεργειών, όπως η τιμολόγηση πραγματικού χρόνου και η απόκριση σε αιτήματα των εταιρειών για μείωση φορτίου στις ώρες αιχμής του δικτύου, με οικονομικά και περιβαλλοντικά οφέλη και για τις εταιρείες αλλά και για τους καταναλωτές. Ακόμα, στο έξυπνο ηλεκτρικό δίκτυο κάθε καταναλωτής μπορεί να γίνει και παραγωγός, θέτοντας απλά στην υπηρεσία του συστήματος τα δεδομένα χρήσης των οικιακών του συσκευών, δηλαδή, πότε και πόση ώρα χρησιμοποιεί πχ το πλυντήριο ρούχων, ώστε τη συγκεκριμένη στιγμή να μπορεί το δίκτυο να μειώνει τη παροχή ρεύματος στο συγκεκριμένο σπίτι και να τη διαθέτει σε έναν άλλο χρήστη, χωρίς κάτι τέτοιο να προκαλεί δυσλειτουργίες.

Έξυπνη μετακίνηση

Με την αυξανόμενη χρήση ηλεκτρικών οχημάτων με σκοπό τη μείωση των εκπομπών αερίων που συμβάλλον στο φαινόμενο του θερμοκηπίου, δημιουργούνται καινούργιες καμπύλες φορτίων στο δίκτυο και νέες ανάγκες διαχείρισης αυτών των οχημάτων. Τα έξυπνα δίκτυα θα οδηγήσουν στην πιο ομαλή ενσωμάτωση και στρατηγική διαχείριση αυτών των φορτίων, καθώς και στην εκμετάλλευσή τους για την παροχή υπηρεσιών ως συσκευές αποθήκευσης ενέργειας.

Έξυπνοι πάροχοι υπηρεσιών

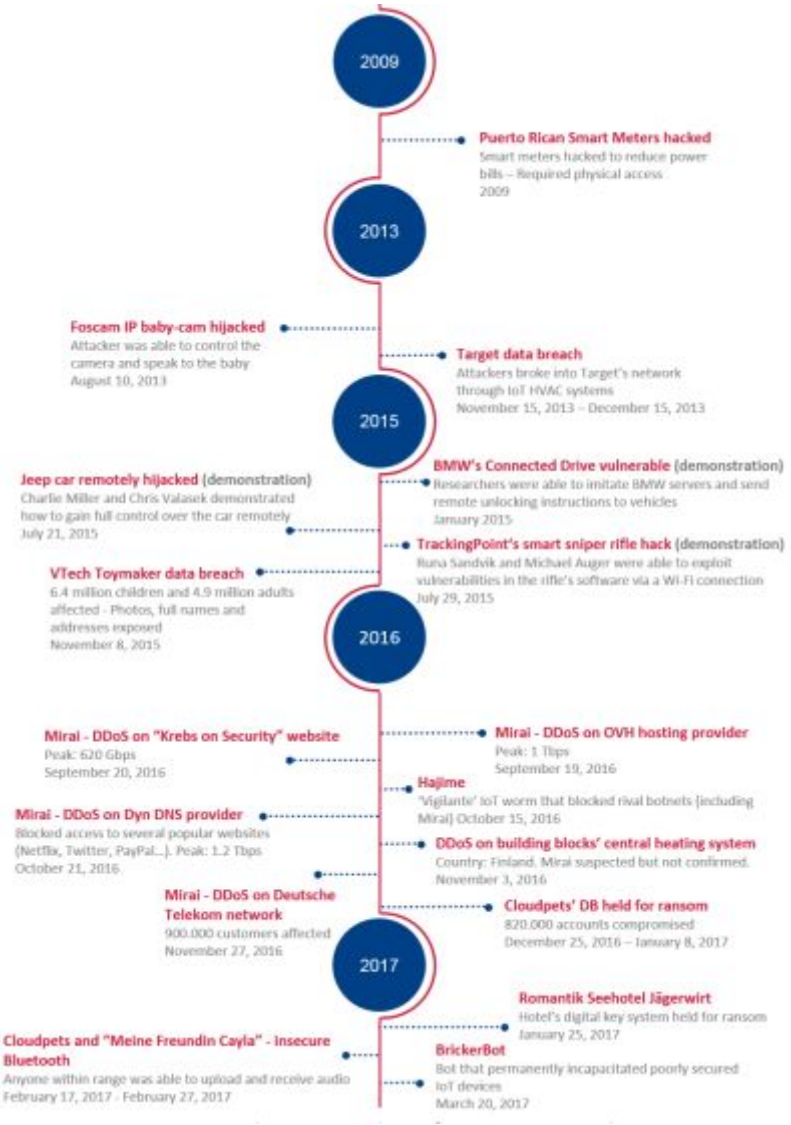
Στην εποχή του έξυπνου δικτύου και με την απελευθέρωση της αγοράς ενέργειας, οι εταιρείες ηλεκτρισμού δεν θα είναι πλέον οι μόνοι σημαντικοί παίκτες στις αγορές. Οι νέες τεχνολογίες οδηγούν στην ανάπτυξη νέων και καινοτόμων ευκαιριών, υπηρεσιών, και προϊόντων και επομένως ανοίγουν θέσεις για νέους παρόχους, με αλλαγμένη ή τελείως νέα μορφή ενέργειας σε σύγκριση με αυτή που έχουν στο σημερινό ηλεκτρικό δίκτυο. Κάποιοι πάροχοι υπηρεσιών που μπορεί να δημιουργηθούν περιλαμβάνουν εταιρείες διαχείρισης μετρητικών δεδομένων, φορείς συγκέντρωσης κατανεμημένων πηγών και εταιρείες διαχείρισης ενέργειας κτιρίων. (Παντισκα Λεονάρδος,2016)

2 IoT Threats

Ο κύριος στόχος αυτού του κεφαλαίου είναι να προσδιορίσει και να απαριθμήσει τις κύριες απειλές για την ασφάλεια, τις αδυναμίες, τους παράγοντες κινδύνου και τα σενάρια επίθεσης που επηρεάζουν τις συσκευές και τα δίκτυα IoT, λαμβάνοντας τα διαφορετικά επίπεδα σπουδαιότητας και κρισιμότητας που έδωσαν διάφοροι εμπειρογνώμονες σε κάθε σενάριο απειλής και κινδύνου. Επιπλέον, αναπτύσσονται λεπτομερώς τα τρία πιο κρίσιμα σενάρια επίθεσης, προκειμένου να υπογραμμιστούν οι πολυπλοκότητες τους και να προταθούν συγκεκριμένα μέτρα ασφαλείας για την αντιμετώπιση των αρνητικών αποτελεσμάτων τους και των δυσμενών επιπτώσεών τους.

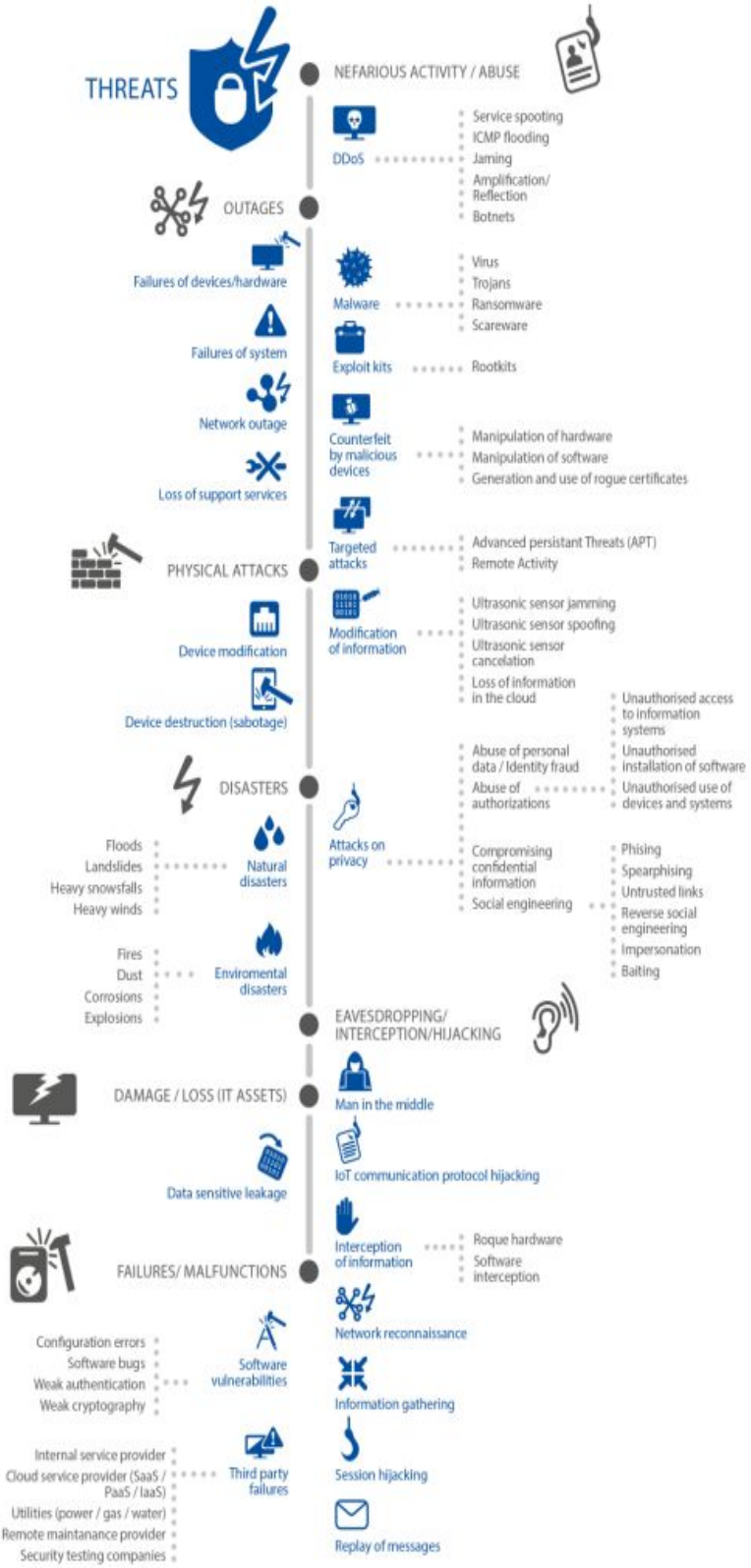
2.1 Συμβάντα ασφαλείας

Ο αριθμός των απειλών κατά της ασφάλειας που αφορούν συσκευές IoT έχει αυξηθεί τα τελευταία χρόνια. Το παρακάτω σχήμα απεικονίζει μερικά από τα βασικά περιστατικά ασφάλειας του Διαδικτύου που έχουν ανακαλυφθεί ή / και έχουν πραγματοποιηθεί από το 2009, συνεπώς ώστε να επισημανθεί ο τρόπος με τον οποίο αυξήθηκαν σημαντικά οι επιθέσεις. Πρέπει να σημειωθεί ότι αυτός ο κατάλογος δεν είναι εξαντλητικός και περιλαμβάνει μόνο τα κύρια παραδείγματα. Δεδομένου του ότι ολοένα και αυξάνεται το φάσμα των καθημερινών δραστηριοτήτων στο χώρο του IoT, είναι δεδομένη η αυξητική τάση που θα παρουσιάσει ο αριθμός των επιθέσεων αλλά και η γκάμα αυτων . Λεπτομερέστερη περιγραφή κάθε συμβάντος ασφαλείας βρίσκεται στο παρακάτω σχήμα.

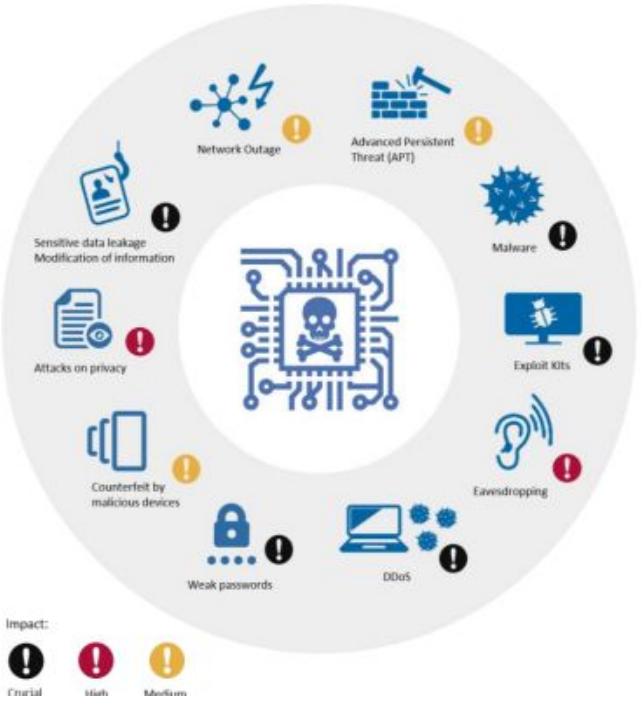


2.2 Ταξινόμηση των κινδύνων

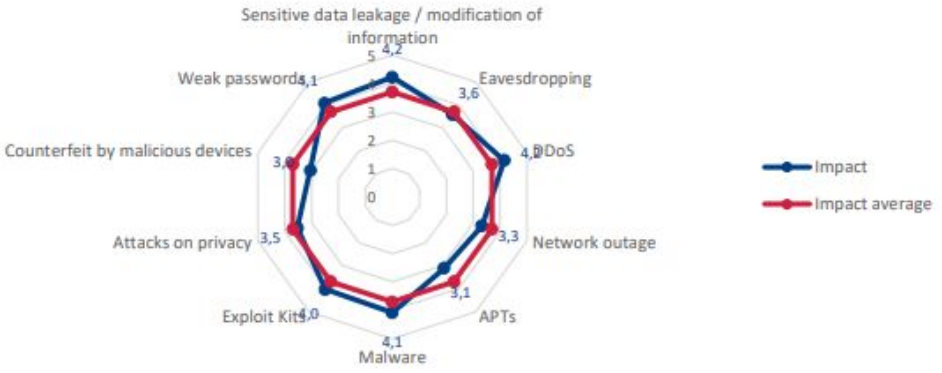
Όπως παρατηρήθηκε στην προηγούμενη ενότητα, ο αριθμός των επιθέσεων που σχετίζονται άμεσα με το διαδίκτυο των πραγμάτων έχει αυξηθεί κατά τα τελευταία χρόνια φτάνοντας στο σημείο όπου έγινε το κύριο άρθρο ειδήσεων το 2016 με τις Mirai botnet επιθέσεις. Αυτές οι επιθέσεις, στην πλειοψηφία τους σχετίζονται με συσκευές ή με συστήματα που έχουν παραβιαστεί αυξάνοντας ταυτόχρονα τον αριθμό των κινδύνων που αντιμετωπίζει το δίκτυο των πραγμάτων. Σύμφωνα με τη ταξινόμηση των απειλών για το IoT που εξέδωσε η ENISA διαμορφώνεται το παρακάτω διάγραμμα των κινδύνων μαζί με κάποια παραδείγματα.


THREATS
NEFARIOUS ACTIVITY / ABUSE
DDoS
Service spooting
ICMP flooding
Jaming
Amplification/ Reflection
Botnets
OUTAGES
Failures of devices/hardware
Failures of system
Network outage
Loss of support services
Malware
Virus
Trojans
Ransomware
Scareware
Exploit kits
Rootkits
Counterfeit by malicious devices
Manipulation of hardware
Manipulation of software
Generation and use of rogue certificates
Targeted attacks
Advanced persistant Threats (APT)
Remote Activity
PHYSICAL ATTACKS
Device modification
Device destruction (sabotage)
Modification of information
Ultrasonic sensor jamming
Ultrasonic sensor spoofing
Ultrasonic sensor cancelation
Loss of information in the cloud
Unauthorised access to information systems
Abuse of personal data / Identity fraud
Unauthorised installation of software
Abuse of authorizations
Unauthorised use of devices and systems
DISASTERS
Floods
Landslides
Heavy snowsfalls
Heavy winds
Natural disasters
Fires
Dust
Corrosions
Explosions
Enviromental disasters
Attacks on privacy
Compromising confidential information
Phising
Spearphising
Untrusted links
Social engineering
Reverse social engineering
Impersonation
Baiting
EAVESDROPPING/ INTERCEPTION/HIJACKING
DAMAGE / LOSS (IT ASSETS)
Man in the middle
Data sensitive leakage
IoT communication protocol hijacking
Interception of information
Roque hardware
Software interception
FAILURES/ MALFUNCTIONS
Network reconnaissance
Configuration errors
Software bugs
Weak authentication
Weak cryptography
Software vulnerabilities
Information gathering
Internal service provider
Cloud service provider (SaaS / PaaS / IaaS)
Utilities (power / gas / water)
Remote maintanance provider
Security testing companies
Third party failures
Session hijacking
Replay of messages

Παρόλα αυτά, διαφορετικοί κίνδυνοι έχουν διαφορετικά πιθανά αποτελέσματα, καθώς ποικίλουν ανάλογα με το use case scenario. Οι ειδικοί του IoT δίνουν μία σαφέστερη εικόνα για τις επιπτώσεις των κινδύνων αυτών. Οι πιό σχετικοί παρουσιάζονται στο παρακάτω σχήμα.



