Τμήμα Μηχανικών Πληροφορικής τ.ε.
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Ελλάδας

Το Διαδίκτυο των Πραγμάτων

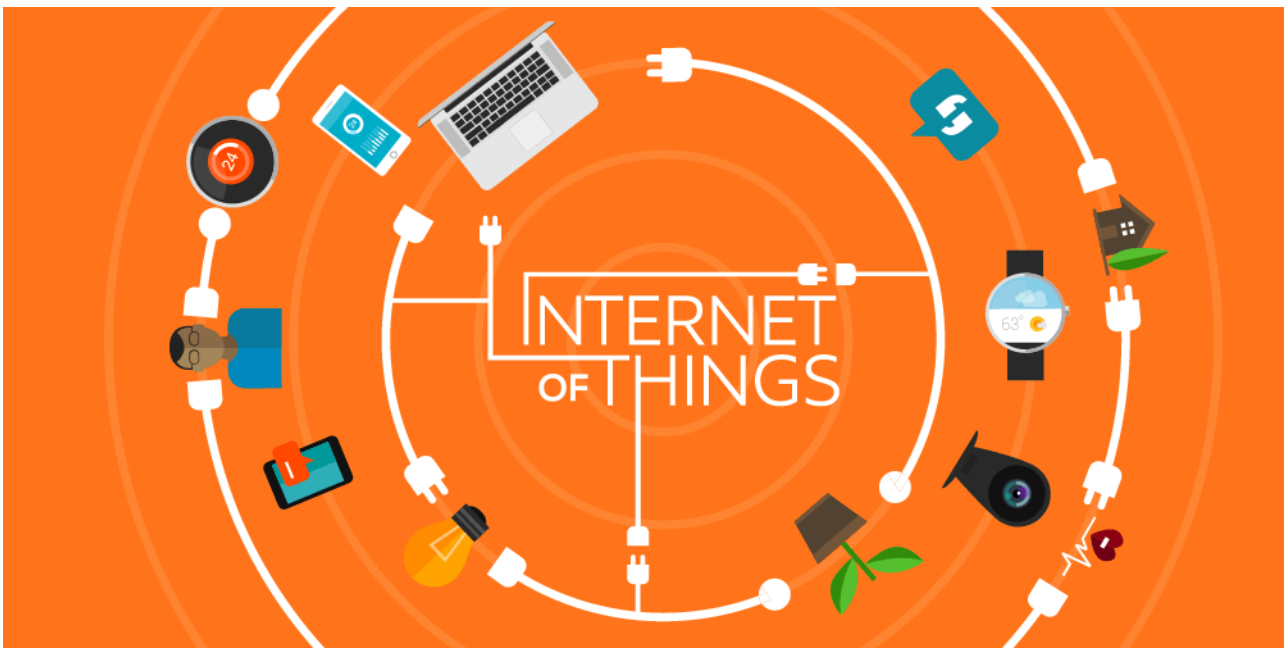
(Internet of Things – IoT)

και οι εφαρμογές του

Θεοδωρακόπουλος Λεωνίδας 0983

Καγκάνης Αθανάσιος 1139

Επιβλέπων: Τζήμας Ιωάννης



Αντίρριο 2016

Περιεχόμενα

ΠΕΡΙΛΗΨΗ

Το *Διαδίκτυο των Πραγμάτων*, ή Internet of Things (που θα αναφέρεται IoT στο εξής για συντομία) είναι η τελευταία καινοτομία στον τομέα της πληροφορικής και χρίζει μεγάλης κοινωνικής και οικονομικής σημασίας. Τα καταναλωτικά προϊόντα, τα μέσα μεταφοράς, βιομηχανικά και βοηθητικά εξαρτήματα, οι αισθητήρες και άλλα καθημερινά αντικείμενα συνδέονται μεταξύ τους μέσω του διαδικτύου και υπόσχονται να μετατρέψουν τον τρόπο εργασίας μας αλλά και την καθημερινή μας ζωή. Οι προβλέψεις για τον αντίκτυπο του IoT στο Διαδίκτυο και στην οικονομία είναι εντυπωσιακές. Κάποιες από αυτές τις προβλέψεις εικάζουν πως θα μπορούν να συνδεθούν στο μέλλον έως 100 δισεκατομμύρια συσκευές μεταξύ τους και αυτό, ουσιαστικά, θα σημαίνει μία παγκόσμια οικονομική επίπτωση πάνω από $11 τρισεκατομμύρια μέχρι το 2025.

Την ίδια στιγμή ωστόσο, το IoT δημιουργεί σημαντικές προκλήσεις, που θα μπορούσαν να σταθούν εμπόδιο στο δρόμο της κατάκτησης των δυνητικών οφελών. Αυτό που μέχρι στιγμής προσελκύει την προσοχή των εφημερίδων σχετίζεται με την πειρατεία στο Διαδίκτυο και τις συσκευές παρακολούθησης. Οι ανησυχίες και οι φόβοι περί απορρήτου έχουν επίσης προσελκύσει τη δημόσια προσοχή, δηλαδή την προσοχή των απλών χρηστών του Διαδικτύου.

Αυτή η επισκόπηση του εγγράφου είναι σχεδιασμένη για να βοηθήσει την κοινωνία του Διαδικτύου και της κοινότητας του Internet και να δει τα πράγματα υπό το πρίσμα των ανταγωνιστικών προβλέψεων σχετικά με τις υποσχέσεις και τους κινδύνους του IoT. Το IoT εμπλέκει μια ευρεία δέσμη ιδεών που είναι πολύπλοκη και διασταυρώνεται από διαφορετικές προοπτικές. Βασικές έννοιες που χρησιμεύουν ως βάση για να διερευνηθούν οι ευκαιρίες και οι προκλήσεις του IoT είναι οι εξής:

Ορισμός του IoT:

Ο όρος IoT γενικά αναφέρεται σε σενάρια όπου η συνδεσιμότητα του δικτύου και η υπολογιστική δυνατότητα επεκτείνεται σε αντικείμενα, αισθητήρες, καθημερινά

αντικείμενα που κανονικά δεν θεωρούνται υπολογιστές, επιτρέποντας σε αυτές τις συσκευές την παραγωγή, ανταλλαγή και κατανάλωση δεδομένων με ελάχιστη ανθρώπινη παρέμβαση. Δεν υπάρχει ωστόσο κάποιος κατοχυρωμένος παγκόσμιος ορισμός.

Enabling Technologies:

Η έννοια των διασυνδεδεμένων υπολογιστών, των αισθητήρων και των δίκτυον για την παρακολούθηση και τον έλεγχο των συσκευών υπάρχει εδώ και δεκαετίες. Ωστόσο οι πρόσφατες τεχνολογικές τάσεις της αγοράς φέρνουν το IoT όλο πιο κοντά στην ευρέως διαδεδομένη πραγματικότητα. Αυτές περιλαμβάνουν συνδεσιμότητα παντού, ευρεία υιοθέτηση AIX Networking, υπολογιστική οικονομία, πρόοδο στην ανάλυση δεδομένων (Data Analytics), και την αύξηση του cloud computing.

Connectivity Models:

Οι υλοποιήσεις του IoT χρησιμοποιούν διαφορετικές τεχνικές μοντέλων επικοινωνίας, το καθένα με τα δικά του χαρακτηριστικά. Τέσσερις κοινές επικοινωνίες των μοντέλων που περιγράφονται από την Επιτροπή Αρχιτεκτονικής Διαδικτύου περιλαμβάνουν: Συσκευή προς συσκευή, συσκευή προς cloud, Device to Gateaway και Back-End Data-Sharing. Αυτά τα μοντέλα υπογραμμίζουν την άνεση των συσκευών του IoT που μπορούν να συνδεθούν μεταξύ τους και να προσφέρουν τις υπηρεσίες τους στον χρήστη

Transformational Potential:

Εάν οι προβλέψεις και οι τάσεις του IoT γίνουν πραγματικότητα, μπορεί να πραγματοποιηθεί μια αλλαγή στον τρόπο σκέψης για τις συνέπειες και τα προβλήματα σε ένα κόσμο όπου η πιο κοινή αλληλεπίδραση με το Διαδίκτυο θα προέρχεται παθητικά με την εμπλοκή των συνδεδεμένων αντικειμένων αντί για ενεργή εμπλοκή με το περιεχόμενο. Οι πιθανές δυνατότητες υλοποίησης αυτού θα μπορέσουν να έχουν ως αποτέλεσμα αυτό που ονομάζουμαι ως “hyper connected world”.

Μερικά βασικά προβλήματα που προκύπτουν από το IoT είναι το να καταφέρουμε να εξερευνήσουμε κάποιες από τις πιεστικές προκλήσεις αλλά και ερωτήματα που

προκύπτουν σχετικά με αυτό. Αυτά περιλαμβάνουν Security, privacy, interoperability and standards.

Security:

Παρόλο που ο τομέας της ασφάλειας δεν είναι κάτι καινούριο για τον τομέα της πληροφορικής, τα χαρακτηριστικά του IoT δημιουργούν νέες και μοναδικές προκλήσεις στον τομέα της ασφαλείας. Η αντιμετώπιση αυτών των προκλήσεων και η εξασφάλιση της ασφάλειας των έξυπνων προϊόντων και υπηρεσιών, οφείλουν να αποτελέσουν θεμελιώδη προτεραιότητα. Οι χρήστες χρειάζεται να εμπιστευτούν πως οι έξυπνες συσκευές και οι συναφείς υπηρεσίες δεδομένων είναι ασφαλής και δεν έχουν τρωτά σημεία, καθώς η τεχνολογία του IoT σκοπεύει να διυσδήσει και να ενσωματωθεί στην καθημερινή μας ζωή. Συσκευές αλλα και υπηρεσίες με χαμηλή ασφάλεια μπορούν να αποτελέσουν πιθανά σημεία για cyber attacks και να εκθέσουν τα δεδομένα του χρήστη προς πιθανή κλοπή, αφήνοντας τις ροές δεδομένων ανεπαρκώς προστατευμένες.