Οι επιπτώσεις κάθε κινδύνου προσδιορίστηκαν με τον υπολογισμό ενός σταθμικού μέσου από τις απαντήσεις των ειδικών, οι οποίες βασίζεται σε ένα σύστημα με μέγιστη βαθμολογία το 5 και εκτείνεται από το καθόλου σημαντικός έως το μεγάλης κρισιμότητας. Καθώς το παραπάνω σχήμα παρουσιάζει το πραγματικό αποτέλεσμα κάθε κινδύνου, το επόμενο σχήμα χρησιμοποιεί το ακριβές αποτέλεσμα του υπολογισμού, όπου τιμές μεταξύ το 3 και το 3.5 στα 5 αντιστοιχούν σε μέτριας σημασίας κινδύνους, τιμές μεταξύ 3.5 και 4 στα 5 αντιστοιχούν σε μεγάλης σημασίας κινδύνους ενώ τιμές μεγαλύτερες του 4 αντιστοιχούν σε κινδύνους τεράστιας κρισιμότητας. Τιμές κάτω από 3 αντιστοιχούν σε κινδύνους χαμηλής σημασίας εώς καθόλου σημασίας αλλά θα πρέπει να σημειωθεί ότι δεν υπάρχει κανένας κίνδυνος που συγκέντρωσε βαθμολογία μικρότερη του 3. Επιπλέον μπορεί να σημειωθεί ότι κατά κύριο λόγο, οι περισσότεροι κίνδυνοι αξιολογήθηκαν ως μεγάλης σημασίας αφού ο μέσος όρος των αποτελεσμάτων βρίσκεται στο 3.7 στα 5.



2.2.1 Κυριότερες απειλές

Ο παρακάτω πίνακας δίνει μία καθαρή εικόνα καθώς περιγράφει και ταξινομεί όλα τα threats που είναι πιθανό να απασχολήσουν ένα δίκτυο IoT

Threat Category	**Threat**	**Description**	**Specific Threat/Attack (Examples)**
Nefarious activity / Abuse	Malware	Software programs designed to carry out unwanted and unauthorised actions on a system without the consent of the user, resulting in damage, corruption or information theft. Its impact can be high.	- Virus, - Trojans, - Ransomware, - Scareware
	Exploit Kits	Code designed to take advantage of vulnerability in order to gain access to a system. This threat is difficult to detect and in IoT environments its impact ranges from high to crucial, depending on the assets affected.	- Rootkits
	Targeted attacks	Attacks designed for a specific target, launched over a long period of time, and carried out in multiple stages. The main objective is to remain hidden and to obtain as much sensitive data/information or control as possible. While the impact of this threat is medium, detecting them is usually very difficult and takes a long time.	- Advanced Persistent Threats (APT)
	DDoS	Multiple systems attack a single target in order to saturate it and make it crash. This can be done by making many connections, flooding a	- Service spoofing, - ICMP flooding,

		communication channel or replaying the same communications over and over.	- Jamming, - Amplification/reflection, - Botnets
	Counterfeit by malicious devices	This threat is difficult to discover, since a counterfeit device cannot be easily distinguished from the original. These devices usually have backdoors and can be used to conduct attacks on other ICT systems in the environment.	- Manipulation of hardware/software, - Use of rogue certificates
	Privacy exposure	This threat affects both the privacy of the user and the exposure of network elements to unauthorised personnel.	- Abuse of personal data/identity fraud - Abuse of authorisations - Unauthorised access to information systems - Unauthorised installation of software - Unauthorised use of devices and systems - Compromising confidential information - Social engineering - Phishing - Untrusted links - Impersonation
	Modification of information	The objective is to manipulate the information in order to cause chaos, or acquire monetary gains (but not to damage the devices).	- Ultrasonic sensor jamming - Ultrasonic sensor spoofing - Ultrasonic sensor cancelation - Loss of information

Eavesdropping / Interception / Hijacking	Man in the middle	Active eavesdropping attack, in which the attacker relays messages from one victim to another, in order to make them believe that they are talking directly to each other	- Man-in-the-middle (MITM) - Active eavesdropping
	IoT communication protocol hijacking	Taking control of an existing communication session between two elements of the network. The intruder is able to sniff sensible information, including passwords. The hijacking can use aggressive techniques like forcing disconnection or denial of service.	- Protocol hijacking
	Interception of information	Unauthorised interception (and sometimes modification) of a private communication, such as phone calls, instant messages, e-mail communications	- Roque hardware - Software interception
	Network reconnaissance	Passively obtain internal information about the network: devices connected, protocol used, open ports, services in use, etc.	- Passive reconnaissance
	Session hijacking	Stealing the data connection by acting as a legitimate host in order to steal, modify or delete transmitted data.	- Session hijacking - Cookie hijacking
	Information gathering	Passively obtain internal information about the network: devices connected, protocols used, etc.	- Footprinting - Social engineering
	Replay of messages	This attack uses a valid data transmission maliciously by repeatedly sending it or delaying it, in order to manipulate or crash the targeted device.	- Replay / playback
Outages	Network Outage	Interruption or failure in the network supply, either intentional or accidental. Depending on the network segment affected, and on the time required to recover, the importance of this threat ranges from high to critical.	- DoS/DDoS on DNS infrastructure (DNS outage)
	Power Outage	Interruption or failure in the power supply, either intentional or accidental. May target power supply to any infrastructure component but with a particular focus on IoT devices and their internal components. The	- Denial-of-sleep

		power source can be external and wired or a battery integrated in the device itself. In case of battery, reduces sensor lifetime to minimum possible.	
	Failures of devices	Threat of failure or malfunction of hardware devices.	- Physical manipulation (see physical attacks below)
	Failure of system	Threat of failure of software services or applications.	- Software/application manipulation - See Malware threat and attacks - See Exploit kits threat and attacks
	Loss of support services	Unavailability of support services required for proper operation of the information system.	
Damage / Loss (IT Assets)	Data / Sensitive information leakage	Sensitive data is revealed, intentionally or not, to unauthorised parties. Application/service reveals sensitive data such as technical details of web/server application, environment, or user-specific data, and used by an attacker to exploit the target web application, its hosting network, or its users. The importance of this threat can vary greatly, depending on the kind of data leaked.	- See Network reconnaissance threat - See Information gathering threat
Failures / Malfunctions	Software vulnerabilities	The most common IoT devices are often vulnerable due to weak/default passwords, software bugs, and configuration errors, posing a risk to the network. This threat is usually connected to others, like exploit kits, and it is considered crucial.	- See Exploit Kits threat
	Third parties failures	Errors on an active element of the network caused by the misconfiguration of another element that has direct relation with it. For example, failures in Internal service provider, Cloud service provider,	

		remote maintenance provider, security testing companies, etc.	
Disaster	Natural Disaster	Includes events such as, floods, heavy winds, heavy snows, landslides, among others natural disaster, which could physically damage the devices.	
	Environmental Disaster	Disasters in the deployment environments of IoT equipment and causing their inoperability.	
Physical attacks	Device modification	Tampering a device by for example taking advantage of bad configuration of ports, exploiting those left open, etc.	
	Device destruction (sabotage)	Incidents such devices theft, bomb attacks, vandalism or sabotage could damage devices.	

Table 1: Threats related to IoT ecosystems

2.2.2 Συσκευές που επηρεάζει κάθε απειλή

IoT Asset presents what IoT assets are affected by the threats presented earlier.

IoT Asset (affected by)	Threat	Threat Category
IoT Devices	- Malware - Exploit Kits - DDoS - Counterfeit by malicious devices - Privacy exposure - Modification of information	Nefarious activity / Abuse
	- Man in the middle - IoT communication protocol hijacking - Interception of information - Network reconnaissance - Session hijacking - Information gathering - Replay of messages	Eavesdropping / Interception / Hijacking
	- Power outage - Failures of devices - Failure of system	Outages

	- Loss of support services	
	- Data / Sensitive information leakage	Damage / Loss (IT Assets)
	- Software vulnerabilities - Third parties failures	Failures / Malfunctions
	- Natural Disaster	Disaster
	- Device modification - Device destruction (sabotage)	Physical attacks
Other IoT Ecosystem (Interact/ Manage) Devices	- Malware - Exploit Kits - DDoS - Counterfeit by malicious devices - Privacy exposure - Modification of information	Nefarious activity / Abuse
	- Failure of system - Loss of support services	Outages
	- Data / Sensitive information leakage	Damage / Loss (IT Assets)
	- Software vulnerabilities - Third parties failures	Failures / Malfunctions
	- Natural Disaster - Environmental Disaster	Disaster
	- Device destruction (sabotage)	Physical attacks
Communications	- Man in the middle - IoT communication protocol hijacking - Interception of information - Network reconnaissance - Session hijacking - Information gathering	Eavesdropping / Interception / Hijacking
	- Network Outage - Loss of support services	Outage
	- Device modification	Physical attacks
Infrastructure	- Exploit Kits - Targeted attacks - DDoS - Counterfeit by malicious devices	Nefarious activity / Abuse

	- Network reconnaissance	Eavesdropping / Interception / Hijacking
	- Network Outage - Loss of support services	Outage
	- Software vulnerabilities - Third parties failures	Failures / Malfunctions
	- Natural Disaster - Environmental Disaster	Disaster
	- Device destruction (sabotage)	Physical attacks
Platform and Backend	- Malware - Targeted attacks - DDoS - Privacy exposure - Modification of information	Nefarious activity / Abuse
	- Failure of system - Loss of support services	Outages
	- Data / Sensitive information leakage	Damage / Loss (IT Assets)
	- Software vulnerabilities - Third parties failures	Failures / Malfunctions
	- Natural Disaster - Environmental Disaster	Disaster
	- Device destruction (sabotage)	Physical attacks
Decision making	- IoT communication protocol hijacking - Replay of messages	Eavesdropping / Interception / Hijacking
	- Loss of support services	Outages
Management Applications & Services	- Software vulnerabilities - Third parties failures	Failures / Malfunctions
	- Loss of support services	Outages
Information (use/transit/rest)	- Targeted attacks - Privacy exposure - Modification of information	Nefarious activity / Abuse
	- Man in the middle - IoT communication protocol hijacking - Interception of information - Network reconnaissance - Session hijacking - Information gathering	Eavesdropping / Interception / Hijacking

	- Replay of messages	
	- Loss of support services	Outages
	- Data / Sensitive information leakage	Damage / Loss (IT Assets)

Table 2: Fields affected the most by threats

2.3 Ανάλυση βασικών σεναρίων επίθεσης

Οι κίνδυνοι που καταγράφηκαν παραπάνω μπορούν να χρησιμοποιηθούν από τους επιτιθέμενους με στόχο να προκαλέσουν μια αλληλουχία από καταστροφές σε διαφορετικά επίπεδα στις υποδομές. Τα διαφορετικά σενάρια επίθεσης καθώς και η βαρύτητα κάθε επίθεσης έχουν οργανωθεί με τη βοήθεια που προσέφεραν οι ειδικοί του κλάδου.

Είναι σημαντικό να αναφερθεί ότι επιθέσεις μπορούν να προκύψουν κατά τη διάρκεια όλης της διαδικασίας και ο αντίκτυπος που μπορεί να έχει κάθε επίθεση σε κάθε κομμάτι της διαδικασίας έχει επίσης αναλυθεί. Το πόσο σημαντικό είναι κάθε σενάριο επίθεσης κυμαίνεται από το λίγο σημαντικό έως το εξαιρετικά σημαντικό. Στο παρακάτω σχήμα παρουσιάζονται ορισμένα σενάρια επίθεσης μαζί με το βαθμό σημαντικότητας της κάθε επίθεσης.

ATTACK SCENARIOS	IMPORTANCE LEVEL
1. Against the network link between controller(s) and actuators	High – Crucial
2. Against sensors, modifying the values read by them or their threshold values and settings	High – Crucial
3. Against actuators, modifying or sabotaging their normal settings	High – Crucial
4. Against the administration systems of IoT	High – Crucial
5. Exploiting protocol vulnerabilities	High
6. Against devices, injecting commands into the system console	High – Crucial
7. Stepping stones attacks	Medium – High
8. DDoS using an IoT botnet	Crucial
9. Power source manipulation and exploitation of vulnerabilities in data readings	Medium – High
10. Ransomware	Medium – Crucial[70]

Πιο αναλυτικά για την κάθε περίπτωση:

1. Against the network link between controller(s) and actuators

Η υποκλοπή είναι μία απειλή η οποία επιτρέπει στον επιτιθέμενο να υποκλέψει ευαίσθητες αλλά και λειτουργικές πληροφορίες που μπορούν να χρησιμοποιηθούν σε πολλές κακόβουλες ενέργειες, συμπεριλαμβανομένου και μεταγενέστερες επιθέσεις στα συστήματα IoT. Σε επιθέσεις τύπου Advanced Persistent Threat (APT), η υποκλοπή και η συγκέντρωση πληροφοριών αποτελεί το πρώτο στάδιο της επίθεσης καθώς με αυτό τον τρόπο αναγνωρίζει αδυναμίες του συστήματος και έτσι εντοπίζει πιθανά σημεία στα οποία θα επιτεθεί και να μπει στο σύστημα.

- Αποτέλεσμα: Το μεγαλύτερο αποτέλεσμα είναι η διαρροή δεδομένων. Ανάλογα με το σύστημα, η επικινδυνότητα της επίθεσης μπορεί να κυμαίνεται από χαμηλή έως υψηλή αλλά μπορεί επίσης να σηματοδοτεί την έναρξη μίας μεγαλύτερης επίθεσης στο σύστημα.
- Σχετικοί κίνδυνοι: Υποκλοπή και διαρροή ευαίσθητων δεδομένων.

2. Against sensors, modifying the values read by them or their threshold values and settings

Ο επιτιθέμενος επεξεργάζεται τις ρυθμίσεις των αισθητήρων, αλλάζοντας τις τιμές κατωφλίου που τους έχουν οριστεί, με αποτέλεσμα να επιτρέπονται τιμές εκτός εμβέλειας που κανονικά θα απαγορεύονταν προκαλώντας έτσι μεγάλο πρόβλημα στα συστήματα και εγκαταστάσεις. Καθώς μεγάλες εγκαταστάσεις συνήθως έχουν πολλούς ανεξάρτητους αισθητήρες, ο επιτιθέμενος θα πρέπει να πειράξει πολλούς αισθητήρες για να πετύχει το στόχο του καθώς αν δεν το κάνει τότε λόγω των δεδομένων από τους υπόλοιπους αισθητήρες που είναι εύκολο να αναγνωριστεί ο πειραγμένος αισθητήρας.

- Αποτέλεσμα: Επιτρέποντας σε αισθητήρες να δέχονται και να στέλνουν λανθασμένες τιμές, βάζει το δίκτυο IoT σε κίνδυνο. Ένας αισθητήρας που δυσλειτουργεί μπορεί να επιτρέψει μία απότομη αύξηση στο πλάτος ενός σήματος να περάσει καταστρέφοντας έτσι μέρος του συστήματος.
- Σχετικοί κίνδυνοι: Επιθέσεις κατά της ιδιοτικότητας καθώς και διαρροής ευαίσθητων δεδομένων ή ακόμα και αλλαγή των πληροφοριών.

3. Against actuators,modifying or sabotaging their normal settings

Μεταχείριση των ρυθμίσεων και των παραμέτρων των ενεργοποιητών κάνοντάς τους να χρησιμοποιούν λανθασμένες ρυθμίσεις, κατώφλια ή δεδομένα και έτσι επηρεάζοντας την φυσιολογική τους λειτουργία παρεμβαίνοντας στις φυσιολογικές ρυθμίσεις λειτουργίας τους.