Αν οι έξυπνες συσκευές που συνδέονται μέσω του IoT διαθέτουν χαμηλά επίπεδα ασφαλείας και είναι συνδεδεμένες online,επηρεάζουν την ασφάλεια αλλα και την αντοχή του Διαδικτύου παγκοσμίως. Η πρόκληση αυτή ενισχύεται και από άλλους παράγοντες όπως η μαζική κλίμακα ανάπτυξης ομοιογενών IoT συσκευών ώπου ορισμένες από αυτές, έχουν την δυνατότητα να συνδέονται αυτόματα με άλλες συσκευές. Αυτό αυξάνει τις πιθανότητες οι συσκευές αυτές να συνδεθούν σε μη ασφαλή περιβάλλοντα.

Ως θέμα αρχής, οι προγραμματιστές αλλα και οι χρήστες των έξυπνων συσκευών οφείλουν να έχουν την υποχρέωση να διαβεβαιώσουν πως δεν θα εκθέσουν τους χρήστες αλλα και το ίδιο το διαδίκτυο σε πιθανή ζημιά. Κατά συνέπεια, η συνεργατική προσέγγιση για την ασφάλεια, θα πρέπει να αναπτύξει αποτελεσματικές και κατάλληλες λύσεις σχετικά με τις προκλήσεις των θεμάτων ασφαλείας του IoT που να είναι κατάλληλες αναλόγως την κλίμακα και την πολυπλοκότητα των θεμάτων

Privacy:

Η υλοποίηση των πλήρων προοπτικών του IoT εξαρτάται από στρατηγικές που αφορούν τις ατομικές επιλογές απορρήτου σε ένα ευρύ φάσμα προσδοκιών. Οι ροές δεδομένων του χρήστη και η εξειδίκευση που του παρέχουν οι έξυπνες συσκευές μπορούν να βελτιώσουν την ζωή του, όμως οι ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής αλλά και των πιθανών ζημιών αποτελούν εμπόδιο για την πλήρη αξιοποίηση του IoT. Αυτό σημαίνει ότι το δικαίωμα της ιδιωτικής ζωής και ο σεβασμός προς τα δεδομένα του χρήστη πρέπει να αποτελεί δεδομένο ώστε να κερδίσει την εμπιστοσύνη του χρήστη αλλά και την εμπιστοσύνη του στο Διαδίκτυο, τις συνδεδεμένες συσκευές και τις συναφείς υπηρεσίες.

Πράγματι, το IoT επαναπροσδιορίζει τη συζήτηση σχετικά με τα θέματα απορρήτου, όπως και πολλές υλοποιήσεις σχετικά με την δραματική αλλαγή του τρόπου περισυλλογής των προσωπικών δεδομένων, ανάλυσης, χρησιμοποίησης αλλά και προστασίας. Για παράδειγμα, το IoT ενισχύει τις ανησυχίες για το ενδεχόμενο αύξησης επιτήρησης και παρακολούθησης, τις δυσκολίες στο να μπορέσουμε να επιλέξουμε ορισμένες συλλογές δεδομένων, καθώς και η αντοχή της άθροισης των ροών δεδομένων αποσκοπώντας στη ψηφιακή δημιουργία πορτραίτων των χρηστών. Προκειμένου να αντιληφθούμε τις ευκαιρίες που μας δίνει το IoT, πρέπει να αναπτυχθούν στρατηγικές οι οποίες να σέβονται τις προσωπικές επιλογές στο φάσμα των προσδοκιών, καθώς και να παραμείνει η προώθηση της καινοτομίας στους τομείς των νέων τεχνολογιών αλλά και υπηρεσιών

Interoperability / Standards:

Ένα κατακερματισμένο περιβάλλον των αποκλειστικών τεχνικών που προσφέρει το IoT πιθανόν να προβληματίσει τους χρήστες αλλά και τη βιομηχανία. Καθώς η πλήρης διαλειτουργικότητα μεταξύ προϊόντων και υπηρεσιών δεν είναι πάντα εφικτή και αναγκαία, οι αγοραστές μπορούν να διστάσουν να αγοράσουν έξυπνες συσκευές, προϊόντα και υπηρεσίες, λόγο αυτού μπορεί να υπάρξει υψηλή κυριότητα πολυπλοκότητας αλλά και ανησυχία για τον προμηθευτή.

Επιπλέον, οι ελλιπώς σχεδιασμένες έξυπνες συσκευές μπορεί να έχουν αρνητικές συνέπειες για τη δικτύωση των πόρων όταν συνδεθούν και αποκτήσουν ευρύτερη

πρόσβαση. Τα κατάλληλα πρότυπα, μοντέλα αναφοράς και οι βέλτιστες πρακτικές θα πρέπει να συμβάλουν στην αναχαίτιση της εξάπλωσης των συσκευών που μπορούν να προκαλέσουν αναστάτωση μέσα στο Internet. Η χρήση των φαρμάκων κοινόχρηστης ονομασίας αλλά και τα ευρέως διαθέσιμα πρότυπα ως τεχνική οικοδομικών τετράγωνων για τις έξυπνες συσκευές και υπηρεσίες (όπως το πρωτόκολλο Internet) θα στηρίξουν την μεγαλύτερη ωφελιμότητα του χρήστη, την καινοτομία και την οικονομική ευκαιρία

ΕΙΣΑΓΩΓΗ

Το Internet of Things (με συντομογραφία IoT), μπορεί κάλλιστα να χαρακτηριστεί ως το Διαδίκτυο του Μέλλοντος (Future Internet). Από τα πρώτα κιόλας χρόνια της επιτυχημένης μεταφοράς δεδομένων μεταξύ δύο υπολογιστών που βρίσκονταν σε διαφορετικά μέρη, η άμεση εξέλιξη των πραγμάτων όριζε πως η δικτύωση όλων των υπολογιστών πρέπει να πάει σε ένα κοινό Δίκτυο. Η ιδέα αυτή όσον αφορά τη δικτύωση των προσωπικών υπολογιστών και των υπολογιστικών συστημάτων έχει τεθεί σε εφαρμογή με το γνωστό σε όλους μας Διαδίκτυο (Internet), το οποίο στην πραγματικότητα είναι η σύνδεση πολλών δικτύων υπολογιστών μεταξύ τους.

Η όλο και αυξανόμενη αναγκαιότητα επέκτασης της υπάρχουσας δικτύωσης υπολογιστών αποσκοπεί στο να βελτιώσει και να κάνει αποδοτικότερες τις υπηρεσίες του Διαδικτύου, με βάση την ανάπτυξη συστημάτων και τη δημιουργία πρωτοκόλλων που να είναι σε θέση να υλοποιήσουν μια νέα βελτιωμένη μετεξέλιξη αυτού που αποκαλούμε σήμερα Διαδίκτυο. Στην πραγματικότητα ο στόχος είναι η διασύνδεση όλων των καθημερινών οικιακών ηλεκτρονικών συσκευών, όπως για παράδειγμα το ψυγείο, το αμάξι, η κουζίνα, σε ένα ευρύτερο δίκτυο, που για λόγους συνήθειας θα συνεχίσουμε να το αποκαλούμε Διαδίκτυο και στην συνέχεια της πτυχιακής μας εργασίας. Επιπρόσθετα, το IoT μπορούμε να το ορίσουμε και ως την αυγή μιας νέας εποχής για την τεχνολογία των επικοινωνιών και της πληροφορίας, όπου σε οποιαδήποτε χρονική στιγμή, σε οποιαδήποτε τοποθεσία και από τον κάθε χρήστη θα έχει τη δυνατότητα για επικοινωνία και σύνδεση στο Διαδίκτυο.

Η εξέλιξη αυτή του Διαδικτύου μπορεί υποστηρίζει και άλλου είδους συσκευές, πέραν των υπολογιστών, με βάση τεχνολογικών μέσων, όπως παραδείγματος χάριν η ηλεκτρονική ετικέτα (electronic tag), αποκαλούμενη και ως RFIDs (Radio Frequency IDentification), σε αισθητήρες ανίχνευσης (sensors) ή και τερματικά που μεταδίδουν φωνή με χρήση του πρωτοκόλλου IP (wireless VoIP (Voice over Internet Protocol) terminals). Τα προαναφερθέντα αντικείμενα είναι χαμηλού κόστους και η παρασκευή τους είναι ευρεία, λόγω αυτών τον γεγονότων μπορούν να τοποθετηθούν εύκολα σε κάθε συσκευή. Η χρήση και διασύνδεση όλων των υπολογιστών στο

διαδίκτυο, δε θα θεωρούνταν λανθασμένο να χαρακτηριστεί, ως μια νέα τεχνολογική επανάσταση, η οποία διαθέτει αρκετά κοινά με αυτήν που υπήρξε με το Διαδίκτυο στις αρχές της δεκαετίες του 90. Σαφώς ένα από τα άμεσα ερωτήματα που προκύπτουν είναι η επίτευξή της επικοινωνίας μεταξύ ηλεκτρονικών συσκευών, από την στιγμή που αρκετές ηλεκτρονικές συσκευές που χρησιμοποιούνται τη συγκεκριμένη χρονική περίοδο, στερούνται τη δυνατότητα σύνδεσης στο Διαδίκτυο. Θεωρητικά η απάντηση είναι προφανής, πρακτικά όμως είναι αρκετά δύσκολο να υλοποιηθεί, διότι χρειάζεται η δημιουργία μιας νέας αρχιτεκτονικής στην οποία τα αντικείμενα να αποκτούν την απαραίτητη «νοημοσύνη» για την δυνατότητα της επικοινωνίας, όπως θα εξηγηθεί και στη συνέχεια.