- Αποτέλεσμα: Εξαρτάται από τους ενεργοποιητές που έχουν επηρεαστεί. Μπορεί να επηρεάσει παραγωγικές διαδικασίες.
- Σχετικοί κίνδυνοι: Διακοπή λειτουργίας του δικτύου και παραπλάνηση από κακόβουλες συσκευές

4. Against the administration systems of IoT

Ένας επιτιθέμενος προσπαθεί να πάρει τον πλήρη έλεγχο του διαχειριστικού συστήματος ενός συστήματος IoT ή μίας συσκευής, με πιθανό αποτέλεσμα να επηρεάζει όλο το σύστημα. Μία τέτοια επίθεση μπορεί να είναι αποτελεσματική κυρίως όταν χρησιμοποιούνται αδύναμοι ή συνηθισμένοι κωδικοί. Αυτού του είδους

η επίθεση περιλαμβάνει διαφορετικά στάδια/φάσεις και συνήθως πραγματοποιείται με κρυφό τρόπο. Πρέπει να σημειωθεί ότι αυτού του είδους η επίθεση πρέπει να λαμβάνεται υπόψιν για ολόκληρο τον κύκλο ζωής μίας συσκευής.

- Αποτέλεσμα: Ο κακόβουλος χειρισμός ή η διακοπή ενός συγκεκριμένου συστήματος IoT μπορεί να επηρεάσει πολλούς ανθρώπους, να προκαλέσει περιβαλλοντικά ζητήματα και ακόμα να επηρεάσει και άλλα συστήματα παρεμβάλλοντας στο σύστημα επικοινωνίας τους.
- Σχετικοί κίνδυνοι: αδύναμοι κωδικοί, επίθεση στα τρωτά σημεία του συστήματος (exploit kit), επίθεση κατά της ιδιοτικότητας, κακόβουλο λογισμικό και επιθέσεις τύπου DDoS (Distributed Denial of Service).

5. Exploit Protocol vulnerabilities

Αυτού του είδους η εκμετάλλευση χρησιμοποιείται συνήθως ως προθάλαμος για να ξεκινήσουν άλλου είδους επιθέσεις. Με αυτό τον τρόπο ο επιτιθέμενος παίρνει προνομιούχα πρόσβαση στο σύστημα χωρίς να τον έχει εξουσιοδοτήσει κανείς. Το γεγονός αυτό μπορεί να οδηγήσει στην εγκατάσταση καινούριου κακόβουλου υλικού ή επιθέσεις από την πίσω πόρτα. Χρησιμοποιείται ως μέρος μίας επίθεσης ανεξάρτητα αν η επίθεση αφορά ένα σύστημα, μία συσκευή ή ολόκληρο το δίκτυο. Είναι δύσκολο να εντοπιστούν τέτοιες επιθέσεις και είναι πολύ πιο εύκολο να εντοπίσεις ενέργειες που έχουν γίνει μετά το τέλος της επίθεσης.

- Αποτέλεσμα: Αν η επίθεση είναι πετυχημένη, δημιουργεί ένα τρωτό σημείο στο σύστημα και σε μερικές περιπτώσεις με πολλά δικαιώματα, αλλιώς το σύστημα είναι πιθανό να πάθει ζημιά ή να γίνει ασταθές. Τέτοιου είδους επιθέσεις συνήθως αποτελούν μέρος μίας μεγαλύτερης επίθεσης η οποία μπορεί να είναι από μία απλή απόπειρα κλοπής δεδομένων μέχρι μία πολυσύνθετη προηγμένη επίθεση διαρκείας (Advanced Persistent Threat).
- Σχετικοί κίνδυνοι: επιθέσεις τύπου exploit kits, κακόβουλο λογισμικό, Advanced Persistent Threats)

6. Against devices by injecting commands into the system console

Μία τέτοια επίθεση λαμβάνει χώρα όταν ο επιτιθέμενος εισάγει και εκτελεί εντολές έχοντας δικαιώματα σε ένα πειραγμένο σύστημα διαμέσου της κονσόλας του.

- Αποτέλεσμα: Αν ο επιτιθέμενος έχει τη δυνατότητα να εισαγάγει δικές του εντολές σε μία συσκευή, μπορεί εν δυνάμη να επηρεάσει και άλλες μηχανές μέσα στο σύστημα. Αυτό θα μπορούσε να προκαλέσει μία αλληλουχία από επιπτώσεις στο σύστημα, ενώ ο επιτιθέμενος θα είναι σε θέση να χρησιμοποιήσει όλες τις συσκευές για κακόβουλους σκοπούς.
- Σχετικοί κίνδυνοι: επιθέσεις expoit kits, DDoS (Distributed Denial of Service), και διακοπή λειτουργίας του δικτύου (network outage)

7. Stepping stone attacks

Αυτού του τύπου επιθέσεις χρησιμοποιούνται ευρέως γιά την έναρξη ανώνυμων επιθέσεων. Χρησιμοποιούνται συχνά από εισβολείς σε ένα δίκτυο ώστε να κρατήσουν κρυφή την ταυτότητά τους, αφού ξεκινούν τις επιθέσεις όχι από τον δικό τους υπολογιστή αλλά διαμέσου άλλων τους οποίους έχουν προηγουμένως παραβιάσει.

- Αποτέλεσμα: Ξεκινώντας μία τέτοια επίθεση, ο επιτιθέμενος παραβιάζει μία σειρά από hosts, χρησιμοποιώντας τους τον έναν μετά τον άλλον για να μεταδώσουν εντολές επίθεσης.
- Σχετικοί κίνδυνοι: Advanced Persistent Threats (APTs), Distributed Denial of Service (DDoS), παραπλάνηση από κακόβουλες συσκευές.

8. DDoS using an IoT botnet

Τέτοιες επιθέσεις δεν στοχεύουν αποκλειστικά σε συσκευές IoT αλλά τις χρησιμοποιούν για να επιτεθούν σε άλλες, όχι απαραίτητα IoT συσκευές. Αρχικά, ένα κακόβουλο λογισμικό αυτόματα εντοπίζει ευάλωτες IoT συσκευές, μολύνοντάς τες και εντάσσοντάς τες σε ένα δίκτυο τύπου botnet, το οποίο μπορεί στη συνέχεια να χρησιμοποιηθεί με στόχο την πραγματοποίηση DDoS επιθέσεων γεμίζοντας τους εξυπηρετητές του στόχου με κακόβουλη κίνηση.

- Αποτέλεσμα: Η συσκευή στόχος θα πλημμυριστεί από κακόβουλη κίνηση η οποία θα την καταστήσει ανενεργή.
- Σχετικοί κίνδυνοι: Επιθέσεις τύπου exploit kits, DDoS και παραπλάνηση από κακόβουλες συσκευές.

9. Power source manipulation and exploitation of vulnerabilities in data readings

Αυτές οι επιθέσεις επικεντρώνονται στον χειρισμό των πηγών ενέργειας και στην αξιοποίηση των τρωτών σημείων για την τροποποίηση του πως διαβάζονται τα δεδομένα που στέλνει η μπαταρία μιας συσκευής. Ένας επιτιθέμενος μπορεί να παραβιάσει τη μπαταρία της συσκευής ή την τροφοδοσία με καλώδιο είτε με το χέρι, είτε χειρίζοντας την ίδια την πηγή τροφοδοσίας με κακόβουλο λογισμικό, χειριζόμενος τον τρόπο με τον οποίο μια συσκευή διαβάζει τις πληροφορίες που προέρχονται από την πηγή ενέργειας, για παράδειγμα, η στάθμη μπαταρίας είναι υψηλότερη ή χαμηλότερη από το πραγματικό επίπεδο. Ορισμένοι τύποι έξυπνων συσκευών ενδέχεται να εξαρτώνται από τις μπαταρίες για την κανονική τους λειτουργία. Αυτό το χαρακτηριστικό μπορεί να φανεί σαν ένα πλεονέκτημα έναντι των λιγότερο συνηθισμένων καλωδίων, αλλά, μακράν αυτού, απαιτεί να ληφθούν υπόψη ορισμένες πτυχές της ασφάλειας.

- Αποτέλεσμα: Η φυσική παραβίαση μιας μπαταρίας μπορεί να προκαλέσει βλάβη, ενδεχομένως να μην μπορεί να λειτουργήσει η συσκευή καθόλου. Ο χειρισμός του τρόπου με τον οποίο μια συσκευή διαβάζει το επίπεδο φόρτισης που προέρχεται από την μπαταρία μπορεί να οδηγήσει τη συσκευή να πιστεύει ότι η στάθμη της μπαταρίας είναι υψηλότερη από την πραγματική, προκαλώντας τη εξάντληση της μπαταρίας και την απενεργοποίηση της ή χαμηλότερη από την πραγματική όπου τότε μπαίνει σε λειτουργία εξοικονόμησης ενέργειας επηρεάζοντας έτσι την απόδοση της συσκευής.
- Σχετικοί κίνδυνοι: κακόβουλο λογισμικό, φυσικές επιθέσεις.

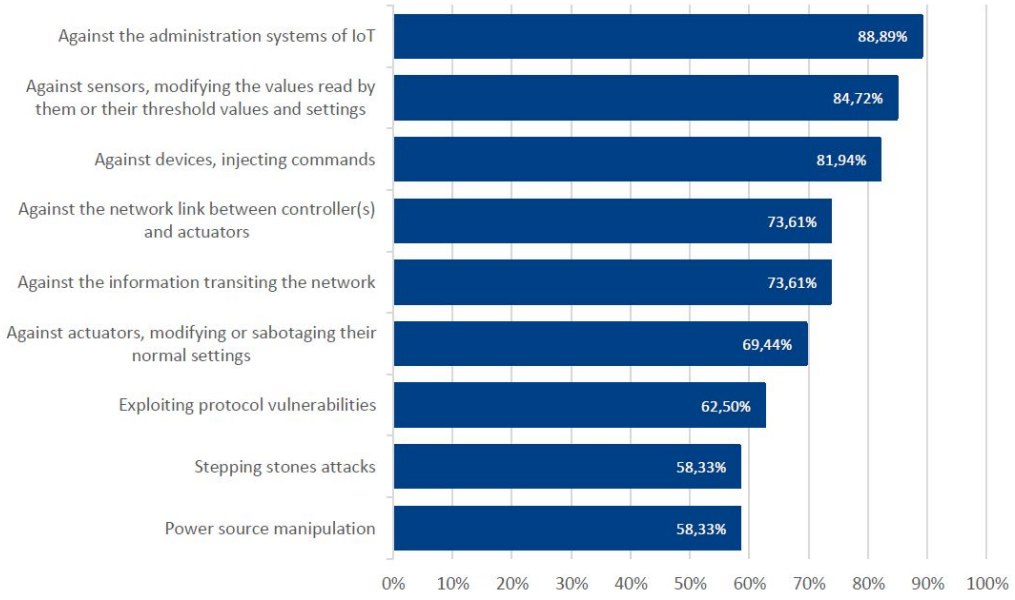
10. Ransomware

Αυτές οι επιθέσεις επιτελούνται από ένα κακόβουλο λογισμικό που παρακωλύει συνεχώς την πρόσβαση στα δεδομένα του θύματος εκτός και αν πληρώνεται η αμοιβή. Δεδομένου ότι οι επιθέσεις αυτές βασίζονται σε κακόβουλο λογισμικό, μπορούν να αποφευχθούν με την ενημέρωση / επιδιόρθωση ευάλωτων συσκευών. Αυτό μπορεί να γίνει και εκτός του οικοσυστήματος του IoT, όπως με την επίθεση WannaCry που έλαβε χώρα τον Μάιο του 2017, όπου το patch για την ευπάθεια που εκμεταλλεύτηκε η WannaCry απελευθερώθηκε μήνες πριν από την επίθεση. Το πρόβλημα σχετικά με το IoT είναι η δυσκολία ενημέρωσης / επιδιόρθωσης των διαφορετικών συσκευών - μερικές από αυτές δεν έχουν καν την δυνατότητα ενημέρωσης ή patch.

- Αποτέλεσμα: Υπάρχουν πολλοί πιθανοί στόχοι για επίθεση ransomware μέσα σε IoT - ένας εισβολέας θα μπορούσε να πάρει τον έλεγχο ενός έξυπνου θερμοστάτη στη μέση του χειμώνα και να ζητήσει χρήματα προτού επιτρέψει τη σωστή λειτουργία του,επίσης θα μπορούσε να ελέγξει ηλεκτρικά το σύστημα ηλεκτρικής ενέργειας ενός νοσοκομείου για λύτρα βάζοντας τους ασθενείς σε κίνδυνο.
- Σχετικοί κίνδυνοι: exploit kits, DDoS, malware, weak passwords

2.4 Κρίσιμα σενάρια επίθεσης

Κατά τη διάρκεια των συνεντεύξεων με εμπειρογνώμονες και σχετικούς ενδιαφερόμενους φορείς, τα παραπάνω σενάρια επίθεσης σχετικά με τα περιβάλλοντα του IoT περιγράφηκαν και αναλύθηκαν λεπτομερώς. Οι εμπειρογνώμονες κλήθηκαν να κατατάξουν τα 10 παραδείγματα σεναρίων επίθεσης όσον αφορά την κρισιμότητα και τα ακόλουθα τρία ήταν τα πιο ανησυχητικά για τους συνεντευξιαζόμενους. Το παρακάτω σχήμα απεικονίζει τη μέση κρισιμότητα ενός δεδομένου σεναρίου επίθεσης με βάση τις πληροφορίες που συγκεντρώθηκαν από τις συνεντεύξεις των εμπειρογνωμόνων. Και πάλι, η πρόκληση έγκειται στο να καθορίσουμε το επίπεδο κρισιμότητας μιας επίθεσης σε περιβάλλον IoT όταν το κάνουμε αυτό με οριζόντιο τρόπο.



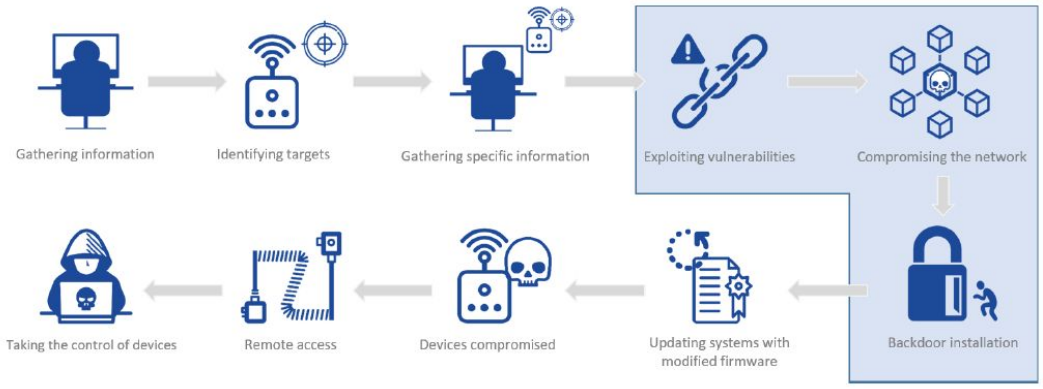
Τα 3 σενάρια που ξεχωρίζουν είναι τα εξής:

1. Attack Scenario 1: IoT administration system compromise
2. Attack Scenario 2: Value manipulation in IoT devices
3. Attack Scenario 3: Botnet / Commands Injection

Attack scenario 1: IoT administration system compromise

Αυτή η επίθεση καλύπτει μια μόλυνση που έχει σχεδιαστεί για να αναλάβει τον έλεγχο μιας ή πολλαπλών συσκευών IoT σε περιβάλλον IoT, προκειμένου να τις χειραγωγήσει ή να τις καταρρεύσει και να μπορέσει να τροποποιήσει τις τιμές, να αλλάξει τη λειτουργία / συμπεριφορά τους ή να αρνηθεί την πρόσβαση σε αυτές. Αυτό το σενάριο επίθεσης βασίζεται σε μια επίθεση Enterprise Gateway.(Armerding, 2018)(Jacoby, 2018)

Όπως απεικονίζεται στο σχήμα 12, το πρώτο βήμα είναι η συγκέντρωση πληροφοριών στο δίκτυο σχετικά με τις διάφορες συσκευές IoT που χρησιμοποιούνται στην επιχείρηση. Όταν εντοπιστεί και επιλεγεί μια συσκευή IoT, ο επιτιθέμενος συγκεντρώνει συγκεκριμένες πληροφορίες σχετικά με τις ευπάθειες της. Το επόμενο βήμα είναι να αξιοποιήσει τις διάφορες ευπάθειες που εντοπίστηκαν σε αυτήν τη συσκευή και να θέσει σε κίνδυνο το δίκτυο. Μετά από αυτό, ο επιτιθέμενος εξασφαλίζει την άμεση πρόσβαση στο σύστημα, ρυθμίζοντας ένα backdoor. Σε αυτό το σημείο, ο επιτιθέμενος χρειάζεται μόνο να ενημερώσει το σύστημα (π.χ. με ένα τροποποιημένο λογισμικό) για να παραβιάζεται συνεχώς η συσκευή. Με αυτόν τον τρόπο, ο επιτιθέμενος αποκτά τον πλήρη έλεγχο της συσκευής - κερδίζει τη δυνατότητα να βλέπει όλα τα δεδομένα και τις πληροφορίες που έχει συλλέξει η συσκευή και έχει απομακρυσμένη πρόσβαση για χρήση όποτε το θέλει.