Συμπερασματικά, πρέπει να τονιστεί ότι η υλοποίηση του IoT, με τη δημιουργία των απαραιτήτων πρωτοκόλλων και αρχιτεκτονικών είναι ακόμη σε πρώιμα στάδια. Παρόλα αυτά δεν έχει βρεθεί κάποια κοινά αποδεκτή λύση από την παγκόσμια κοινότητα. Στη συνέχεια αναφέρονται οι τελευταίες τεχνολογικές εξελίξεις, η θεωρητική προσέγγιση του IoT, τα βασικά στοιχεία που το αποτελούν, όπως επίσης και οι απαραίτητες λειτουργίες για την επίτευξη της ιδέας της δικτύωσης όλων των πραγμάτων στο Διαδίκτυο. Ακόμη αναφέρονται μερικά προβλήματα που παρουσιάζονται στην ανάπτυξη και στη χρήση της νέας τεχνολογίας, καθώς και οι λύσεις που έχουν εντοπιστεί. Επιπροσθέτως αναφέρονται οι κίνδυνοι και τα οφέλη από τη χρήση του IoT όπως και παραδείγματα εφαρμογών που σχετίζονται άμεσα με τη χρήση του.

ΚΕΦΑΛΑΙΟ 1

ΤΙ ΕΙΝΑΙ ΤΟ IoT

Προέλευση, κινητήριες δυνάμεις και εφαρμογές

Ο όρος “IoT” (IoT) χρησιμοποιήθηκε πρώτη φορά το 1999 από τον Βρετανό πρωτοπόρο στον τομέα της τεχνολογίας Kevin Άστον. Ο Kevin Άστον περιέγραψε ένα σύστημα στο οποίο τα αντικείμενα στο φυσικό κόσμο θα μπορούσαν να συνδεθούν με το Διαδίκτυο μέσω αισθητήρων. Ο Ashton επισήμανε πως οι RFID αισθητήρες μπορούν να χρησιμοποιηθούν σε εταιρίες εφοδιασμού στο Internet προκειμένου να μπορούμε να υπολογίσουμε τα αγαθά χωρίς την ανάγκη για ανθρώπινη παρέμβαση. Σήμερα, το IoT έχει γίνει ένας πολύ δημοφιλής όρος για την περιγραφή των σεναρίων που η συνδεσιμότητα στο Internet και η υπολογιστική δυνατότητα μπορεί να επεκταθεί σε μια ποικιλία πραγμάτων, δηλαδή αισθητήρων, συσκευών και άλλων δικτυωμένων αντικείμενων.

Ενώ το "IoT" αποτελεί ένα σχετικά νέο όρο, η έννοια του συνδυασμού υπολογιστών και δικτύων για τον έλεγχο των συσκευών και την παρακολούθηση έχει υπάρξει εδώ και δεκαετίες. Για παράδειγμα από τα τέλη της δεκαετίας του '70, τα συστήματα για την εξ αποστάσεως παρακολούθηση στο ηλεκτρικό δίκτυο μέσω τηλεφωνικών γραμμών ήταν ήδη σε χρήση. Η πρώτη απόπειρα κατασκευής μιας συσκευής IoT αποτελούσε μια μηχανή κοκτέιλ πεπόνι στο Πανεπιστήμιο Carnegie στις αρχές του 1980. Οι προγραμματιστές μπορούσαν να συνδεθούν στο μηχάνημα μέσω του Διαδικτύου και να ελέγχουν την κατάσταση του μηχανήματος και να καθορίσουν το κατά πόσον θα υπάρξει ένα κρύο ποτό αν ήθελαν να πιούν ένα.

Στη δεκαετία του '90, οι εξελίξεις στην ασύρματη τεχνολογία "machine to machine" (M2M) έδωσαν λύσεις στις επιχειρήσεις και στις βιομηχανίες για τον εξοπλισμό παρακολούθησης. Πολλές από αυτές τις λύσεις M2M, βασίζονται σε “κλειστής” κατασκευής ιδιόκτητα δίκτυα ή άλλων ειδικών προδιαγραφών αντί για το Internet Protocol (IP) που βασίζεται στα πρότυπα του Διαδικτύου.

Δεν είναι κάτι καινούργιο το να συνδέσουμε μέσω του πρωτοκόλλου IP συσκευές,

εκτός των υπολογιστών, με το Internet. Η πρώτη "έξυπνη συσκευή" ήταν μια IP enabled φρυγανιέρα που μπορούσε να απενεργοποιηθεί και να ενεργοποιηθεί μέσω του Διαδικτύου η οποία ήταν διαθέσιμη στο Internet Convection το 1990. Με την πάροδο του χρόνου, δημιουργήθηκαν και άλλα "έξυπνα πράγματα" που ήταν IP-Enabled, συμπεριλαμβανομένου και του ανθρακικού μηχανήματος στο Πανεπιστήμιο Carnegie Mellon των ΗΠΑ αλλα και μίας καφετιέρας στο Trojan room του Πανεπιστημίου του Cambridge, στο Ηνωμένο Βασίλειο (το οποίο αξίζει να σημειωθεί πως παρέμεινε συνδεδεμένο στο Internet μέχρι το 2001). Έτσι λοιπόν, μέσω αυτού του ξεκινήματος, δόθηκε το έναυσμα στον τομέα της έρευνας και της ανάπτυξης σε "smart object networking" τα οποία βοήθησαν στη δημιουργία αυτού που γνωρίζουμε σήμερα ως *IoT*

Από τη στιγμή που η ιδέα σύνδεσης των αντικειμένων με το Διαδίκτυο δεν είναι κάτι καινούργιο, αποτελεί εύλογο ερώτημα το "Γιατί το IoT είναι ένα τόσο δημοφιλές θέμα σήμερα;". Από μια ευρύτερη προοπτική, η συμβολή αρκετών τεχνολογιών και τάσεων της αγοράς προσφέρουν τη δυνατότητα για να διασυνδεθούν περισσότερες και μικρότερες έξυπνες συσκευές, εύκολα και φθηνά:

- *Απεριόριστες δυνατότητες σύνδεσης*, υψηλής ταχύτητας και χαμηλού κόστους, διάχυτη συνδεσιμότητα δικτύου, ιδίως μέσω των ασύρματων υπηρεσιών και τεχνολογιών, που έχουν τη δυνατότητα να κάνουν σχεδόν τα πάντα "συνδεθούν".

- *Ευρεία υιοθέτηση IP networking*. Το IP (Internet Protocol) έχει γίνει το κυρίαρχο παγκόσμιο πρότυπο για τη δικτύωση, παρέχοντας μια καλά καθορισμένη πλατφόρμα λογισμικού και εργαλεία έτσι ώστε να μπορεί να ενσωματωθεί σε ένα ευρύ φάσμα συσκευών οικονομικά και εύκολα.

- *Υπολογιστική οικονομία,* όπως, για παράδειγμα, τη βιομηχανία επενδύσεων στον τομέα της έρευνας, της ανάπτυξης και της κατασκευής, Ο νόμος του Moore συνεχίζει να αποδίδει μεγαλύτερη υπολογιστική ισχύ σε χαμηλότερες τιμές και με χαμηλότερη κατανάλωση ρεύματος.

- *Miniaturization,* δηλαδή κατασκευαστικές εξελίξεις που επιτρέπουν μέσω της τελευταίας τεχνολογίας της πληροφορικής και των επικοινωνιών να

ενσωματωθούν σε πολύ μικρά αντικείμενα, σε συνδυασμό με την μεγαλύτερη υπολογιστική οικονομία. Έχει καταφερθεί η κατασκευή πολλών μικρών και ανέξοδων αισθητήρων για την ερφαρμογή τους σε έξυπνες συσκευές.

- Πλεονεκτήματα *στην ανάλυση δεδομένων,* δηλαδή Δημιουργία νέων αλγορίθμων και ταχεία αύξηση της υπολογιστικής ισχύος, αποθήκευσης δεδομένων και υπηρεσιών cloud με σκοπό την ομαδοποίηση, τη συσχέτιση και ανάλυση των τεράστιων ποσοτήτων δεδομένων, εκ των οποίων μας δίνετε η δυνατότητα νέων ευκαιριών για την εξαγωγή πληροφοριών και γνώσεων.

- *Εξάπλωση του Cloud Computing*, το οποίο μπορεί να μας δώσει τη δυνατότητα για μια απομακρυσμένη διαχείριση δικτυωμένων πόρων για την επεξεργασία, κατανομή και αποθήκευση δεδομένων. Επίσης επιτρέπει σε μικρές συσκευές διανομής να χρησιμοποιούν ισχυρές back-end analytics και δυνατότητες ελέγχου.

Βάση λοιπόν αυτών των προοπτικών ανάπτυξης, το IoT αντιπροσωπεύει τη συνεργασία μιας ποικιλίας υπολογιστικών συστημάτων και τις δυνατότητες εξέλιξης που έχουν στο μέλλον. Σήμερα, ένα ευρύ φάσμα του τομέα της βιομηχανίας, συμπεριλαμβανομένης της αυτοκινητοβιομηχανίας, της υγείας, της κατασκευής ηλεκτρονικών ειδών, εξετάζουν το ενδεχόμενο ενσωμάτωσης της τεχνολογίας του IoT σε προϊόντα, δραστηριότητες και υπηρεσίες τους.

Στην έκθεση "Αξιοποίηση των δυνατοτήτων του IoT", το McKinsey Global Institute περιγράφει το ευρύ φάσμα των δυνητικών εφαρμογών όπου το IoT αναμένεται να ωφελήσει τους χρήστες αλλά και τη βιομηχανία.

Ρυθμίσεις	**Περιγραφές**	**Παραδείγματα**
Άνθρωποι	Συσκευές προσκολλημένες ή εσωτερικά στο ανθρώπινο σώμα	Συσκευές για την παρακολούθηση (φορητές ή ενσωματωμένες στο ανθρώπινο σώμα) και συντήρηση της ανθρώπινης υγείας όπως διαχείριση ασθενειών, αυξημένη ευεξία και υψηλότερη παραγωγικότητα
Σπίτια	Κτήρια όπου ζουν άνθρωποι	Συστήματα ελέγχου σπιτιού και συστήματα ασφαλείας
Καταστήματα	Μέρη στα οποία οι σε καταναλωτές έρχονται επαφή με το εμπόριο	Καταστήματα, τράπεζες, εστιατόρια, Στάδια Και γενικότερα οπουδήποτε μπορεί ένας καταναλωτής να αγοράσει αγαθά, ενημερώσεις προσφορών εντός του καταστήματος, βελτιστοποίηση στην καταγραφή εμπορευμάτων
Γραφεία	Μέρη στα οποία ειδικευόμενοι υπάλληλοι εργάζονται.	Διαχείριση ενέργειας και ασφαλείας των κτηρίων που στεγάζονται τα γραφεία. Βελτιωμένη παραγωγικότητα περιλαμβανομένου και τους κινούμενους εργαζομένους (mobile employees)

Εργοστάσια	Συγκεκριμένα περιβάλλοντα παραγωγής.	Μέρη με καθημερινή ρουτίνα εργασίας περιλαμβανομένου νοσοκομεία και φάρμες, λειτουργικές δραστηριότητες, βελτιωμένος εξοπλισμός χρήσης για την απογραφή εμπορευμάτων
Εργοτάξια	Ειδικά περιβάλλοντα παραγωγής.	Εξόρυξη, πετρέλαιο και αέριο, οικοδομές (κατασκευές)
Μέσα μεταφοράς	Συστήματα ενσωματωμένα σε οχήματα.	Οχήματα όπως αυτοκίνητα, φορτηγά, πλοία, αεροσκάφη και τρένα, Προϋποθέσεις που βασίζονται για την συντήρηση.
Πόλεις	Αστικά περιβάλλοντα.	Δημόσιοι χώροι και υποδομές σε αστικά περιβάλλοντα. Προσαρμοσμένος έλεγχος κυκλοφορίας, έξυπνοι μετρητές, παρακολούθηση περιβάλλοντος, διαχείριση πόρων.
Εξωτερικοί χώροι	Ανάμεσα σε αστικά περιβάλλοντα και διάφορες θέσεις εκτός αυτών.	Εξωτερική χρήση συμπεριλαμβανομένων σιδηροδρομικών γραμμών, Αυτόνομων μέσων μεταφοράς οχημάτων, πλοηγός αεροπλάνων, Διαδρομές σε πραγματικό χρόνο, συνδεδεμένες πλοηγήσεις, ανα πάσα στιγμή εντοπισμός της αποστολής.

Πολλοί οργανισμοί έχουν αναπτύξει ειδικούς τρόπους ταξινόμησης και κατηγοριοποίησης των εφαρμογών του IoT. Για παράδειγμα, το "βιομηχανικό IoT" είναι ένας όρος που χρησιμοποιείται ευρέως από τις επιχειρήσεις και τις ενώσεις όταν θέλουν να περιγράψουν τις εφαρμογές του IoT που σχετίζονται με την παραγωγή αγαθών και υπηρεσιών, περιλαμβανομένου της κατασκευής και της χρησιμότητας. Άλλοι εστιάζουν στον τύπο της συσκευής του IoT, όπως οι φορητές συσκευές και οι εφαρμογές. Άλλοι επικεντρώνονται στο γενικό πλαίσιο του IoT με βάση την τοποθεσία όπως τα "έξυπνα σπίτια" ή οι "έξυπνες πόλεις". Ανεξάρτητα από την εφαρμογή, είναι σαφές ότι η χρήση του IoT θα μπορούσε να επεκταθεί σε σχεδόν κάθε πτυχή της ζωής μας.

Καθώς ο αριθμός των συνδεδεμένων συσκευών αυξάνεται, το ποσό κυκλοφορίας που παράγεται αναμένεται να αυξηθεί εξίσου σημαντικά. Για παράδειγμα, η Cisco υπολογίζει ότι η χρήση του Internet που χρησιμοποιείται από λοιπές συσκευές πέραν των υπολογιστών θα αυξηθεί από το 40% που χρησιμοποιείται το 2014 στο 70% το 2019. Η Cisco προβλέπει επίσης ότι ο αριθμός των "Machine to Machine " ("M2M") συνδέσεων (συμπεριλαμβανομένης της βιομηχανικής, του σπιτιού, της υγείας, των αυτοκινήτων, κλπ) θα αυξηθούν από 24% σε 43% έως το 2019.

Μία συνέπεια αυτών των τάσεων είναι ότι τα επόμενα δέκα χρόνια θα μπορέσουμε να δούμε μια μετατόπιση στην δημοφιλή αντίληψη του τι σημαίνει "να είσαι στο Διαδίκτυο" δηλαδή να είσαι online.

Ο Παγκόσμιος Ιστός (World Wide Web – WWW) έχει γίνει σχεδόν συνώνυμο με το ίδιο το Internet. Οι Τεχνολογίες Web πλέον διευκολύνουν την αλληλεπίδραση μεταξύ των ανθρώπων και του περιεχομένου του, καθιστώντας ένα ξεκάθαρο χαρακτηριστικό της τρέχουσας εμπειρίας της χρήσης του Διαδικτύου. Η διαδικτυακή εμπειρία σε μεγάλο βαθμό χαρακτηρίζεται από την ενεργή συμμετοχή των χρηστών στο κατέβασμα δεδομένων και στη δημιουργία περιεχομένου μέσω των υπολογιστών και των smartphones. Εάν τα σχέδια ανάπτυξης για το IoT γίνουν πραγματικότητα, θα μπορέσουμε να δούμε μια περισσότερο παθητική στάση των χρηστών με τα αντικείμενα και τις συσκευές όπως τα εξαρτήματα των αυτοκινήτων, οι οικιακές συσκευές και οι συσκευές παρακολούθησης. Αυτές οι συσκευές εκπέμπουν και λαμβάνουν δεδομένα του χρήστη κατ εντολήν του, με μικρή

ανθρώπινη παρέμβαση.

Το IoT μπορεί να πραγματοποιήσει αλλαγή στον τρόπο σκέψης, αν αναλογιστεί κανείς πως η πιο κοινή αλληλεπίδραση με το Διαδίκτυο προέρχεται παθητικά στην εμπλοκή με τα συνδεδεμένα αντικείμενα στο ευρύτερο περιβάλλον. Οι δυνατότητες υλοποίησης αυτής της έκβασης "hyperconnected world" αποτελούν το γενικό χαρακτήρα της αρχιτεκτονικής του IoT, η οποία δεν πραγματοποιεί περιορισμούς στις εφαρμογές ή τις υπηρεσίες που μπορούν να κάνουν μέσω αυτής.

Διαφορετικοί ορισμοί, παρόμοιες έννοιες

Παρά την παγκόσμια ερμηνεία γύρω από το IoT, δεν υπάρχει συγκεκριμένος αποδεκτός ορισμός περί αυτού. Χρησιμοποιούνται πολλοί ορισμοί από διάφορες ομάδες για να περιγράψουν ή να προωθήσουν μια συγκεκριμένη άποψη για το τι σημαίνει το IoT και ποια είναι τα σημαντικά χαρακτηριστικά του. Μερικοί ορισμοί προσδιορίζουν την έννοια του Διαδικτύου ή του πρωτοκόλλου Internet (IP), ενώ άλλοι όχι. Για παράδειγμα δίνονται οι παρακάτω ορισμοί:

Η Επιτροπή Αρχιτεκτονικής Διαδικτύου (IAB) ξεκινά το RFC 7452 με θέμα «Τα αρχιτεκτονικά θέματα Smart Object Networking», με την παρακάτω περιγραφή:

Ο όρος "IoT" υποδηλώνει ένα γράφημα, όπου ένας μεγάλος αριθμός από ενσωματωμένες συσκευές χρησιμοποιούν τις υπηρεσίες τους επικοινωνώντας με τα πρωτόκολλα που προσφέρει το Διαδίκτυο. Πολλές από αυτές τις συσκευές, που συχνά ονομάζονται "έξυπνα αντικείμενα", δεν χειρίζονται άμεσα από τον άνθρωπο, αλλά υφίστανται ως εξαρτήματα σε κτίρια και αυτοκίνητα, ή είναι διάσπαρτα στο περιβάλλον.

Στο Internet Engineering Task Force (IETF), ο όρος "Smart Object Networking" χρησιμοποιείται συνήθως όταν αναφερόμαστε στο IoT. Σε αυτό το πλαίσιο, τα «έξυπνα αντικείμενα» είναι συσκευές που συνήθως έχουν σημαντικούς περιορισμούς, περιορισμένη ισχύ, μνήμη και επεξεργασία των πόρων ή το εύρος ζώνης. Οι εργασίες στην IETF οργανώνονται γύρω από ειδικές απαιτήσεις για να επιτευχθεί η διαλειτουργικότητα των δικτύων μεταξύ διαφόρων τύπων έξυπνων αντικειμένων.

Το 2012 δημοσιεύθηκε από την Διεθνή Ένωση Τηλεπικοινωνιών (ITU) ITU-T Recommendation Y. 2060, *επισκόπηση του IoT*, η οποία πραγματεύεται την έννοια της διασυνδεσιμότητας, αλλά δεν ενσωματώνει το IoT στο Διαδίκτυο:

IoT: μια παγκόσμια υποδομή για την κοινωνία των πληροφοριών, παρέχοντας προηγμένες υπηρεσίες μέσω διασυνδεδεμένων (φυσικών και εικονικών) συσκευών ("πράγματα") που βασίζονται στις υφιστάμενες και εξελισσόμενες διαλειτουργικές τεχνολογίες πληροφόρησης και επικοινωνίας.

Σημείωση 1. Αξιοποιώντας την αναγνώριση, συλλογή δεδομένων, την επεξεργασία και τις δυνατότητες επικοινωνίας, το IoT κάνει πλήρη χρήση των δυνατοτήτων του με σκοπό να προσφέρει υπηρεσίες σε όλα τα είδη των εφαρμογών, διασφαλίζοντας την ασφάλεια και η ιδιωτικότητα.

Σημείωση 2. Από μια ευρύτερη προοπτική, το IoT μπορεί να εκληφθεί ως ένα όραμα με τεχνολογικές και κοινωνικές επιπτώσεις.