RECOVERY TIME / EFFORT	GAPS AND CHALLENGES
Medium: it depends on the perimeter of the assets compromised and on the number of assets infected. It ranges from a few hours to up to several days if critical systems are compromised.	Insecure design or development Lack of proper product lifecycle management

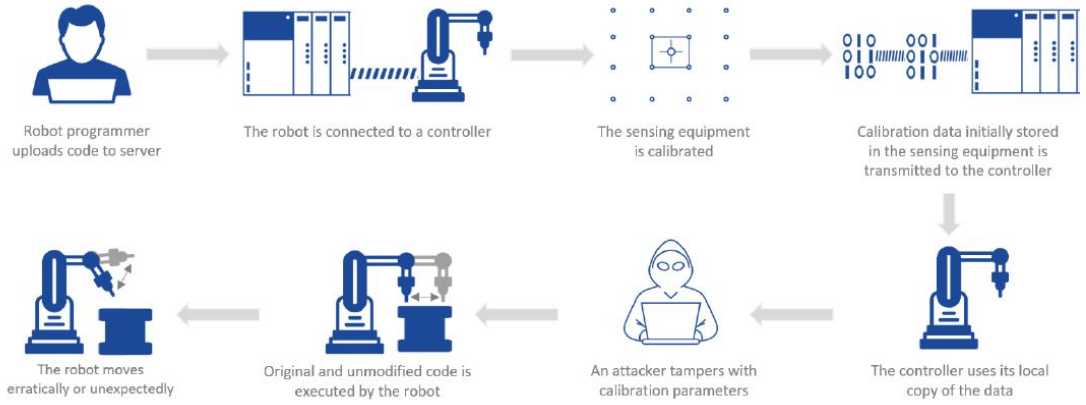
COUNTERMEASURES

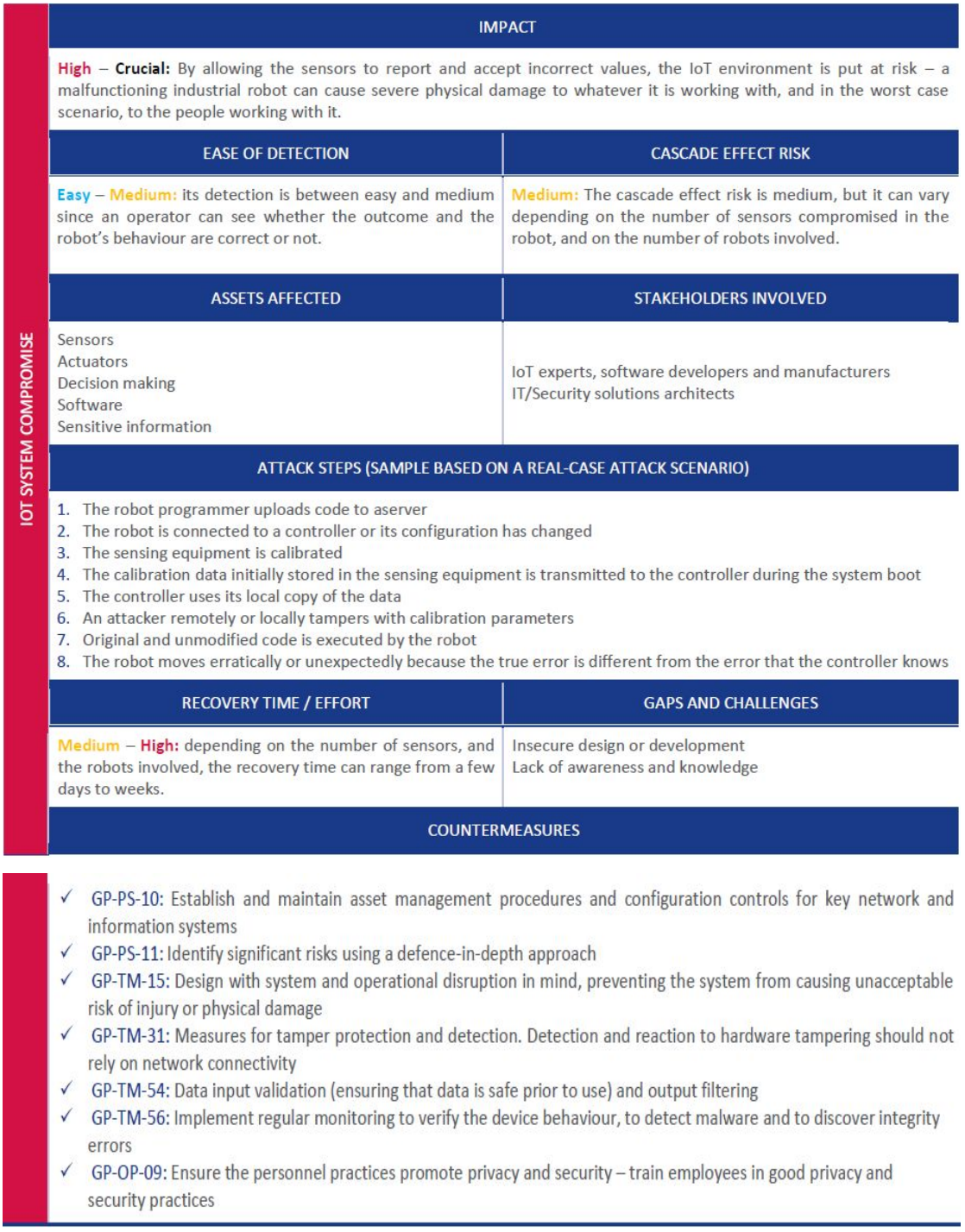
- ✓ GP-TM-04: Sign code cryptographically to ensure it has not been tampered after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded
- ✓ GP-TM-05: Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it
- ✓ GP-TM-06: Enable a system to return to a state that is known to be secure, after a security breach occurs or if an upgrade is not successful
- ✓ Hardening assets:
  - ✓ GP-PS-11: Identify significant risks using a defence-in-depth approach
  - ✓ GP-TM-22: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed
  - ✓ GP-TM-27: Limit the permissions of actions allowed for a given system by Implementing fine-grained authorisation mechanisms and using the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible
  - ✓ GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates
  - ✓ GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud
  - ✓ GP-TM-55: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system
  - ✓ GP-TM-56: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors

Attack scenario 2: Value manipulation in IoT devices

Ο χειρισμός των παραμέτρων βαθμονόμησης που έχουν καθοριστεί για τους αισθητήρες επιτρέπει την αποδοχή ανεπιθύμητων τιμών όταν δεν πρέπει, πράγμα που αποτελεί σοβαρή απειλή για τα κρίσιμα συστήματα. Αυτή η επίθεση στοχεύει τα επίπεδα επεξεργασίας αισθητήρων και μοντέλων γνώσης του συστήματος ελέγχου ενός βιομηχανικού ρομπότ σε ένα περιβάλλον Industry 4.0.(Federico Maggi)

Το σχήμα 13 περιγράφει αυτήν την επίθεση, η οποία αρχίζει με τη βαθμονόμηση ενός ρομποτικού εξοπλισμού από μια αλλαγή στις ρυθμίσεις ή όταν συνδέεται σε ένα ελεγκτή. Τα δεδομένα βαθμονόμησης που αποθηκεύονται αρχικά στον εξοπλισμό ανίχνευσης μεταδίδονται στον ελεγκτή κατά τη διάρκεια της εκκίνησης του συστήματος. Δεδομένου ότι το ρομπότ χρησιμοποιεί το τοπικό αντίγραφό του, ο επιτιθέμενος μπορεί να χειριστεί τις παραμέτρους βαθμονόμησης, προκαλώντας το ρομπότ να κινείται απροσδόκητα (κατά τη λήψη αποφάσεων, λανθασμένες τιμές εισόδου οδηγούν σε λανθασμένες αποφάσεις).



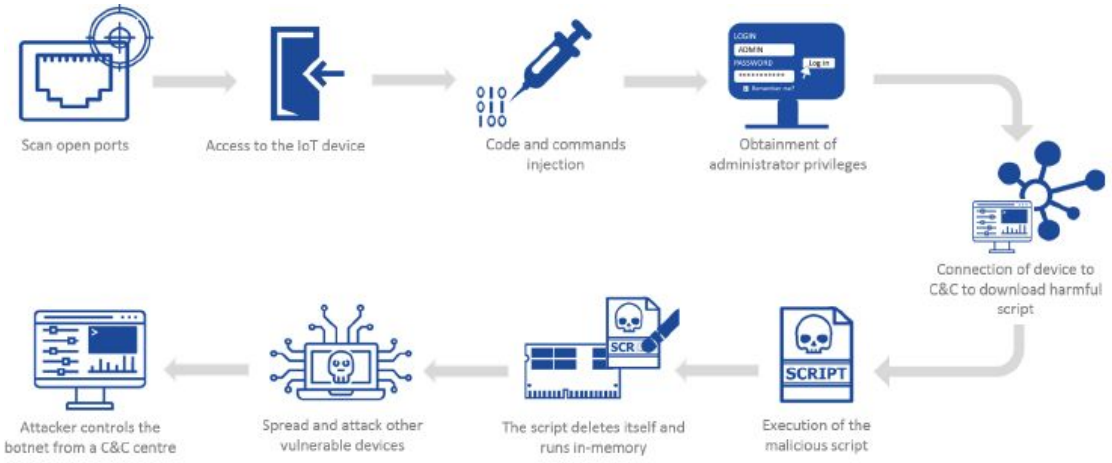


Attack scenario 3: Botnet / Commands injection

Αυτή η επίθεση συνεπάγεται την εκμετάλλευση κάποιου τρωτού σημείου μέσα σε μια συσκευή για την έγχυση εντολών και τη λήψη προνομίων διαχειριστή, με σκοπό τη δημιουργία ενός botnet που αποτελείται από αυτές τις ευάλωτες συσκευές IoT. Ένα botnet είναι ένα δίκτυο αυτόματων συσκευών που αλληλεπιδρούν για να ολοκληρώσουν κάποια κατανεμημένη εργασία. Λόγω της χαρακτηριστικής διασύνδεσης των συσκευών IoT και της κακής διαμόρφωσής τους, η πραγματοποίηση μιας τέτοιας επίθεσης είναι απλή. Αυτό το σενάριο επίθεσης βασίζεται στο

botnet(Enisa.europa.eu, 2018) της Mirai, το οποίο έχει πραγματοποιήσει αρκετές από τις ισχυρότερες επιθέσεις DDoS στην πρόσφατη ιστορία και έχει αποδειχθεί ικανό να επιτεθεί σε ποικίλα είδη στόχων, από την ιστοσελίδα του KrebsOnSecurity έως την τηλεπικοινωνιακή υποδομή ολόκληρης χώρας.(Energycollection.us, 2018). Ως εκ τούτου, με πιθανούς στόχους, όπως μια επικίνδυνη ενεργειακή υποδομή, ο αντίκτυπος της επίθεσης του Mirai μπορεί να φτάσει σε εξαιρετικά κρίσιμα επίπεδα.

Τα βήματα που πρέπει να ακολουθήσετε για να εκτελέσετε αυτό το είδος επίθεσης φαίνονται στο παρακάτω σχήμα. Το πρώτο είναι η σάρωση ανοιχτών θυρών σε συσκευές IoT που είναι προσβάσιμες μέσω του Διαδικτύου, οι οποίες συνήθως είναι κακώς προστατευμένες από προεπιλεγμένα ονόματα χρήστη και κωδικούς πρόσβασης που οι χρήστες ποτέ δεν αλλάζουν. Μόλις ο επιτιθέμενος αποκτήσει πρόσβαση στη συσκευή, αυτός ή αυτή θα εισάγει εντολές στην κονσόλα της συσκευής για να αποκτήσει δικαιώματα διαχειριστή. Εάν ο επιτιθέμενος επιτύχει να αποκτήσει αυτά τα δικαιώματα, αυτός ή αυτή θα κάνει τη συσκευή να συνδεθεί σε ένα Command and Control (C & C) υπό τον έλεγχό του, για να κατεβάσει και να εκτελέσει κακόβουλο script. Στη συνέχεια, θα εκτελεστεί το script, το οποίο θα διαγραφεί και θα τρέχει στη μνήμη. Στη συνέχεια, θα αρχίσει να εξαπλώνεται, κάνοντας επίθεση με τον ίδιο τρόπο και σε άλλες ευάλωτες συσκευές, προκειμένου να συγκεντρώσει έναν στρατό εξοπλισμού IoT, τοποθετώντας τα σε ένα botnet, το οποίο ο επιτιθέμενος θα είναι σε θέση να ελέγχει από ένα κέντρο C & C, διεξάγοντας επιθέσεις με χρήση του botnet.



IOT SYSTEM COMPROMISE

IMPACT

High – **Crucial:** The impact of the attacks carried out by a botnet ranges from high to critical, depending on the volume of the distributed attack, which is directly related to the number of compromised assets that are part of the botnet, and the criticality of the target.

EASE OF DETECTION	CASCADE EFFECT RISK
Hard: due to the ignorance about the characteristics and configuration of these devices, these attacks tend to be hard to detect and identify the source, which allows them to pass undetected for long periods of time, and they are also complex to investigate and recover from.	**Critical:** this type of attack has a tremendous cascade effect. Once a device is infected, the goal is to identify other vulnerable devices to extend the network.

ASSETS AFFECTED	STAKEHOLDERS INVOLVED
Devices to interface with things Devices to manage things Device and network management Communications Software	IoT experts, software developers and manufacturers Information security experts IT/Security solutions architects Chief Information Security Officers (CISOs)

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)

1. The attacker scans open ports in devices belonging to an IoT network
2. If there are any open ports, the attacker tries to gain access to the device using weaknesses such as weak or default passwords, or through exploiting the test/debug modes
3. Once inside, the attacker injects commands in order to obtain administrator privileges
4. With these permissions, the attacker tries to connect the device to the Command and Control of the botnet
5. The attacker downloads and executes a malicious script
6. The script deletes itself and runs in-memory
7. Then, it will begin to spread, attacking other vulnerable devices in the same way, in order to gather an IoT device army, conscripting them into a botnet.
8. The attacker can now control the botnet from a Command and Control (C&C) centre, from where he or she will launch distributed attacks conducted by the botnet.

RECOVERY TIME / EFFORT	GAPS AND CHALLENGES
High: the main issue is the amount of time it takes to detect that the system that has been manipulated, which can take several days/weeks, or even months in extreme cases	Insecure design or development Lack of proper product lifecycle management

COUNTERMEASURES

- ✓ GP-TM-04: Sign code cryptographically to ensure it has not been tampered after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded
- ✓ GP-TM-05: Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it
- ✓ GP-TM-06: Restore Secure State - Enable a system to return to a state that is known to be secure, after a security breach occurs or if an upgrade is not successful
- ✓ GP-TM-08: Enable security by default. Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default
- ✓ GP-TM-09: Establish hard to crack device individual default passwords
- ✓ GP-TM-22: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed
- ✓ GP-TM-50: Ensure only necessary ports are exposed and available
- ✓ GP-TM-56: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors

3 Blockchain

3.1 Ιστορικό σημείωμα

(BlockchainTech)

Το 2008 μία ομάδα ή απλώς ένα άτομο υπό το όνομα Satoshi Nakamoto δημοσίευσε ένα paper με τίτλο: "Bitcoin: A Peer-To-Peer Electronic Cash System". Σε αυτή τη δημοσίευση παρουσιάζεται ένας τρόπος ηλεκτρονικής πληρωμής με χρήση της τεχνολογίας της ομότιμης σύνδεσης που θα επιτρέπει την απευθείας συναλλαγή μεταξύ των δύο ενδιαφερόμενων χωρίς τη διαμεσολάβηση οποιουδήποτε χρηματοπιστοτικού ιδρύματος. Στην πορεία δημιουργήθηκαν και άλλα ηλεκτρονικά συναλλάγματα (cryptocurrencies). Ο Συγγραφέας της πρώτης δημοσίευσης παρέμεινε ανώνυμος και ως αποτέλεσμα κανείς δεν γνωρίζει τον Satoshi Nakamoto ως σήμερα.

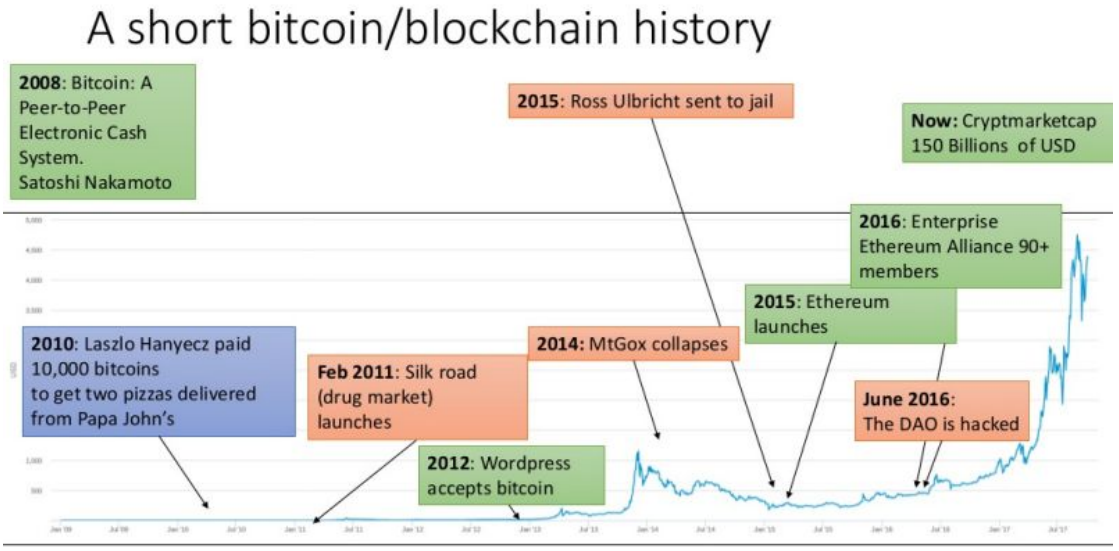
Μέσα στο 2008: δημιουργήθηκε το domain name "bitcoin.org" (18 Αυγούστου). Δημοσιεύτηκε το σχεδιαστικό μοντέλο του Bitcoin (31 Οκτωβρίου)

Το bitcoin project καταγράφτηκε στο SourceForge.net (9 Νοεμβριου)

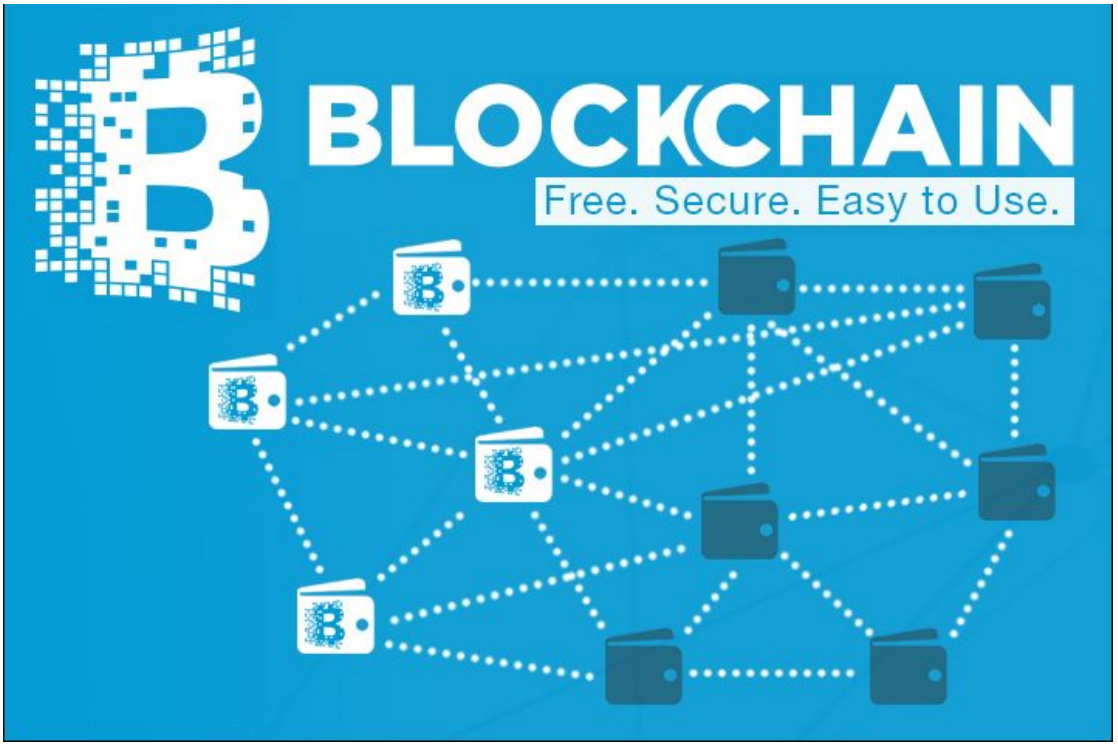
Μέσα στο 2009: Εγκαθιδρύθηκε το genesis block (3 Ιανουαρίου)

Το Bitcoin v0.1 ανακοινώθηκε στο cryptography mailing list (9 Ιανουαρίου)

Πραγματοποιήθηκε η πρώτη συναλλαγή σε bitcoin από τον Satoshi στον Hal Finney (12 Ιανουαρίου)



Το bitcoin άρχισε να γίνεται ιδιαίτερα δημοφιλές με το πέρασμα του χρόνου και είναι η πιό διαδεδομένη εφαρμογή του blockchain. Ωστόσο το blockchain βρίσκει πρόσφορο έδαφος και σε εφαρμογές που δεν σχετίζονται με τα οικονομικά.



3.2 Τι είναι το blockchain

Το blockchain είναι μια κατανεμημένη βάση δεδομένων από μπλοκ καταγραφών όλων των συναλλαγών ή των ψηφιακών γεγονότων που έχουν πραγματοποιηθεί από όλους τους συμμετέχοντες σε αυτό. Κάθε συναλλαγή που πρόκειται να πραγματοποιηθεί πρέπει πρώτα να εγκριθεί από την πλειοψηφία των συμμετεχόντων στο σύστημα. Ένα από να βασικά χαρακτηριστικά του blockchain είναι ότι κάθε γεγονός που καταγράφεται, δεν μπορεί ποτέ να διαγραφεί. Δηλαδή, στο blockchain υπάρχει γραμμένη η πληροφορία για όλα τα γεγονότα που έχουν πραγματοποιηθεί στο παρελθόν χωρίς να υπάρχει η δυνατότητα αλαγής της αλληλουχίας των γεγονότων. Η μεγαλύτερη καινοτομία του blockchain είναι ότι η λειτουργια του βασίζεται στην ομοφωνία όλων των συμμετεχόντων (distributed consensus) για την πραγματοποίηση οποιουδήποτε γεγονότος. Το blockchain ήδη χρησιμοποιείται ευρέως σε ένα πολύ μεγάλο αριθμό εφαρμογών. Το πιό τρανό παράδειγμα εφαρμογής της τεχνολογίας αυτής αποτελεί το Bitcoin. Το Bitcoin αποτελεί και την πιό

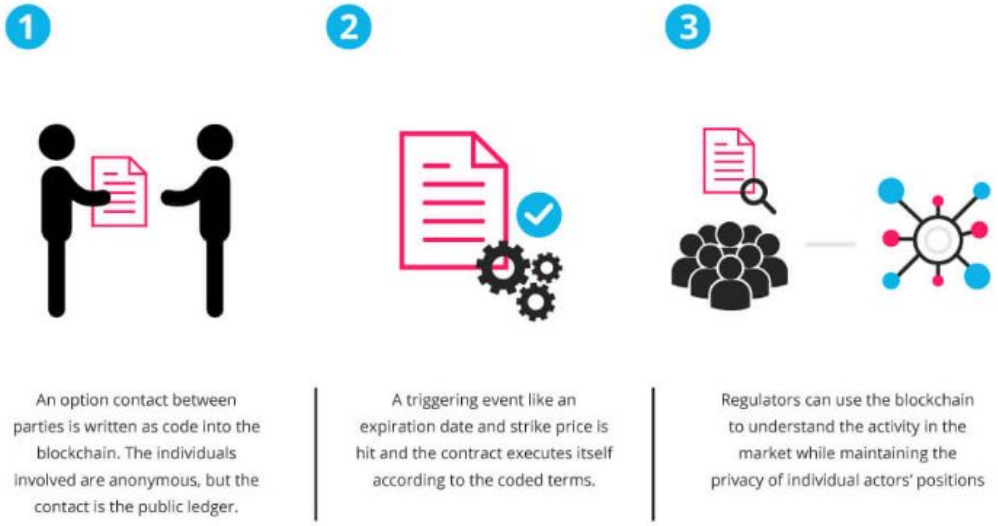
αμφιλεγόμενη εφαρμογή καθώς συμβάλλει στη δημιουργία μιας ψηφιακής αγοράς πολλών δισεκατομμυρίων δολαρίων χωρίς να υπάρχει κεντρικός έλεγχος ή κάποιο τραπεζικό σύστημα που να αποτελεί την ρυθμιστική αρχή.

(Reference: Blockchain for securing IoT)

Καθώς το σύστημα είναι κατανεμημένο, δεν υπάρχει ένα κεντρικό υπολογιστικό σύστημα που να κρατάει την συνολική πληροφορία των συναλλαγών και την αλληλουχία των block στην αλυσίδα αλλά κάθε κόμβος του συστήματος (άτομα που χρησιμοποιούν την πλατφόρμα του bitcoin) έχει ένα αντίγραφο της συνολικής πληροφορίας. Επίσης η αλυσίδα συνεχώς αυξάνεται, δεν υπάρχει δυνατότητα άλλης δραστηριότητας (παρέμβαση με άλλο τρόπο στην αλυσίδα του blockchain). Δύο είναι τα βασικά στοιχεία του blockchain, οι συναλλαγές που πραγματοποιούν οι συμμετέχοντες του συστήματος και τα blocks στα οποία καταγράφονται οι συναλλαγές αναλλοίωτες με σωστή χρονολογική σειρά. Για να εγκριθεί μία συναλλαγή πρέπει όλοι οι συμμετέχοντες ομόφωνα να συμφωνήσουν και το πιο σημαντικό, είναι ασφαλές. Ένα σετ από συναλλαγές που έχουν εγκριθεί συγκροτεί ένα block. Το block αυτό αποστέλλεται σε όλους τους συμμετέχοντες και αυτοί με τη σειρά τους εγκρίνουν το νέο block. Κάθε block περιέχει ένα κωδικό (hash) ο οποίος αποτελεί το δακτυλικό αποτύπωμα του αμέσως προηγούμενου block στην αλυσίδα.

3.3 Τι είναι τα smart contracts;

Τα smart contracts είναι συμβόλαια που καταγράφονται σε ένα σύστημα blockchain. Πιό αναλυτικά, όταν δύο μεριές θέλουν να δημιουργήσουν ένα συμβόλαιο μεταξύ τους, το συμβόλαιο αυτό καταγράφεται στο blockchain σε μορφή κώδικα. Τα μέλη που εμπλέκονται στο συμβόλαιο είναι ανώνυμα όμως το συμβόλαιο είναι δημόσια διαθέσιμο σε όλους τους κόμβους του αποκεντρωμένου συστήματος. Ένα προκαθορισμένο γεγονός όπως μια ημερομηνία ή ένα ποσό που πληρώθηκε πυροδοτεί την εκτέλεση των συμφωνηθέντων όπως αυτά έχουν καταγραφεί με τη μορφή κώδικα. Οι ρυθμιστές (συμμετέχοντες) χρησιμοποιούν το blockchain για να κατανοήσουν την κίνηση της αγοράς και ταυτόχρονα να κρατούν την ανωνυμία τους. Πρώτος που διατύπωσε την ιδέα για τα smart contracts ήταν ο Nick Szabo το 1994 όταν και ίδρυσε την εφαρμογή “Smart contracts”. Ωστόσο η εφαρμογή δεν είχε ιδιαίτερη χρησιμότητα μέχρι την εισαγωγή των ηλεκτρονικών συναλλαγμάτων “crypto currencies”. Πλέον ένα πρόγραμμα, ένα smart contract και το blockchain μπορούν να συνεργαστούν για να πραγματοποιηθούν πληρωμές όταν μία προγραμματισμένη συνθήκη που έχει συμφωνηθεί στο συμβόλαιο υλοποιηθεί. Η εφαρμογή Smart Contracts είναι πραγματικά η πιό σπουδαία μέχρι στιγμής που έχει φέρει ο κόσμος των κρυπτογραφημένων συναλλαγμάτων.



Ένα παράδειγμα smart contract. Έστω ότι ένας χρήστης θέλει να νοικιάσει ένα δωμάτιο και πληρώνει με bitcoin. Παίρνει πίσω μία απόδειξη η οποία είναι καταγεγραμμένη στο εικονικό συμβόλαιο. Ο χρήστης που έχει στην κατοχή του τα δωμάτια, στέλνει το ψηφιακό κλειδί εισόδου εντός μιας ημερομηνίας. Αν το κλειδί δεν φτάσει στην ώρα του τότε το blockchain αποζημιώνει τον ενδιαφερόμενο. Αν το κλειδί φτάσει εγκαίρως τότε η χρέωση γίνεται κανονικά ενώ ενημερώνονται όλες οι μεριές για την άφιξη του κλειδιού. Αν φτάσει το κλειδί τότε είναι σίγουρο ότι ο ιδιοκτήτης θα πληρωθεί. Αν ο ενδιαφερόμενος πληρώσει το σωστό ποσό σε bitcoin τότε θα πάρει το κλειδί. Το αρχείο ακυρώνεται με τη λήξη της συναλλαγής και κανείς δεν μπορεί να παρέμβει σε αυτό καθώς θα γίνει αντιληπτός από το σύνολο των χρηστών.

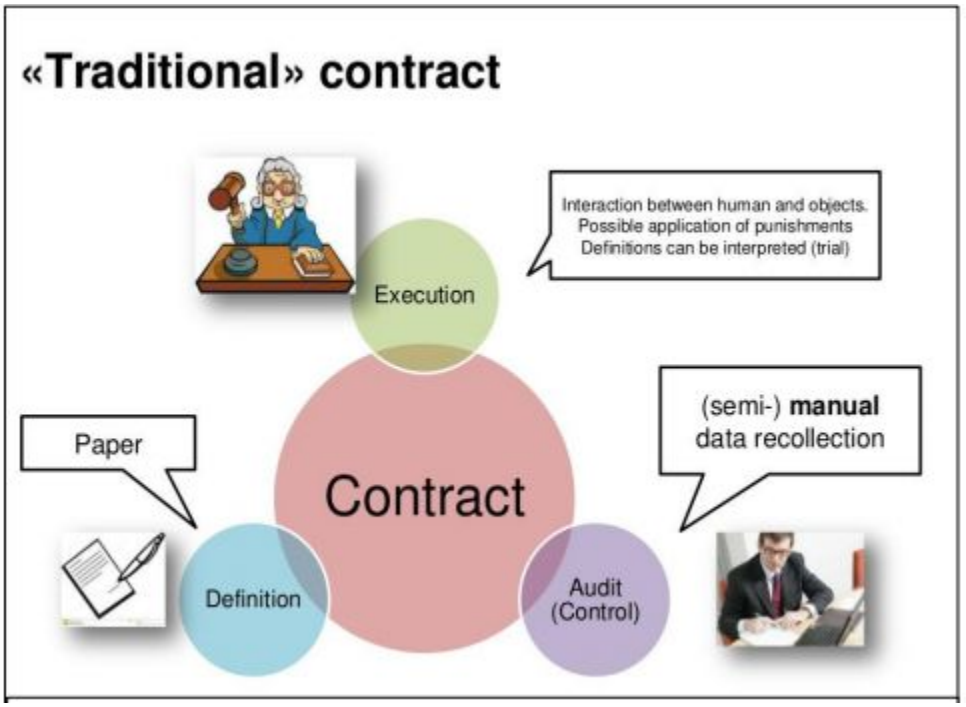
Οι πιό γνωστές εταιρείες ανοιχτού κώδικα που υποστηρίζουν τα Smart Contracts χρησιμοποιώντας την τεχνολογία του blockchain είναι η Etherium και η Codius. Πολλές εταιρείες που λειτουργούν πάνω στο bitcoin και στο blockchain υποστηρίζουν τα Smart Contracts. Υποθέσεις που αφορούν την μεταφορά περιουσιακών στοιχείων υπό προϋποθέσεις, οι οποίες απαιτούν την παρουσία δικηγόρων για να συνταχθεί ένα συμβόλαιο καθώς και τράπεζες που θα παρέχουν χρηματικές εγγυήσεις μπορούν πλέον να αντικατασταθούν από Smart Contracts.