Βάση του προαναφερθέντος ορισμού, το IEEE Communications Magazine συνδέει το IoT με τις cloud υπηρεσίες:

Το IoT είναι ένα πλαίσιο στο οποίο όλα τα πράγματα έχουν εκπροσώπηση και παρουσία στο Διαδίκτυο. Πιο συγκεκριμένα, το IoT στοχεύει στο να προσφέρουν νέες εφαρμογές και υπηρεσίες με σκοπό τη γεφύρωση των φυσικών και εικονικών κόσμων, στις οποίες ο τρόπος το M2M αντιπροσωπεύει τη γραμμή επικοινωνίας που επιτρέπει την αλληλεπίδραση μεταξύ των πραγμάτων και εφαρμογών σε cloud επίδεδο.

Τα λεξικά Oxford προσφέρουν έναν πιο περιεκτικό ορισμό που επικαλείται το Διαδίκτυο ως στοιχείο του IoT:

Το IoT (ουσιαστικό): η διασύνδεση μέσω του Διαδικτύου υπολογιστικών συσκευών είναι ενσωματωμένη σε καθημερινά αντικείμενα, παρέχοντάς τους τη δυνατότητα να στείλουν και να λάβουν δεδομένα.

Όλοι οι ορισμοί που περιγράφουν τα σενάρια στα οποία η συνδεσιμότητα δικτύου και η υπολογιστική δυνατότητα εκτείνεται σε πληθώρα αντικειμένων όπως

συσκευές, αισθητήρες, και καθημερινά αντικείμενα που κανονικά δεν θεωρούνται "υπολογιστές"· αυτό επιτρέπει στις συσκευές να παράγουν, να ανταλλάξουν, και να καταναλώνουν δεδομένα, συχνά με ελάχιστη ανθρώπινη παρέμβαση. Δεν είναι απαραίτητο να διαφωνούμε με τους διάφορους ορισμούς του IoT διότι μάλλον τονίζουν διαφορετικές πτυχές του φαινομένου από διαφορετικά σημεία εστίασης και περιπτώσεων χρήσης.

Ωστόσο, η ανομοιογένεια των ορισμών θα μπορούσε να είναι μια πηγή σύγχυσης στο διάλογο για θέματα IoT, ιδιαίτερα στις συζητήσεις μεταξύ των ενδιαφερομένων ομάδων ή σε τμήματα του κλάδου. Παρόμοια σύγχυση είχε συμβεί και πριν από μερικά χρόνια και για το ζήτημα του cloud computing, όπου διαφορετικές ερμηνείες και ορισμοί είχαν μερικές φορές αποτελέσει εμπόδιο στην επικοινωνία. Ενώ είναι μάλλον περιττό να αναπτυχτεί ένας ενιαίος ορισμός του IoT, καθώς πρέπει να αναγνωριστεί ότι υπάρχουν διαφορετικές προοπτικές περί του θέματος ώστε και αυτές να συμπεριληφθούν στις συζητήσεις.

Για τους σκοπούς της παρούσας πτυχιακής εργασίας, ο όρος “IoT” θα θεωρούμε πως δηλώνει τη συνδεσιμότητα του δικτύου και την υπολογιστική ικανότητα για αντικείμενα, συσκευές, αισθητήρες και στοιχεία που συνήθως δεν θεωρούνται υπολογιστές. Αυτά τα “έξυπνα αντικείμενα” απαιτούν ελάχιστη ανθρώπινη παρέμβαση για την παραγωγή, ανταλλαγή και κατανάλωση δεδομένων. Επίσης διαθέτουν συνδεσιμότητα για απομακρυσμένη συλλογή δεδομένων, ανάλυση, και δυνατότητες διαχείρισης.

Τα δικτυακά και επικοινωνιακά μοντέλα για έξυπνα αντικείμενα αποτελούνται απο εκείνα όπου ανταλλάσουν δεδομένα στο Διαδίκτυο ή σε ένα απλό IP δίκτυο. Αυτό περιλαμβάνει τα μοντέλα μιας ευρείας περιγραφής του “IoT” που χρησιμοποιούνται για αυτή τη πτυχιακή. Όπως είναι πιθανό τα δεδομένα που παράγονται ή μεταποιούνται από εκείνα τα έξυπνα αντικείμενα τελικά θα συνδεθούν μέσω δικτύων IP ή, διαφορετικά, θα πρέπει να ενσωματωθούν στο προϊόν που είναι προσβάσιμο μέσω του Διαδικτύου.

Αισθητήρες RFID

Η βασική τεχνολογία για τη υλοποίηση των έξυπνων συσκευών είναι οι αισθητήρες

RFID (RFID sensors). Η τεχνολογία RFID (Radio Frequency Identification) χρησιμοποιείται με σκοπό την αυτοματοποιημένη ανίχνευση πραγμάτων και ανθρώπων και αποτελεί μια μετεξέλιξη του κλασικού κώδικα (barcode). Μια συσκευή RFID επιπλέον ονομάζεται ετικέτα RFID (RFID tag). Αυτή είναι ένας μικροεπεξεργαστής ο οποίος έχει σχεδιαστεί για την μετάδοση δεδομένων ασύρματα. Η βασική λειτουργία του είναι να μεταδίδει δεδομένα σε τυχόν ερωτήσεις από μία συσκευή ανάγνωσης (RFID Reader). Τα είδη των ετικετών RFID είναι τρία και χωρίζονται σε δύο κατηγορίες αναλόγως με το αν έχουν μπαταρία σαν βασική πηγή ενέργειας.

Η πρώτη κατηγορία είναι οι παθητικές ετικέτες RFID (passive tags), οι οποίες διαθέτουν μικρό μέγεθος και επίσης χαμηλό κόστος. Δεν έχουν από τη κατασκευή τους κάποια συγκεκριμένη πηγή ενέργειας, αλλά παίρνουν την απαιτούμενη ενέργεια για την αποστολή δεδομένων από το λαμβανόμενο σήμα όπου στέλνετε από την συσκευή ανάγνωσης.

Η δεύτερη κατηγορία είναι οι ετικέτες ή οι αισθητήρες RFID που έχουν μπαταρίες. Αυτούς μπορούμε να τους χωρίσουμε σε δύο (2) υποκατηγορίες, τους ημι-παθητικούς αισθητήρες (semi-passive tags), οι οποίοι χρησιμοποιούν την ενέργεια από τη μπαταρία τους για την λειτουργία τους σε περίπτωση ερώτησης από τη συσκευή ανάγνωσης. Η άλλη υποκατηγορία είναι οι ενεργητικοί (active tags), οι οποίοι την ενέργεια από τη μπαταρία τους την χρησιμοποιούν για την αποστολή δεδομένων. Αξίζει να σημειωθεί ότι οι ενεργοί αισθητήρες RFID έχουν εμβέλεια μεγαλύτερη από εκατό μέτρα (100 m) και είναι πιο ακριβοί από τους υπόλοιπους αισθητήρες με τιμές μεγαλύτερες των είκοσι Ευρώ (20€). Τέλος παρακάτω εικονίζονται οι προαναφερόμενοι ανά κατηγορία RFID αισθητήρες

Δύο είναι τα κυρίως χαρακτηριστικά που καθιστούν τον αισθητήρα RFID κατάλληλο για την υλοποίηση του IoT. Πρώτον είναι το κόστος του RFID αισθητήρα το οποίο στη κύρια μορφή ενός barcode RFID είναι χαμηλότερο από 0.13 USD (δολλάρια Αμερικής). Δεύτερον και επίσης σημαντικό χαρακτηριστικό αποτελεί το μέγεθος του. Σημαντικό είναι να σημειωθεί ότι ο τύπος μ-RFID έχει μέγεθος 0.4x 0.4 χιλιοεκατοστών (mm) κάθιστώντας το κατάλληλο για την τοποθέτηση σε κάθε είδους αντικείμενο. Επίσης υπάρχουν δύο βασικές λειτουργίες

των αισθητήρων RFID που ενισχύουν την καταλληλότητα των αισθητήρων RFID για την σήμανση των πραγμάτων:

Μοναδικός τρόπος ανίχνευσης

Συγκριτικά με το κλασικό κώδικα barcode (γραμμωτό), ο αισθητήρας RFID πέραν από την δήλωση του τύπου του αντικειμένου, στέλνει ένα μοναδικό σειριακό αριθμό, ο οποίος διακρίνει το αντικείμενο μέσα από χιλιάδες πανομοιότυπα αντικείμενα. Επίσης με σκοπό την καλύτερη λειτουργία της αναγνώρισης, μπορεί να διαθέτει μια βάση δεδομένων ώστε να του παρέχει περισσότερες πληροφορίες για το κάθε ένα αντικείμενο.

Αυτοματοποίηση

Οι μέθοδοι ανίχνευσης που παραδοσιακά χρησιμοποιούνται (γραμμωτός κώδικας) απαιτείται να υπάρχει οπτική επαφή με τη συσκευή ανάγνωσης του barcode που είναι χαραγμένος στα αντικείμενα, καθώς επίσης και στις περισσότερες περιπτώσεις απαιτείται ανθρώπινη παρέμβαση. Στην RFID ετικέτα όμως, όλες οι ανιχνεύσεις αντικειμένων γίνονται αυτόματα. Ένα παράδειγμα της αυτοματοποίησης είναι μια συσκευή ανάγνωσης (barcode scanner) που μπορεί να σαρώνει εκατό (100) ετικέτες ανα δευτερόλεπτο

Μοντέλα Επικοινωνίας του IoT

Από επιχειρησιακή άποψη, είναι χρήσιμο να σκεφτούμε πώς οι έξυπνες συσκευές συνδέονται και επικοινωνούν μεταξύ τους με διάφορα επικοινωνιακά μοντέλα. Το Μάρτιο του 2015, η Επιτροπή Αρχιτεκτονικής Διαδικτύου (IAB) κυκλοφόρησε ένα καθοδηγητικό έγγραφο αρχιτεκτονικής για τη δικτύωση των έξυπνων αντικειμένων (RFC 7452),που περιγράφει ένα πλαίσιο τεσσάρων κοινών επικοινωνιακών μοντέλων που χρησιμοποιούνται από τις έξυπνες συσκευές. Παρακάτω ακολουθεί το πλαίσιο που εξηγεί βασικά χαρακτηριστικά του κάθε μοντέλου.