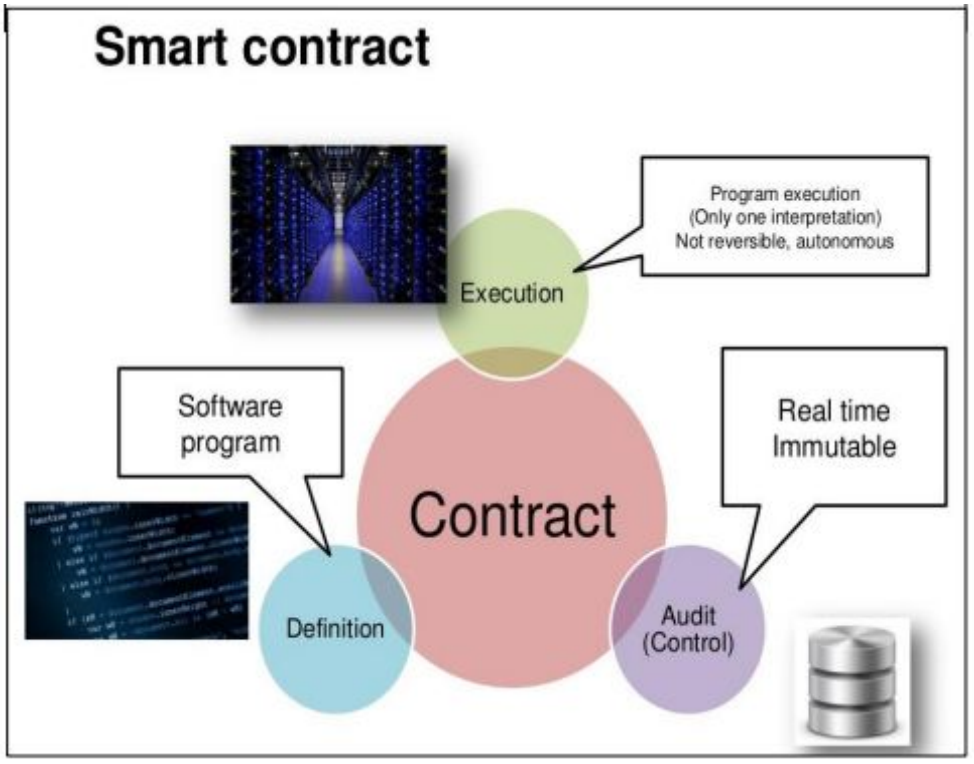
Η Ethereum έχει δημιουργήσει πολύ ενθουσιασμό με τις δυνατότητες που προσφέρει. Το πιο βασικό είναι ότι επιτρέπει σε όλους να δημιουργήσουν το δικό τους κρυπτογραφημένο νόμισμα και να το χρησιμοποιήσουν για την εκτέλεση και την πληρωμή των smart contracts. Η Ethereum από μόνη της έχει το δικό της κρυπτονόμισμα (ether). Η Ethereum ήδη τροφοδοτεί μία μεγάλη γκάμα από εφαρμογές σε τομείς όπως η διακυβέρνηση, οι αυτόνομες τράπεζες, η πρόσβαση

χωρίς κλειδί (keyless access), η χρηματοδότηση από το πλήθος (crowdfunding) συναλλαγές με χρηματοοικονομικά παράγωγα και άλλα.

Επιπλέον υπάρχει πολλά blockchains τα οποία υποστηρίζουν μία μεγάλη γκάμα εφαρμογών και όχι μόνο κρυπτογραφημένα συναλλάγματα. Αυτή τη στιγμή τρεις είναι οι βασικές προσεγγίσεις στην βιομηχανία οι οποίες αποσκοπούν στην υποστήριξη άλλων εφαρμογών καθώς επίσης και την υπερπήδηση αντιλειπτών περιορισμών του Bitcoin blockchain:

1) **Alternative Blockchains** είναι ένα σύστημα που χρησιμοποιεί τον αλγόριθμο του blockchain για να πετύχει κατανεμημένη ομοφωνία πάνω σε ένα συγκεκριμένο ψηφιακό θέμα. Μπορεί να μοιράζεται και miners με ένα γονικό δίκτυο όπως του Bitcoin (αυτό αποκαλείται merged mining). Τα alternative blockchains έχουν προταθεί ώστε να εφαρμοστούν σε εφαρμογές όπως DNS, SSL αρχή πιστοποίησης, αποθήκευση αρχείων καθώς επίσης και ψηφοφορίες.
2) Τα **Colored Coins** τα οποία περιγράφουν μια κλάση μεθόδων για την αναπαράσταση και διαχείριση περιουσιακών στοιχείων του πραγματικού κόσμου πάνω στο Blockchain του Bitcoin. Παρά το γεγονός ότι το Bitcoin σχεδιάστηκε για να γίνει συνάλλαγμα, η scripting language του Bitcoin επιτρέπει την αποθήκευση μικρών ποσοτήτων μεταδεδομένων στο blockchain τα οποία μπορούν να αναπαριστούν εντολές για την διαχείριση περιουσιακών στοιχείων. Για παράδειγμα, μπορούμε να καταγράψουμε σε μία συναλλαγή ότι 100 μονάδες ενός αντικειμένου έχουν πιστωθεί σε μια δεδομένη διεύθυνση Bitcoin.
3) **Sidechains** είναι εναλλακτικές blockchains οι οποίες υποστηρίζονται από το Bitcoin μέσω του Bitcoin Blockchain όπως το δολάριο και η λίρα υποστηρίζονται από το χρυσό. Ένας μπορεί να έχει στην κατοχή του χιλιάδες sidechains συνδεδεμένες με το Bitcoin, κάθε μία με διαφορετικά χαρακτηριστικά και χρησιμότητα ενώ όλα εκμεταλλεύονται την σπανιότητα και την ελαστικότητα που εξασφαλίζει το Bitcoin Blockchain. Το Bitcoin Blockchain μπορεί με τη σειρά του να υποστηρίξει επιπλέον χαρακτηριστικά για πειραματικές sidechains, αφού έχουν πρώτα δοκιμαστεί και ελεγχθεί.Εταιρίες όπως οι IBM, Samsung, Overstock, Amazon, UBS, Citi, Ebay, Verizon Wireless αναζητούν εναλλακτικές και καινοτόμες χρήσεις του Blockchain για τις δικές τους εφαρμογές.





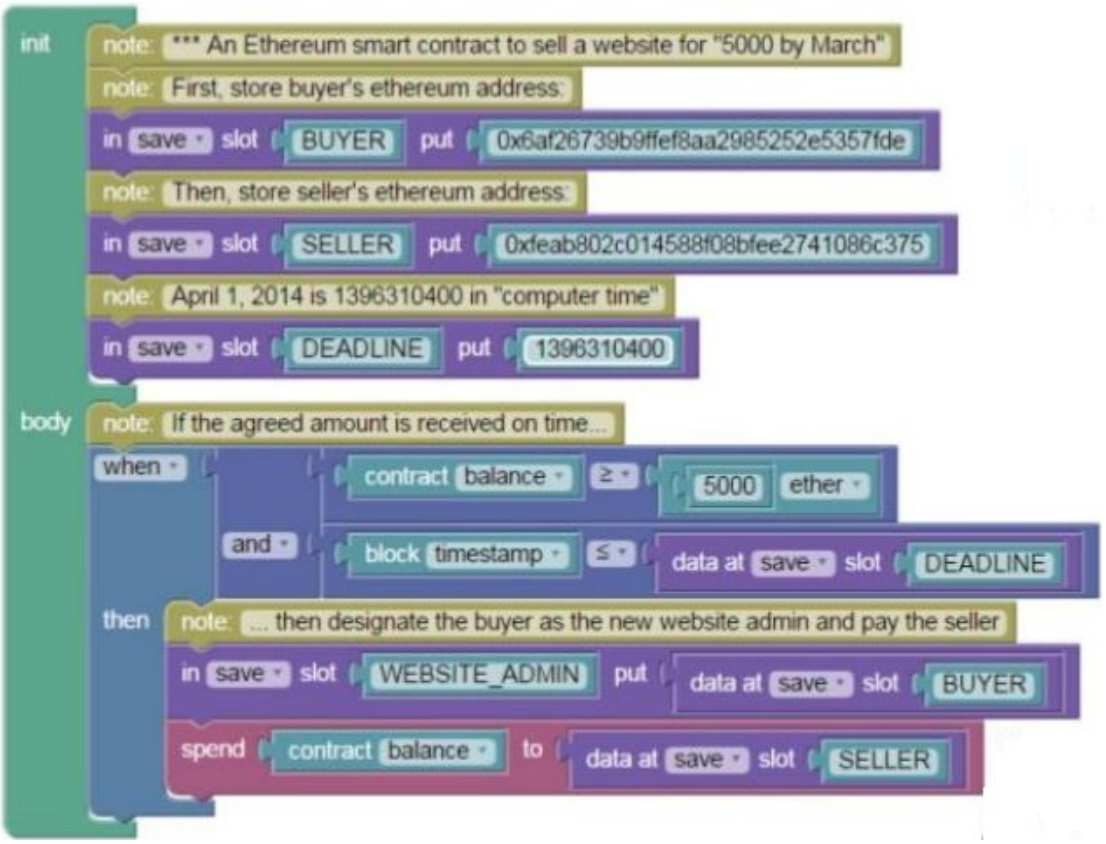
Το bitcoin είναι ένα smart contract.

1) Είναι πρόγραμμα
2) Η εκτέλεση του είναι αυτόνομη (επειδή το δίκτυο είναι αποκεντρωμένο)
3) Όλες οι συναλλαγές πραγματοποιούνται δημόσια

4) Δεν υπάρχει δυνατότητα να μεταβληθεί το ιστορικό των συναλλαγών (δηλαδή η εκτέλεση δεν μπορεί να αναστραφεί)

Κάποια άλλα χαρακτηριστικά του είναι:

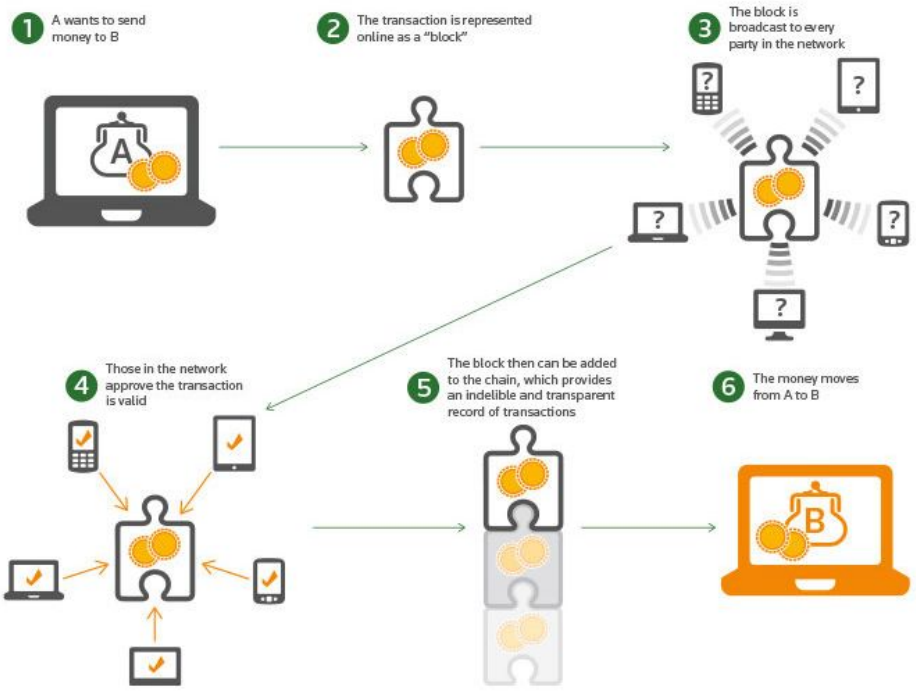
1) Δεν μπορούν να υπάρξουν συνολικά πάνω από 21.000.000 bitcoins
2) Ένα νέο block παράγεται κάθε 10 λεπτά
3) Η δυσκολία εξόρυξης bitcoin εξαρτάται άμεσα από την ενέργεια του συστήματος
4) Μόνο ένα υποσύνολο των πιθανών συναλλαγών γίνονται δεκτές



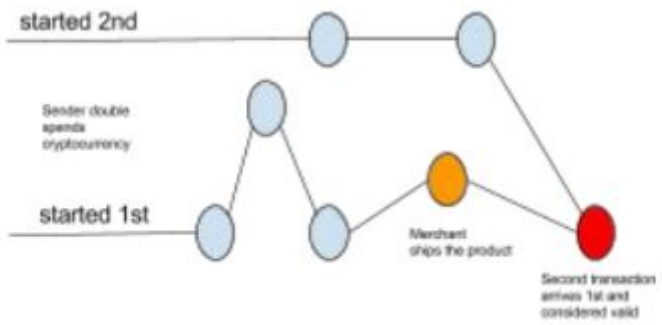
3.4 Περιγραφή του Framework

Οι οικονομικές συναλλαγές που λαμβάνουν χώρα στο διαδίκτυο είναι στενά συνδεδεμένες με κάποιο χρηματοπιστωτικό ινστιτούτο. Αυτό συμβαίνει διότι στο ηλεκτρονικό εμπόριο υπάρχει μεγάλος κίνδυνος απάτης. Ωστόσο, η εξάρτηση των συναλλαγών από κάποια τράπεζα ή κάποιον άλλο εγγυητή έχει ώς αποτέλεσμα την

αύξηση του κόστους κάθε συναλλαγής. Η καινοτομία του blockchain (μέσω του bitcoin) έγκειται στην αποδέσμευση του εμπορίου από τραπεζικά συστήματα και την εμπιστοσύνη πλέον στο λογισμικό ανοιχτού κώδικα και τους νόμους των μαθηματικών. Καθε συναλλαγή προστατεύεται από μία ηλεκτρονική υπογραφή. Κάθε συναλλαγή στέλνεται στο δημόσιο κλειδί του δέκτη ψηφιακά υπογεγραμμένο με το ιδιωτικό κλειδί του αποστολέα. Για να ξοδέψει κάποιος bitcoin πρέπει πρώτα να αποδείξει την κατοχή του ιδιωτικού κλειδιού. Ο δέκτης της συναλλαγής με το ηλεκτρονικό νόμισμα, επαληθεύει την ψηφιακή υπογραφή (άρα και τον κάτοχο του ιδιωτικού κλειδιού) χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα.

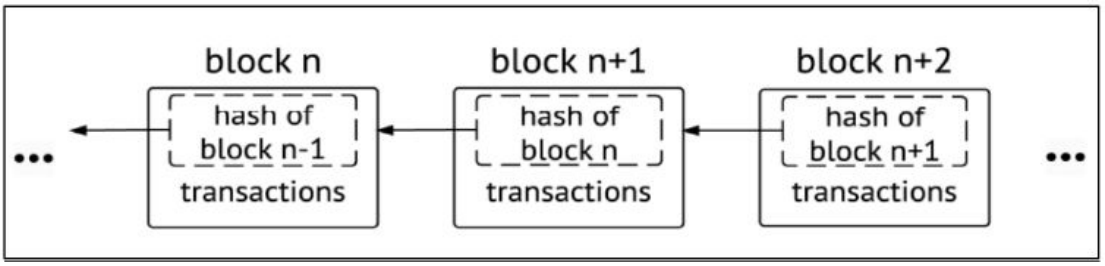


Εντούτοις, έχει δημιουργηθεί το ερώτημα για το πως θα διατηρείται ή σωστή χρονολογική σειρά των συναλλαγών που αποστέλλονται σε όλους τους κόμβους του συστήματος του bitcoin. Οι συναλλαγές δεν είναι δεδομένο ότι θα φτάσουν με τη σειρά με την οποία δημιουργήθηκαν και γι αυτό το λόγο υπάρχει ανάγκη στο σύστημα η αποφυγή του φαινομένου double-spending, δηλαδή το να καταφέρει κάποιος κακόβουλος χρήστης να ξοδέψει ένα ποσό σε bitcoin 2 φορές. Αυτό συμβαίνει διότι η πληροφορία της συναλλαγής περνάει από κόμβο σε κόμβο με αποτέλεσμα δύο συναλλαγές που «γεννήθηκαν» με κάποια χρονική σειρά, να φτάσει πρώτη σε κάποιον κόμβο εκείνη που παράχθηκε τελευταία.



Double spending due to propagation delays in peer-to-peer network.

Γι αυτό το λόγο υπάρχει ανάγκη να αναπτυχθεί ένας μηχανισμός ώστε ολόκληρο το δίκτυο του Bitcoin να μπορεί να συμφωνεί σχετικά με την αλληλουχία των συναλλαγών, κάτι που είναι ιδιαίτερα απαιτητικό σε ένα κατανεμημένο σύστημα. Το bitcoin λύνει αυτό το πρόβλημα χρησιμοποιώντας την τεχνολογία του Blockchain. Το bitcoin ταξινομεί τις συναλλαγές σε ομάδες που ονομάζονται blocks και στη συνέχεια συνδέει μεταξύ τους αυτά τα blocks και έτσι δημιουργεί το blockchain, δηλαδή μία αλυσίδα από blocks. Όλες οι συναλλαγές που έχουν ταξινομηθεί σε ένα block θεωρείται ότι έχουν συμβεί την ίδια χρονική στιγμή. Τα blocks με τη σειρά τους είναι και αυτά ταξινομημένα με τη σωστή χρονολογική σειρά και κάθε block περιέχει τον κωδικό του προηγούμενου block.



Παραμένει όμως ένα πρόβλημα. Κάθε κόμβος του συστήματος μπορεί να συλλέξει συναλλαγές που δεν έχουν εγκριθεί και να δημιουργήσει ένα block και να το προτείνει στο σύστημα ως το επόμενο block που θα πρέπει να μπει στην αλυσίδα. Πως το σύστημα επιλέγει ποιό block θα πρέπει να μπει επόμενο στην αλυσίδα; Θα μπορούσαν πολλά blocks που έχουν δημιουργηθεί από διαφορετικούς κόμβους την ίδια χρονική στιγμή. Προφανώς δεν μπορούμε να αποφασίσουμε με βάση τη σειρά που έφτασαν σε έναν κόμβο καθως μπορεί να φτάσουν με διαφορετική σειρά σε διαφορετικά σημεία του δικτύου. Το bitcoin λύνει και αυτό το πρόβλημα εισάγοντας ένα μαθηματικό puzzle: κάθε block θα γίνεται αποδεκτό στο blockchain με την προϋπόθεση ότι έχει τη λύση για κάποιο ειδικό μαθηματικό πρόβλημα. Αυτό είναι επίσης γνωστό και ως “proof of work” δηλαδή απόδειξη ότι ο υπολογιστής «εργάστηκε» καταναλώνοντας υπολογιστικούς πόρους ώστε να λύσει το μαθηματικό πρόβλημα. Όταν ένας υπολογιστής κατασκευάζει ένα block, στο τέλος αυτού

μαντεύει και τη λύση ενός συγκεκριμένου μαθηματικού προβλήματος. Το πρόβλημα αυτό είναι τύπου cryptographic hash, δηλαδή ο υπολογιστής μαντεύει έναν αριθμό ο οποίος περνά από μία συνάρτηση hash για να βγει το τελικό αποτέλεσμα ώστε να ελεγχθεί αν η λύση είναι σωστή. Ένα απλό παράδειγμα είναι ότι μετά το hash, το αποτέλεσμα συγκρίνεται με έναν αριθμό και ανάλογα το τι ζητάει το πρόβλημα η λύση σημειώνεται ως σωστή ή ως λανθασμένη. Πρέπει να σημειωθεί ότι η συνάρτηση που χρησιμοποιεί η διαδικασία του hash είναι η SHA-256^2. Επιπλέον, η δυσκολία συγκεντρώνεται στην επίλυση του προβλήματος καθώς όλοι οι κόμβοι μπορούν άμεσα να ελέγξουν την εγκυρότητα μιας απάντησης, οπότε μπορούν αμέσως να επαληθεύσουν αν ένα block είναι έγκυρο αλλά δεν μπορεί να μαντέψει ποιό ήταν το input της hash.(ICCS-NTUA, January 2018)

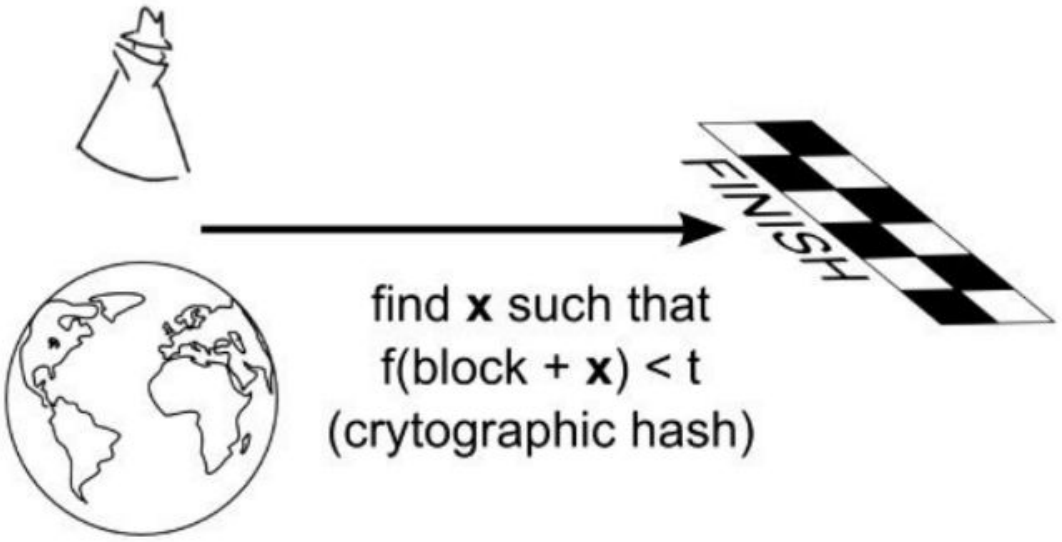
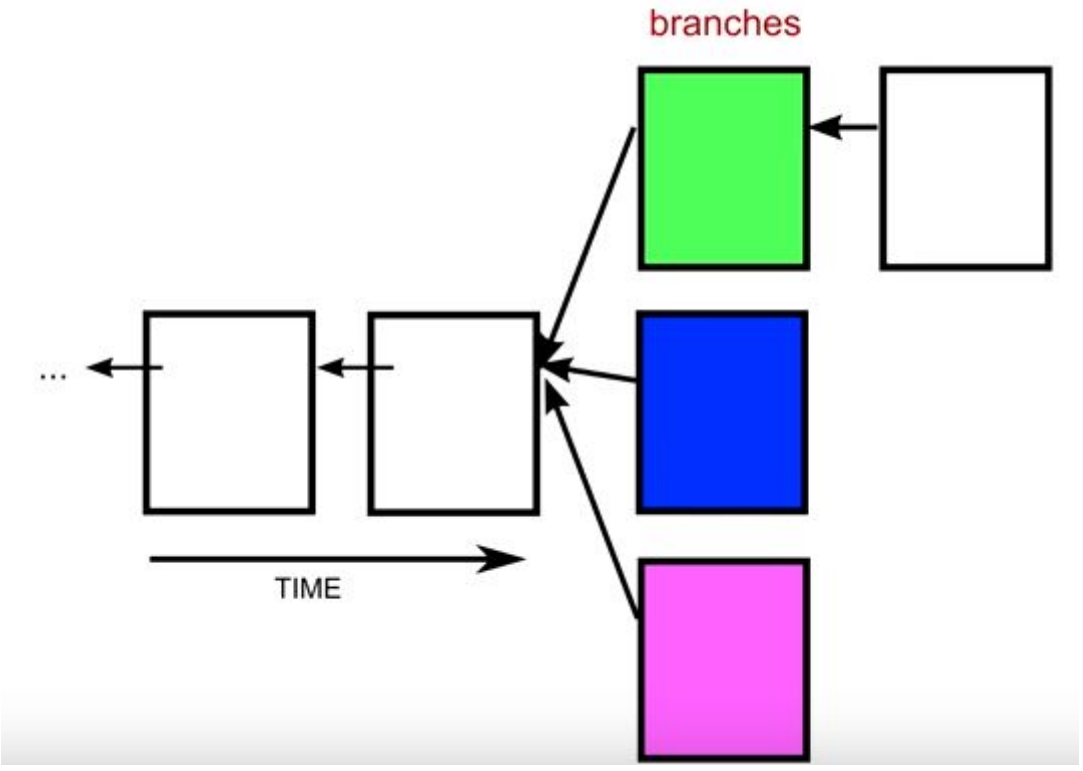


Figure 5 Mathematical race to protect transactions-I[3].

Έχει υπολογιστεί ότι το μαθηματικό πρόβλημα που καλείται να λύσει ένας απλός υπολογιστής (δηλαδή μέχρι να μαντέψει σωστά τη λύση), απαιτεί κατα μέσο όρο κάποια χρόνια. Στο δίκτυο όμως του bitcoin ένας υπολογιστής θα βρίσκει λύση καθε 10 λεπτα περίπου. Έτσι λοιπόν δεν μπορεί ο καθένας να προτείνει οποιαδήποτε στιγμή το δικό του block συνεπώς η τυχαιότητα του νικητή προσδίδει αξιοπιστία στο σύστημα. Επιπλέον, το σύστημα προσπαθεί να κρατάει αυτό το διάστημα των 10 λεπτών. Όσο μεγαλώνει το σύστημα σε ποσότητα (περισσότεροι υπολογιστές) αλλά και εξελίσσεται η απόδοση των επεξεργαστών, αν κρατούσαμε σταθερή την πολυπλοκότητα των μαθηματικών προβλημάτων του blockchain τότε ο αναμενόμενος χρόνος επίλυσης του προβλήματος από κάποιον κόμβο του δικτύου θα μειωνόταν. Οπότε ανάλογα με την υπολογιστική δύναμη του δικτύου την κάθε στιγμή,

προσαρμόζεται η πολυπλοκότητα ώστε ο χρόνος των 10 λεπτών να παραμένει πρακτικά σταθερός.

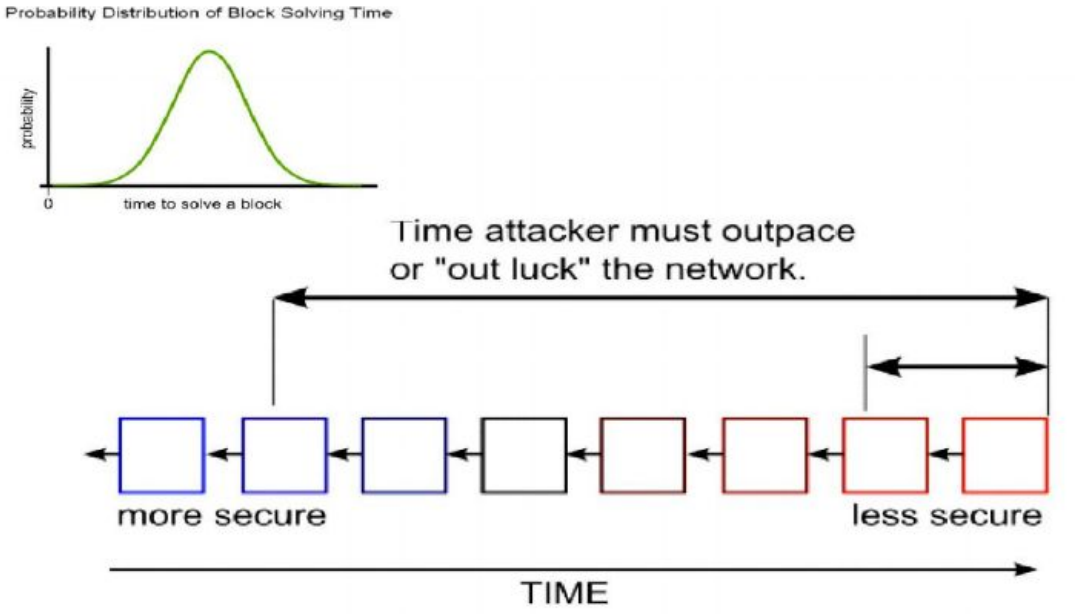
Κανείς όμως δεν μπορεί να αποκλείσει το ενδεχόμενο 2 ή παραπάνω υπολογιστες να βρουν τη λύση ταυτόχρονα (ή πολύ κοντά χρονικά). Αυτό σημαίνει ότι τα block που προτείνουν είναι όλα αποδεκτά. Όταν λοιπόν 3 υπολογιστές βρουν ταυτόχρονα λύση, τότε και οι τρείς στέλνουν τα block που δημιούργησαν στο σύστημα, με αποτέλεσμα όλοι οι κόμβοι να λάβουν 3 blocks. Αφού λοιπόν και τα 3 blocks είναι αποδεκτά, αυτό σημαίνει ότι η αλυσίδα που έχει ο κάθε κόμβος διακλαδώνεται.



Ο επόμενος κόμβος που θα λύσει το επόμενο μαθηματικό πρόβλημα θα συνεχίσει το χτίσιμο της αλυσίδας του πάνω στο block που του ήρθε πρώτο από τα προηγούμενα 3 ενώ τα άλλα 2 block θα καταργηθούν ενώ τα transactions που περιέχουν θα περιμένουν εκ νέου να εγκριθούν και να οργανωθούν σε κάποιο επόμενο block. Έτσι λοιπόν ανεξάρτητα με το ποιό από τα 3 block εφτασε πρώτο σε κάθε κόμβο, η αλυσίδα που θα υιοθετήσουν από εδώ και στο εξής όλοι οι κόμβοι θα είναι αυτή που πρότεινε ο επόμενος νικητής του μαθηματικού διαγωνισμού. Υπάρχει περίπτωση και στην επόμενη φάση να υπάρχουν πάνω από 2 νικητές οπότε η διαδικασία θα συνεχιστεί όπως περιγράφηκε. Ωστόσο η πιθανότητα το να υπάρχουν πάνω από δύο λύσεις ταυτόχρονα είναι πολύ μικρή και ώς εκ τούτου η πιθανότητα να συμβεί αυτό σε συνεχόμενους διαγωνισμούς είναι ακόμα μικρότερη, με αποτέλεσμα το σύστημα να σταθεροποιείται σχετικά γρήγορα.

Οι κόμβοι που χρησιμοποιούν τους υπολογιστικούς τους πόρους για να επιλύσουν το μαθηματικό πρόβλημα και να δημιουργήσουν ένα καινούριο block αποκαλούνται “miners” και αμείβονται οικονομικά (σε bitcoin) για την συμβολή τους.

Το δίκτυο αποδέχεται την μεγαλύτερη αλυσίδα ως αποδεκτή. Το γεγονός αυτό καθιστά σχεδόν αδύνατο για οποιονδήποτε κακόβουλο να προτείνει μία απατηλή συναλλαγή αφού για να το πράξει αυτό δεν πρέπει μόνο να παράξει ένα νέο block επιλύοντας το μαθηματικό πρόβλημα αλλά πρέπει και να το πράξει την ίδια στιγμή που ανταγωνίζεται όλο το σύστημα για να παράξει όλα τα μεταγενέστερα blocks. Μόνο έτσι θα μπορέσει να πείσει όλους τους υπόλοιπους κόμβους να δεχτούν τις συναλλαγές και τα block τα οποία εκείνος έχει προτείνει. Το έργο του κακόβουλου κόμβου γίνεται ακόμη πιο δύσκολο καθώς τα blocks στο blockchain συνδέονται μεταξύ τους μέσω κρυπτογραφίας.



4 Blockchain για IoT Security

Ενώ είναι ακόμα στα πρώτα στάδια ανάπτυξης του, το IoT αποτελείται ως επί το πλείστων από τεχνολογίες που επιτρέπουν τη συλλογή δεδομένων, την απομακρυσμένη παρακολούθηση και τον έλεγχο των συσκευών. Καθώς η τεχνολογία προχωράει, το IoT θα εξελιχθεί σε ένα δίκτυο αυτόνομων συσκευών που μπορούν να αλληλεπιδρούν μεταξύ τους και με το περιβάλλον τους και να κάνουν έξυπνες αποφάσεις χωρίς ανθρώπινη παρέμβαση. Εδώ το blockchain μπορεί να λάμψει και να αποτελέσει τη βάση που θα υποστηρίξει μια κοινή οικονομία που βασίζεται στην

μηχανή-to-machine (M2M) επικοινωνία. Η Blockchain τεχνολογία είναι ο συνδετικός κρίκος για να διευθετήσει τις ανησυχίες προστασία της ιδιωτικής ζωής και την αξιοπιστία του IoT. Μπορεί να χρησιμοποιηθεί για την παρακολούθηση δισεκατομμύρια συνδεδεμένων συσκευών, που επιτρέπει την επεξεργασία των συναλλαγών και του συντονισμού μεταξύ των συσκευών. Αυτό επιτρέπει σημαντική εξοικονόμηση για τους κατασκευαστές της βιομηχανίας IoT. Αυτή η αποκεντρωμένη προσέγγιση θα εξαλείψει ενιαία σημεία της αποτυχίας, δημιουργώντας ένα πιο ανθεκτικό οικοσύστημα για συσκευές που θα τρέξουν πάνω σε αυτό. Οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται στα blockchains θα κάνει τα δεδομένα των καταναλωτών πιο ιδιωτικά και ασφαλή. Το καθολικό (ledger) του blockchain είναι απαραβίαστο και δεν μπορεί να χειραγωγηθεί από κακόβουλους παράγοντες, διότι δεν υπάρχει σε μία μόνο θέση, και επιθέσεις δεν μπορούν να οργανωθούν επειδή δεν υπάρχει ένα ενιαίο νήμα της επικοινωνίας που μπορεί να υποκλαπεί. Το blockchain καθιστά δυνατή ασφαλή, peer-to-peer ανταλλαγή μηνυμάτων και έχει

4.1 Introduction

- Blockchain Technologies will have a great impact on our lives in the near future. It was initially introduced to make Bitcoin work and since then the idea behind the Blockchain is being used in many deferent areas. There is currently a lot of market speculation about Blockchain and its possible use-cases on securing IoT ecosystem.