Device-to-Device Communications

Το μοντέλο επικοινωνίας device-to-device εφαρμόζεται σε δύο ή περισσότερες συσκευές που συνδέονται και επικοινωνούν μεταξύ τους με την χρήση ενός

μεσάζοντα application server. Αυτές οι συσκευές επικοινωνούν σε πολλούς τύπους δικτύων, συμπεριλαμβανομένων των δικτύων IP ή το Διαδίκτυο. Συχνά, ωστόσο, αυτές οι συσκευές χρησιμοποιούν πρωτόκολλα, όπως το Bluetooth, Z-Wave, ή ZigBee

Π*αράδειγμα 1: επικοινωνία Συσκευής προς Συσκευή*

Το device-to-device δίκτυο επιτρέπει στις συσκευές που χρησιμοποιούν ένα συγκεκριμένο πρωτόκολλο επικοινωνίας να επικοινωνήσουν και να ανταλλάξουν μηνύματα για την επίτευξη της λειτουργίας τους. Αυτό το μοντέλο επικοινωνίας χρησιμοποιείται συνήθως σε εφαρμογές όπως το Smart Home, το οποίο συνήθως χρησιμοποιεί μικρά πακέτα δεδομένων πληροφοριών για επικοινωνία μεταξύ έξυπνων συσκευών με σχετικά χαμηλό ποσοστό πακέτων δεδομένων. Οι έξυπνες οικιακές συσκευές όπως λάμπες, διακόπτες φώτων, θερμοστάτες και κλειδαριές συνήθως στέλνουν μικρά ποσά πληροφοριών το ένα στο άλλο (π.χ. μια κλειδαριά πόρτας όταν ξεκλειδώνεται στέλνει μήνυμα εντολής ενεργοποίησης στα φώτα).

Το μοντέλο επικοινωνίας device-to-device επίσης όμως παρουσιάζει πολλά προβλήματα συνεργασιμότητας τα οποία θα αναφερθούν αργότερα σε αυτή την πτυχιακή. Η Εφημερίδα IETF σε ένα άρθρο της περιγράφει: "Οι συσκευές αυτές έχουν συχνά μια άμεση σχέση, συνήθως έχουν ενσωματωμένη ασφάλεια, αλλά, επίσης, τα device-to-device μοντέλα επικοινωνίας χρησιμοποιούν ειδικά μοντέλα δεδομένων που απαιτούν εφεδρικές προσπάθειες ανάπτυξης [από τους κατασκευαστές συσκευών]". Αυτό σημαίνει ότι οι κατασκευαστές των έξυπνων συσκευών, πρέπει να επενδύσουν στην ανάπτυξη των προσπαθειών για την εφαρμογή συσκευών με ειδικές μορφές δεδομένων αντί να χρησιμοποιήσουν τυποποιημένες μορφές δεδομένων.

Από τη μεριά του χρήστη, αυτό συχνά σημαίνει ότι βασικό πρωτόκολλο επικοινωνίας device-to-device δεν είναι συμβατό, υποχρεώνοντας το χρήστη να επιλέξει μια οικογένεια συσκευών που χρησιμοποιούν ένα κοινό πρωτόκολλο. Για παράδειγμα, η οικογένεια συσκευών χρησιμοποιώντας το Z-Wave πρωτόκολλο δεν είναι εγγενώς συμβατό με το ZigBee πρωτόκολλο. Οι ασυμβατότητες αυτές, περιορίζουν την επιλογή του χρήστη σε συσκευές μέσα σε ένα συγκεκριμένο

πρωτόκολλο επομένως ο χρήστης επωφελείται όταν γνωρίζει ότι τα προϊόντα με συγκεκριμένη οικογένεια έχουν την δυνατότητα να επικοινωνούν σωστά μεταξύ τους.

Device-to-Cloud Communications

Στο μοντέλο επικοινωνίας Device to cloud, η έξυπνη συσκευή συνδέεται άμεσα με μια δωρεάν υπηρεσία cloud (πχ μια εφαρμογή παροχέα ασύρματων υπηρεσιών) για την ανταλλαγή δεδομένων και ελέγχου της κυκλοφορίας του μηνύματος. Η προσέγγιση αυτή συχνά αξιοποιεί τους υπάρχων μηχανισμούς όπως του ενσύρματου Ethernet ή συνδέσεις Wi-Fi για να δημιουργηθεί μια σύνδεση μεταξύ της συσκευής και του δικτύου IP, το οποίο τελικά συνδέεται με το cloud.

Αυτό το μοντέλο επικοινωνίας χρησιμοποιείται από ορισμένες δημοφιλείς καταναλωτικές έξυπνες συσκευές όπως στο Learning Thermostat της Nest Labs και στις SmartTV της Samsung. Στην περίπτωση του Nest Labs Thermostat , η συσκευή μεταδίδει δεδομένα με μια Cloud βάση δεδομένων, όπου τα δεδομένα αυτά μπορούν να χρησιμοποιούνται για την ανάλυση του σπιτιού και την κατανάλωσης ενέργειας. Περαιτέρω, η cloud σύνδεση επιτρέπει στο χρήστη να επιτύχει απομακρυσμένη πρόσβαση στο θερμοστάτη του μέσω ενός έξυπνου τηλεφώνου ή μέσω Web Interface, και υποστηρίζει επίσης τις ενημερώσεις λογισμικού για το θερμοστάτη. Ομοίως και με το Samsung SmartTV, η τηλεόραση χρησιμοποιεί μια σύνδεση στο Διαδίκτυο για να μεταδώσει στο χρήστη πληροφορίες για την έξυπνη τηλεόραση του όπως και επίσης του επιτρέπει την αμφίδρομη φωνητική αναγνώριση. Στις περιπτώσεις αυτές το μοντέλο επικοινωνίας cloud to device δίνει νέες προοπτικές στον χρήστη, επεκτείνοντας τις δυνατότητες της συσκευής πέρα από τα βασικά χαρακτηριστικά της.

Ωστόσο, αρκετές είναι οι προκλήσεις διαλειτουργικότητας που μπορούν να προκύψουν όταν προσπαθεί να ενσωματώσει συσκευές από διάφορους κατασκευαστές. Συχνά, οι υπηρεσίας της συσκευής και του cloud είναι από τον ίδιο προμηθευτή. Αν τα πρωτόκολλα δεδομένων ιδιοκτησίας που χρησιμοποιούνται μεταξύ της συσκευής και του cloud, η συσκευή ή ο χρήστης μπορεί να συνδέεται με μια συγκεκριμένη υπηρεσία cloud, περιορίζοντας ή εμποδίζοντας τη χρησιμοποίηση των εναλλακτικών παρόχων. Αυτό συνήθως αναφέρεται ως "vendor lock in", ένας

όρος που περιγράφει τις άλλες πτυχές της σχέσης της με τον πάροχο υπηρεσιών όπως η ιδιοκτησία και η πρόσβαση σε αυτά τα δεδομένα. Την ίδια στιγμή, οι χρήστες μπορούν να έχουν τη βεβαιότητα ότι οι συσκευές που έχουν σχεδιαστεί για τη συγκεκριμένη πλατφόρμα μπορεί να ενσωματωθούν με αυτή.

Device-to-Gateway Model

Στο μοντέλο επικοινωνίας device-to-gateway με την εφαρμογή-layer gateway (ALG), η έξυπνη συσκευή συνδέεται μέσω μιας ALG υπηρεσίας ως παράγοντας για να επιτευχθεί ένα Cloud. Με απλά λόγια, αυτό σημαίνει ότι υπάρχει εφαρμογή λογισμικού που λειτουργεί σε local gateway device, η οποία δρα ως ενδιάμεσος μεταξύ της συσκευής και του cloud και παρέχει ασφάλεια και άλλες λειτουργίες όπως δεδομένα ή πρωτόκολλο μετάφρασης.

Πολλές μορφές του μοντέλου αυτού βρίσκονται στις καταναλωτικές συσκευές. Σε πολλές περιπτώσεις, το local gateway είναι ένα έξυπνο τηλέφωνο το οποίο χρησιμοποιεί ένα app για να επικοινωνεί με τη συσκευή και να αναμεταδίδει στοιχεία σε ένα cloud. Συχνά αυτό το μοντέλο χρησιμοποιείται από δημοφιλή καταναλωτικά είδη όπως οι personal fitness trackers. Οι συσκευές αυτές δεν έχουν την βασική δυνατότητα να συνδέονται απευθείας σε ένα cloud, με αποτέλεσμα συχνά να βασίζονται σε ενα smartphone app για να χρησιμεύσει ως μεσάζων gateway για να συνδεθεί η συσκευή στο cloud.

Η άλλη μορφή αυτής της συσκευής με το μοντέλο του gateway είναι η ανάδυση του "hub" σε συσκευές οικιακού αυτοματισμού. Αυτές οι συσκευές που χρησιμεύουν ως local gateway μεταξύ μεμονωμένων έξυπνων συσκευών και ενός cloud, μπορούν επίσης να γεφυρώσουν το χάσμα της διαλειτουργικότητας μεταξύ των συσκευών. Για παράδειγμα, το SmartThings hub είναι ένα αυτόνομο gateway που έχει το Z-Wave αλλά και οι πομποδέκτες Zigbee εγκατεστημένο για να επικοινωνεί με τις δύο οικογένειες των συσκευών. Στη συνέχεια, συνδέεται με την SmartThings cloud υπηρεσίες, επιτρέποντας στο χρήστη να αποκτήσει πρόσβαση σε συσκευές χρησιμοποιώντας ένα smartphone app και μια σύνδεση στο Διαδίκτυο.

Η εξέλιξη των συστημάτων με τη χρήση του μοντέλου επικοινωνίας device-to-gateway έχει βοηθήσει πολύ στην αντιμετώπιση των προκλήσεων της

διαλειτουργικότητας μεταξύ των έξυπνων συσκευών.