- IoT Security is an open issue. There have been proposed many deferent ways in order to find solutions, although there are still many difficulties. There are many different ways to attack an IoT system and none of the solutions that have been already proposed are able to offer catholic protection. In this report, three different reasons are introduced to explain why Blockchain is an attractive technology to use in IoT solutions. Blockchain can also help operators increase the IoT value chain by enabling new business models.

What is Blockchain?

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer-to-peer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has

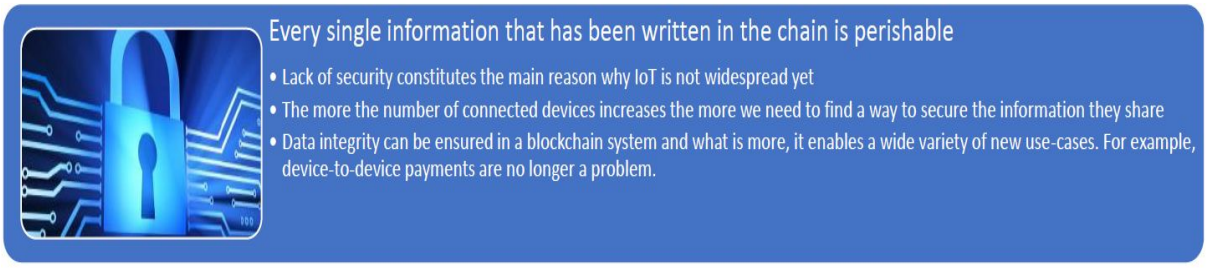
worked flawlessly and found wide range of applications in both financial and nonfinancial world.

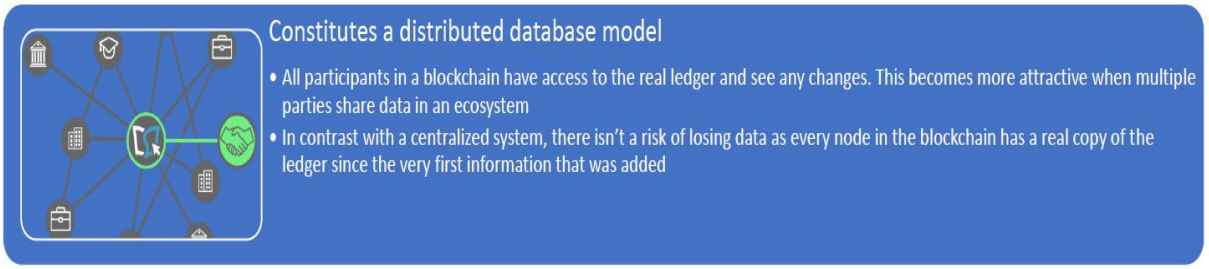
The new concept behind blockchain is that establishes a system of creating a **distributed consensus** in the digital online world. This allows everyone participating in a specific blockchain to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It is the first step to a more democratic open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology and revolution in this space has just begun.

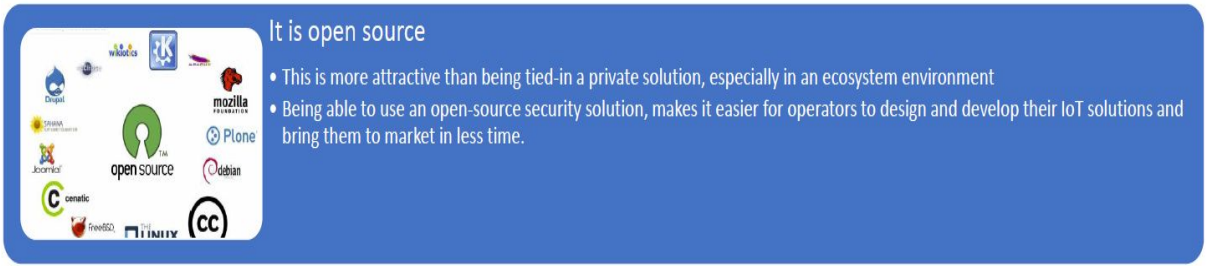
4.2 Securing IoT Systems with Blockchain Technology

Is IOT the new cash cow? Not as simple as it seems

4.2.1 Why blockchain may be vital for iot systems?

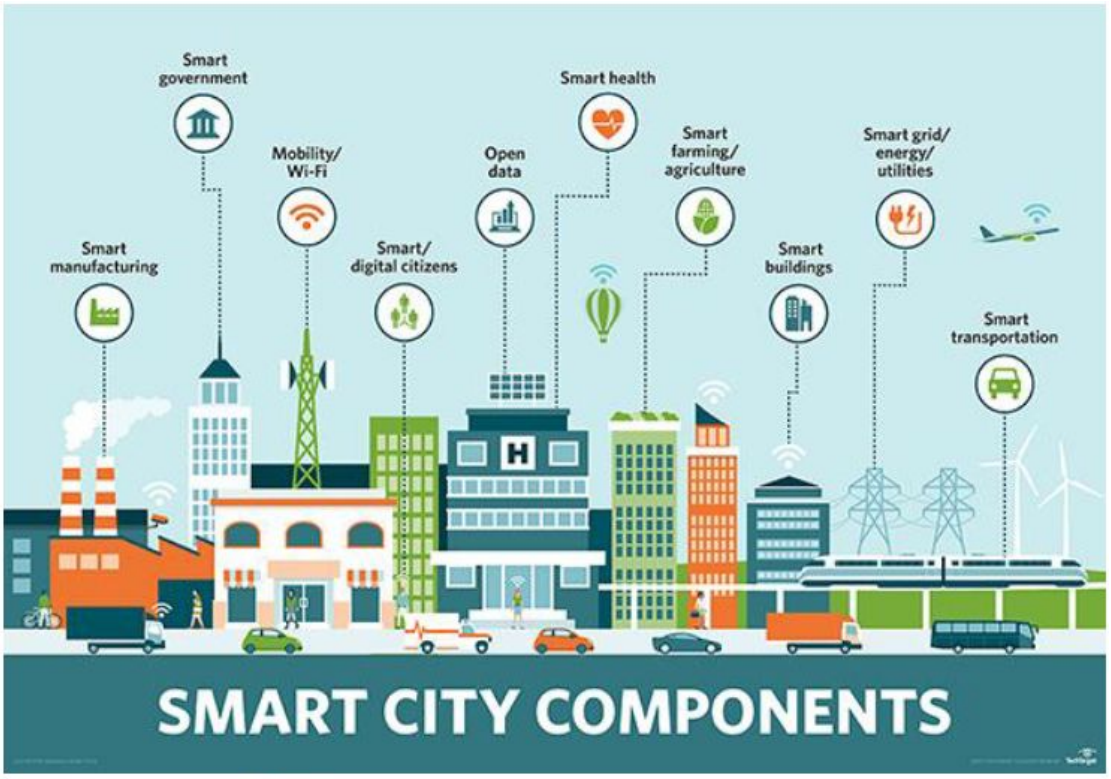






4.2.2 The iot revolution has begun. The world is moving rapidly in a new era of hyper-connection and automation

How this idea is going to become a reality if data shared between any component are not secure?



Smart city components share information autonomously

4.3 Smart cars and the necessity of a secure IoT ecosystem

Autonomous car in a smart city

-By sending and receiving information, a car can communicate with its environment seamlessly. So it becomes possible to automatize operations such as paying road tolls and parking fees, share insurance details in case of an accident. These operations don't demand real time transactions so there is no need for an ultra-low latency network.

Can blockchain play the role of a regulator?

- It is unlikely that a city would choose ONLY ONE network provider
- Cities are more likely to build these capabilities gradually using more than one network providers
- On the other hand blockchain can provide a trusted platform for data sharing

How blockchain's audit trail enhances iot device security

- Blockchain becomes a part of an IoT device since its manufacturing stage

- The details of the device's configuration is compressed into a hash code and connected to the blockchain network while an individual public/private key is created

- Now the device is uniquely identified in the Blockchain

- A smart contract is embedded in the device and determines who has the authority to change its configuration

Security specifics

- Every different configuration of the device is continually logged as a transaction in the blockchain

- Any minimal change of the hash code is detected and raises an incident alert

- Any change of the device's configuration by the owner requires:

-The device to validate the identity of the owner through public/private keys

-The device to identify the information. The software update is hashed by the owner and placed in the blockchain. Once the device receives the update information it automatically creates a hash. The match of the two hashes provides the evidence of compatibility. After this condition is fulfilled the device installs the new software update and logs the new hash of its new configuration o the blockchain

Use-cases

Telstra experimenting with blockchain

- Telstra has been experimenting with using blockchain to prevent smart home device fraud using the protocol explained above

- Implements the usage of biometric data to ensure that any modification to the device's configuration can be authenticated via fingerprint

- Any attempt to violate the blockchain-protected device's configuration is detected in less than a second

Minimizing financial loss in the logistics industry

- Cargo and logistics industry experiences significant losses due to goods being damaged, lost, stolen or delayed in transit every year

- Installing an IoT chip to track goods, sharing data describing the condition as well as the location of the products enables:

  -The identification of the place and time of a potential theft -Liability when goods are lost or damaged

4.4 Human intervention can be excluded from device-to-device networks

We are moving in a world of hyper-connection and hyper-automation. In order for that vision to become a reality, a distributed cloud platform is essential so that IoT devices can share data securely.

Imagine a car with a smart contract and a cryptocurrency wallet embedded

- Possibilities:

-The smart contract enables the device to share or sell information with appropriate timing

-A cryptocurrency wallet allows the device to make and receive payments

Use-cases

Device-to-device payments

Granting location access through smart locks

Enabling the 'sharing economy'

D2D payments

- Smart cars (smart contract + crypto embedded) to make payments without human intervention can increase user convenience. It could also be very useful with shared vehicles.

- The car can make transactions using its cryptocurrency wallet:

-In some cases a city may want to introduce a crypto-token system tied to the dollar, for instance, to be used for payments made to city infrastructure

-These payments can then be settled with “real money” at the end of the month, like a credit card.

smart locks allowing exclusive location access

- Blockchain introduces the smart locks. Smart locks allow access only to those who meet certain criteria, which is securely stored on a blockchain
- Access can be given to anybody by sending an encrypted key
- The user is uniquely identified and the access can be time limited

eg. You could use a smart key to grant a healthcare worker access to your elderly relatives’ home for two hours – the key would only be useable during that time period

The “death” of possession

- Assets can be shared and not owned privately eg. cars and expensive equipment
- One of the challenges of that vision is what happens when damage or loss occurs

-the assets’ location and condition can be connected to a blockchain which provides liability

-the user can be uniquely identified by using smart keys or biometric data.

Blockchain can contribute significantly but it doesn't consist a panaceA

- Blockchain doesn't prevent attemps to tamper data although it quickly identifies such attemps
- High computing power is massively required
- Time-sensitive applications can take a hit due to the increasing latency of the blockchain network
- It is not clear which party is going to be charged with the extra costs of the D2D transactions

References:

[1] The Blockchain Concept in the Serlot Project (ICCS-NTUA)

[2]Ευφροσύνη Θ. Ζώτου, 2012, "Σύγχρονες Τεχνολογίες Πρόσβασης και Διαδικτύου σε Έξυπνα Δίκτυα (SmartGrids)"

[3]Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, 17(4), pp.2347-2376.

[4].Whitmore, A., Agarwal, A. and Da Xu, L. (2014). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, 17(2), pp.261-274.

[5]"Αρχιτεκτονική και Λειτουργιά οικιακού δικτύου smart home", Καλύβας Βασίλειος,

[6].Perera, C., Liu, C., Jayawardena, S. and Min Chen (2014). A Survey on Internet of Things From Industrial Market Perspective. *IEEE Access*, 2, pp.1660-1679.

[7] Kevin Ashton,1999,"That 'Internet of Things' Thing"

[8]Καλύβας Βασίλειος,2015,"Αρχιτεκτονική και Λειτουργία οικιακού δικτύου smart home"

[9]IERC Cluster Book, 2014,' Internet of Things: From Research and Innovation to Market Deployment'

[10] Geng Wu, Talwar, S., Johnsson, K., Himayat, N. and Johnson, K. (2011). M2M: From mobile to embedded internet. *IEEE Communications Magazine*, 49(4), pp.36-43.

[11]Παντισκα Λεονάρδος,2016, "Έξυπνα Ενεργειακά Δίκτυα: Διαχείριση και Εφαρμογές"

[12]Armerding, T. (2018). *The IoT: Gateway for enterprise hackers*. [online] CSO Online. Available at: http://www.csoonline.com/article/3148806/internet-of-things/the-iot-gateway-for-enterprise-hackers.html [Accessed 27 Jun. 2018].

[13]Jacoby, D. (2018). *IoT: el día que ataqué mi propia casa*. [online] Securelist - Kaspersky Lab: informes y resultados de investigaciones sobre ciberamenazas. Available at: https://securelist.lat/iot-el-da-que-ataqu-mi-propia-casa/72452/ [Accessed 27 Jun. 2018].

[14] Romualdo-Suzuki, L. (2015). Internet of Things, the Hype and the Roadmap for Intelligent Buildings. *Engineering & Technology Reference*.

[15] Federico Maggi,'Rogue Robots:Testing the limits of an industrial robot's security'

[16]Shancang Li & Li Da Xu &Shanshan Zhao,'The internet of things: A survey'

[17]Enisa.europa.eu. (2018). *Major DDoS Attacks Involving IoT Devices — ENISA*. [online] Available at: https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices [Accessed 27 Jun. 2018].

[18]Energycollection.us. (2018). [online] Available at: http://www.energycollection.us/Companies/ICIT/Rise-Machines.pdf [Accessed 27 Jun. 2018].

[19]Perera, C., Liu, C., Jayawardena, S. and Min Chen (2014). A Survey on Internet of Things From Industrial Market Perspective. *IEEE Access*, 2, pp.1660-1679.

[20]Manufacturingtomorrow.com. (2018). *What is Smart Manufacturing & the Smart Factory? | ManufacturingTomorrow*. [online] Available at: https://www.manufacturingtomorrow.com/article/2017/02/what-is-smart-manufacturing--the-smart-factory/9166) [Accessed 27 Jun. 2018].

[21]Today's Motor Vehicles. (2018). *Caterpillar advancing Internet of Things strategy - Today's Motor Vehicles*. [online] Available at:

http://www.todaysmotorvehicles.com/article/truck-design-caterpillar-uptake-internet-of-things-030615/ [Accessed 27 Jun. 2018].

[22]Anon, (2018). [online] Available at: http://blogs.ptc.com/2015/05/05/airbus-uses-iot-to-fuel-factory-of-the-future/?_ga=1.116069893.2673346 23.1477138158 [Accessed 27 Jun. 2018].

[23]Drinkwater, D. (2018). *How IoT is helping Airbus to make better planes - and bigger revenues*. [online] Internet of Business. Available at: https://internetofbusiness.com/iot-helping-airbus-make-planes-better/ [Accessed 27 Jun. 2018].

[24]Think Progress UK. (2018). *Industry 4.0 - What is it and why it matters - Think Progress UK*. [online] Available at: http://www.think-progress.com/blog/performance-and-productivity/industry-4-0-what-is-it-and-why-it-matters/ [Accessed 27 Jun. 2018].

[25]Internet Of Things Wiki. (2018). *Nest Learning Thermostat, 3rd Generation - Internet Of Things Wiki*. [online] Available at: http://internetofthingswiki.com/nest-learning-thermostat/559/ [Accessed 27 Jun. 2018].

[26]Νέα, κατάλογος για Αλληλέγγυα, Κοινωνική Οικονομία enallaktikos.gr. (2018). *Η Χαλκίδα θα γίνει η πρώτη 'έξυπνη' πόλη στην Ελλάδα*. [online] Available at: http://www.enallaktikos.gr/ar29533el-i-xalkida-tha-ginei-i-prwti-eksypni-poli-stin-ellada.html [Accessed 27 Jun. 2018].

[27]The Globe and Mail. (2018). *Eight ways the Internet of Things will change the way we live and work*. [online] Available at: https://www.theglobeandmail.com/report-on-business/rob-magazine/the-future-is-smart/article24586994/ [Accessed 27 Jun. 2018].