Μοντέλο Back-End Data-Sharing

Το back-end data-sharing μοντέλο αναφέρεται στην αρχιτεκτονική που επιτρέπει στους χρήστες να εξάγουν και να αναλύσουν τα smart object δεδομένα από ένα cloud σε συνδυασμό με δεδομένα από άλλες πηγές. Η αρχιτεκτονική αυτή υποστηρίζει την επιθυμία του χρήστη για την πρόσβασης αποστολής δεδομένων σε τρίτους. Η προσέγγιση αυτή αποτελεί προέκταση του μοντέλου επικοινωνίας device-to-cloud, το οποίο μπορεί να οδηγήσει σε δεδομένα όπου οι έξυπνες συσκευές στέλνουν δεδομένων μόνο για μια ενιαία εφαρμογή υπηρεσιών. Το μοντέλο back-end sharing architecture επιτρέπει στα δεδομένα που συλλέγονται από την έξυπνη συσκευή να συγκεντρώνονται και να αναλύονται.

Για παράδειγμα, ένας χρήστης με ένα συγκρότημα γραφείων θα ενδιαφέρεται για την εδραίωση και την ανάλυση της ενεργειακής κατανάλωσης, με βοηθητικές εφαρμογές δεδομένων που παράγονται από όλους τους αισθητήρες των έξυπνων συσκευών στις εγκαταστάσεις του. Μια αποτελεσματική αρχιτεκτονική back-end data sharing θα επιτρέψει στην εταιρεία να αποκτήσει εύκολη πρόσβαση και να αναλύσει τα δεδομένα στο cloud των συσκευών του κτιρίου. Επίσης, αυτό το είδος της αρχιτεκτονικής διευκολύνει τη φορητότητα των αναγκών των δεδομένων. Αποτελεσματικές back-end data-sharing αρχιτεκτονικές επιτρέπουν στους χρήστες να μετακινούν τα δεδομένα όταν εναλλάσσονται μεταξύ έξυπνων υπηρεσιών.

Το back-end data-sharing μοντέλο προτείνει μια ομόσπονδη υπηρεσία προσέγγισης cloud ή cloud applications programmer interfaces (APIs) τα οποία είναι αναγκαία για την επίτευξη της διαλειτουργικότητας του δεδομένων των έξυπνων συσκευών που φιλοξενείται στο cloud.

Παράδειγμα 4. Back-end data sharing model diagram

IPv6 and the IoT

Παρόλο που διαφέρουν με τους ακριβείς αριθμούς, οι παρατηρητές της τεχνολογίας συμφωνούν ότι δισεκατομμύρια επιπλέον συσκευές από βιομηχανικούς αισθητήρες

οικιακών συσκευών μέχρι και οχημάτων θα συνδέονται στο Internet και μέχρι το 2025. Το IoT συνεχίζει να αυξάνεται, γι' αυτό οι συσκευές που απαιτούν την end-to-end σύνδεση στο Διαδίκτυο δεν θα είναι σε θέση να επικαλεστούν το IPv4, δηλαδή το πρωτόκολλο υπηρεσίας Internet που χρησιμοποιούμε σήμερα. Θα χρειαστεί μια νέα τεχνολογία η οποία ονομάζεται: IPv6.

Το IPv6 είναι μια πολυαναμενόμενη αναβάθμιση του Διαδίκτυου στο βασικό πρωτόκολλο IP, το οποίο υποστηρίζει όλες τις επικοινωνίες στο Διαδίκτυο. Το IPv6 είναι απαραίτητο διότι το Διαδίκτυο τείνει να ξεμείνει από διευθύνσεις IPv4. Όταν το IPv4 μπορεί να υποστηρίξει 4.3 δις συσκευές συνδεδεμένες στο Διαδίκτυο, το IPv6 με 2 εις την 128 διαθέσιμες διευθύνσεις, μπορεί να χρησιμοποιηθεί για οτιδήποτε χρειαστεί χωρίς να εξαντλείται. Αυτό αντιπροσωπεύει περίπου 340 τρισεκατομμύρια διευθύνσεις, οι οποίες είναι πολύ περισσότερο ικανοποιητικές από την ζήτηση των περίπου 100 δισεκατομμυρίων έξυπνων συσκευών που υπολογίζεται ότι θα χρησιμοποιούμε τις επόμενες δεκαετίες.

Οι βασικές προκλήσεις για τους προγραμματιστές του IoT είναι πως το IPv6 δεν είναι εγγενώς διαλειτουργικό με το πρωτόκολλο IPv4. Επίσης πιο χαμηλού κόστους λογισμικό είναι άμεσα διαθέσιμο για ενσωμάτωση στις έξυπνες συσκευές που υλοποιούνται μόνο με το πρωτόκολλο IPv4. Ωστόσο πολλοί ειδικοί πιστεύουν, ότι το IPv6 είναι η καλύτερη επιλογή συνδεσιμότητας και θα επιτρέψει στο IoT να φτάσουν το επιθυμητό αποτέλεσμα.

ΚΕΦΑΛΑΙΟ 2

ΕΦΑΡΜΟΓΕΣ ΤΟΥ IoT

i)ΤΟ IoT ΣΕ ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΕΠΙΠΕΔΟ

Διευρυμένη επιχειρηματική ατζέντα για το οικοσύστημα του IoT (IoT) έχουν, για το τρέχον έτος, οι εταιρείες ανά τον κόσμο, με το IoT να εξελίσσεται σε mainstream τάση για μια σειρά από κλάδους της οικονομίας. Ενδεικτικό της εξοικείωσης του επιχειρείν με το IoT είναι ότι, έως τα τέλη του 2016, περίπου μία στις δύο επιχειρήσεις (43%) αναμένεται να έχει υιοθετήσει σχετικές λύσεις και υπηρεσίες.

Μέχρι τα τέλη του 2016 εκτιμάται ότι μία στις δύο εταιρείες στον κόσμο θα έχει υιοθετήσει λύσεις και υπηρεσίες IoT Σήμερα, λιγότερο από το ένα τρίτο των εταιρειών σε παγκόσμιο επίπεδο (το 29%) κάνει χρήση υπηρεσιών IoT, ενώ ένα πρόσθετο ποσοστό 14% σκοπεύει να το υιοθετήσει εντός του 2016. Με βάση αυτές τις εκτιμήσεις, οι εταιρείες και οι οργανισμοί που υιοθετούν IoT αναμένεται να αυξηθούν κατά 50% στη διάρκεια του 2016. Επιπλέον, υπάρχει ένα ποσοστό εταιρειών, της τάξης του 21%, το οποίο σχεδιάζει να εισάγει λύσεις και υπηρεσίες, που σχετίζονται με το IoT, μετά από το 2016.

Σύμφωνα με έρευνα της Gartner, που διενεργήθηκε σε περίπου 500 στελέχη του IT σε ΕΜΕΑ, Βόρεια Αμερική, Ασία - Ειρηνικό και Λατινική Αμερική, Πάντως, παρά τη στροφή επιχειρήσεων και οργανισμών στο IoT, η έρευνα εντοπίζει ένα σημαντικό ποσοστό εταιρειών, το οποίο δεν έχει καθόλου πλάνα σχετικά με τη νέα αυτή τάση της ψηφιακής τεχνολογίας. Παράλληλα, υπάρχει και ένα 9% των εταιρειών που δηλώνει ότι δεν έχει κανένα ενδιαφέρον όχι μόνο για το IoT, αλλά συνολικά για την υιοθέτηση των νέων ψηφιακών τεχνολογιών.

Η βιομηχανία

Παρά την εμφανή στροφή εταιρειών και οργανισμών στο IoT, η εικόνα στους επιμέρους κλάδους της οικονομίας είναι σαφώς διαφορετική, με άλλους τομείς να είναι εξαιρετικά εξοικειωμένοι και άλλους να υστερούν. Για παράδειγμα, οι επιχειρήσεις κοινής ωφέλειας, οι πετρελαϊκές εταιρείες, οι εταιρείες φυσικού αερίου

και οι κατασκευαστικές πρωταγωνιστούν στην υιοθέτηση του IoT. Στον αντίποδα, οι εταιρείες παροχής υπηρεσιών φαίνεται να υστερούν.

Σύμφωνα με τις εκτιμήσεις της Gartner, περισσότερες από τις μισές επιχειρήσεις (56%) της λεγόμενης βαριάς βιομηχανίας θα έχουν υιοθετήσει σχετικές λύσεις μέχρι τα τέλη του 2016. Το αντίστοιχο ποσοστό για τους τομείς της παροχής υπηρεσιών τοποθετείται στο 36%.

Οι συντάκτες της έρευνας διαπιστώνουν, παράλληλα ότι, μέχρι σήμερα, οι επιχειρήσεις που έχουν υιοθετήσει λύσεις και υπηρεσίες IoT το έχουν πράξει με στόχο τη βελτίωση της εσωτερικής τους οργάνωσης και δευτερευόντως την εξυπηρέτηση των πελατών. Συγκεκριμένα, μέχρι σήμερα, οι εταιρείες που έχουν εστιάσει στο IoT επιδιώκοντας βελτιωμένη λειτουργία, καλύτερη χρήση των πόρων και εξοικονόμηση κόστους αντιστοιχούν στο 52%, ενώ εκείνες που υιοθέτησαν σχετικές λύσεις με στόχο τη βελτίωση της εμπειρίας του καταναλωτή αντιπροσωπεύουν το 40%.

Οι κλάδοι

Η έρευνα διαπιστώνει ότι, παρά το γεγονός πως συγκεκριμένοι κλάδοι της οικονομίας καθοδηγούν την παγκόσμια ζήτηση για προϊόντα και υπηρεσίες cloud, όλοι οι τομείς της οικονομικής δραστηριότητας έχουν αρχίσει να διερευνούν το cloud. Σύμφωνα με τα ευρήματα της έρευνας, κλάδοι, όπως οι Τηλεπικοινωνίες, τα Media και η Ψυχαγωγία, αλλά και οι επαγγελματικές υπηρεσίες πρωταγωνιστούν στην υιοθέτηση του cloud computing (με 68% και 61% αντίστοιχα). Ωστόσο και οι υπόλοιποι τομείς, αν και υστερούν στη χρήση υπηρεσιών cloud, κάθε άλλο παρά αδιάφοροι είναι στην υιοθέτησή τους: οι κατασκευές και η αυτοκινητοβιομηχανία (με 48%), καθώς και ο τομέας της ενέργειας (με 51%), επίσης, φαίνεται να κάνουν στροφή προς το cloud.

Οι πάροχοι

Σε κάθε περίπτωση, οι ανάγκες που καλύπτουν οι μικρομεσαίες επιχειρήσεις μέσα από τη χρήση του cloud είναι τόσο διαφορετικές, που οι πάροχοι σχετικών υπηρεσιών - όπως υποδεικνύει η έρευνα - πρέπει να στοχεύουν στις προσωποποιημένες ανάγκες κάθε εταιρείας.

Για παράδειγμα, η πλειοψηφία των ΜΜΕ και συγκεκριμένα το 75%, επιθυμεί οι λύσεις cloud να συνδυάζονται με τις παραδοσιακές τηλεπικοινωνιακές υπηρεσίες που χρησιμοποιεί (κινητή και σταθερή τηλεφωνία, Internet, κλπ.).

Επιπλέον, περίπου επτά στις δέκα δηλώνουν ότι θα επιθυμούσαν να λαμβάνουν το σύνολο των υπηρεσιών από έναν και μόνο πάροχο, ενώ το 68% δηλώνει ότι είναι πιο πιθανό να ανανεώσουν το συμβόλαιο τους με τον παραδοσιακό πάροχο τηλεπικοινωνιακών υπηρεσιών, εφόσον αυτός είναι σε θέση να τους παρέχει και υπηρεσίες cloud.

Τέλος, το 80% των ΜΜΕ απαντά ότι θα προτιμούσε να λαμβάνει έναν ενιαίο λογαριασμό για όλες τις τηλεπικοινωνιακές υπηρεσίες που λαμβάνει (παραδοσιακές και βασισμένες στο cloud).

Εμπόδια

Την ίδια στιγμή που η υιοθέτηση του Cloud ενισχύεται, η έρευνα διαπιστώνει ότι πολλοί παράγοντες είναι εκείνοι που εμποδίζουν την περαιτέρω διείσδυση των σχετικών υπηρεσιών στις μικρομεσαίες επιχειρήσεις ανά τον κόσμο. Μεταξύ αυτών, η έρευνα κατατάσσει το νομοθετικό και ρυθμιστικό πλαίσιο κάθε χώρας, που πολλές φορές αποθαρρύνει τις επιχειρήσεις από την υιοθέτηση του cloud. Ο δεύτερος παράγοντας, σύμφωνα με τη μελέτη, είναι η γενικότερη πορεία της οικονομίας κάθε χώρας.

Εφαρμογές του IoT σε επιχειρησιακό επίπεδο που διατίθενται στην Ελλάδα σήμερα:

- Προοπτικές από την εφαρμογή του IoT για την ανάπτυξη νέων ή τη βελτίωση των υφιστάμενων επιχειρηματικών δραστηριοτήτων.

- Κλάδοι που θα μπορούσαν να ωφεληθούν από το IoT. Θα μπορούσε το IoT να υποβοηθήσει τις νέες επενδύσεις προς τις ελληνικές επιχειρήσεις;

- Επένδυση σε εφαρμογές IoT με αξιοσημείωτο και μετρήσιμο ROI.

- Οικονομίες κλίμακας που επιτυγχάνονται μέσω της εφαρμογής του IoT.

- Μπορεί το IoT να εντοπίσει έγκαιρα «προβλήματα» σε μια παραγωγική διαδικασία (Big data & Analytics);

- Έξυπνη διαχείριση ενέργειας προς όφελος κάθε επιχείρησης.

- Παρακολούθηση στόλου οχημάτων και διαχείριση εφοδιαστικής αλυσίδας.

- Λιανική πώληση, big data, τεχνολογία Beacon, εξατομικευμένες εφαρμογές που προσαρμόζονται ανάλογα με την τοποθεσία και τις συνήθειες του καταναλωτή (location-based and personalization).

- Το σούπερ μάρκετ του μέλλοντος.

- Το IoT στην υπηρεσία του ασφαλιστικού κλάδου.

- Τάσεις, αναδυόμενες πλατφόρμες και εφαρμογές του IoT στο άμεσο μέλλον.

- Εφαρμογές που αυξάνουν την απόδοση και την παραγωγικότητα των εργαζομένων.

- IoT και αλλαγές στον τρόπο καταναλωτικής συμπεριφοράς. Εμπειρία καταναλωτή και προγράμματα loyalty.

- Απειλές και ασφάλεια συστημάτων IoT.

Η αυξημένη ελληνική συμμετοχή σε ευρωπαϊκά ερευνητικά έργα για το IoT και η ανάπτυξη συνεργασιών και δικτύωσης μεταξύ ακαδημαϊκής και επιχειρηματικής κοινότητας, με τη δημιουργία ενός ελληνικού οργανισμού για το IoT, ήταν μερικά από τα θέματα που αναδείχθηκαν στην ιδιαίτερα επιτυχημένη εκδήλωση που διοργάνωσαν το Εθνικό Κέντρο Τεκμηρίωσης (ΕΚΤ) και η ευρωπαϊκή Συμμαχία για το IoT (Alliance for the IoT Innovation, AIOTI). Η εκδήλωση πραγματοποιήθηκε με την υποστήριξη της Ευρωπαϊκής Επιτροπής, στις 8 Φεβρουαρίου 2016 στο Εθνικό Ίδρυμα Ερευνών.

Σύμφωνα με όσα αναφέρονται σε ανακοίνωση του Εθνικού Κέντρου Τεκμηρίωσης, η εκδήλωση "AIOTI Open Day: Χρηματοδότηση & καινοτομία μέσω του IoT στην

Ελλάδα" απευθυνόταν στους δρώντες του οικοσυστήματος IoT, τόσο από την πλευρά της προσφοράς (technology providers) όσο και της ζήτησης (end users) τεχνολογίας, και είχε σκοπό τη διεύρυνση της εθνικής συμμετοχής σε μια από τις σημαντικότερες μελλοντικές τεχνολογίες, παράλληλα με τις ενέργειες που γίνονται για το IoT σε ευρωπαϊκό επίπεδο.

Όπως τονίζεται στην ανακοίνωση, το IoT αφορά τη διασύνδεση ατόμων, μηχανών, οικιακών συσκευών, απλών αντικειμένων και διαδικασιών, γεγονός που δημιουργεί απεριόριστες δυνατότητες και προοπτικές για τις κυβερνήσεις, τις επιχειρήσεις και τους πολίτες. Σήμερα, οι συσκευές που είναι online αγγίζουν τα 10 δισεκατομμύρια, ενώ μέχρι το 2020 προβλέπεται ότι θα φτάσουν τα 34 δισεκατομμύρια. Τα επόμενα πέντε χρόνια, η έρευνα προβλέπει ότι θα επενδυθούν 6 τρισεκατομμύρια δολάρια στο IoT.

Όπως επισήμανε σε χαιρετισμό της η Εύη Σαχίνη, Διευθύντρια του ΕΚΤ, η επιστημονική αριστεία της Ελλάδας τεκμηριώνεται από την επιτυχημένη συμμετοχή σε μία από τις πιο ανταγωνιστικές προκηρύξεις του Ορίζοντα 2020 στο πρόγραμμα ICT με θέμα το IoT. Παράλληλα υπογράμμισε ότι το ΕΚΤ, πέρα από τον ρόλο του ως Εθνικό Σημείο Επαφής για το πρόγραμμα ICT, προσφέρει υποδομές και υπηρεσίες για την αξιοποίηση και διάχυση τόσο του έγκριτου ελληνικού ψηφιακού περιεχομένου, όσο και των δεδομένων, δίνοντας έμφαση στην ανοικτή διάθεση και επανάχρηση. Σε αυτό το πλαίσιο, τα δεδομένα που θα προέλθουν από το IoT στο μέλλον θα αποκτήσουν ιδιαίτερη δυναμική και το ΕΚΤ θα την υποστηρίξει ενεργά, απευθυνόμενο σε ολοένα και περισσότερες κοινότητες χρηστών.

Ο Ηρακλής Αγιοβλασίτης από το ΕΚΤ, Εθνικό Σημείο Επαφής για το πρόγραμμα ICT του Ορίζοντα 2020 (ευρωπαϊκό χρηματοδοτικό πλαίσιο για την έρευνα και καινοτομία), αναφέρθηκε στα αποτελέσματα της προκήρυξης ICT-30-2015: IoT and Platforms for Connected Smart Objects για έρευνα σε τεχνολογίες του IoT, στην οποία υποβλήθηκαν 137 προτάσεις για έργα και εγκρίθηκαν 7 έργα έρευνας και ανάπτυξης (Research and Innovation Actions) και 2 έργα συντονισμού και υποστήριξης (Coordination and Support Actions).

Η Ελλάδα συμμετέχει σε 4 από τα 7 εγκεκριμένα έργα έρευνας και ανάπτυξης σε

πανευρωπαϊκό επίπεδο, αντλώντας συνολικά 3,36 εκατ. ευρώ κοινοτικής συγχρηματοδότησης, ενώ η συνολική κοινοτική συγχρηματοδότηση για έρευνα και ανάπτυξη είναι 51,5 εκ ευρώ. Η συμμετοχή της Ελλάδας ανέρχεται στο 6,5% της συνολικής διαθέσιμης κοινοτικής συγχρηματοδότησης. Συγκεκριμένα, ελληνική συμμετοχή υπάρχει στα έργα BIG IoT, Agile, SymbIoTe και Vicinity. Σε αυτά τα έργα συμμετέχουν οι παρακάτω 7 φορείς: Εθνικό Κέντρο Έρευνας & Τεχνολογικής Ανάπτυξης (ΕΚΕΤΑ), GNOMON Informatics SA, Δήμος Πυλαίας Χορτιάτη, Econais A.E., Bioassist A.E., Intracom A.E. Telecom Solutions, Οργανισμός Τηλεπικοινωνιών Ελλάδος (ΟΤΕ).

Στο πρώτο μέρος της εκδήλωσης παρουσιάστηκαν αναλυτικά οι δυνατότητες χρηματοδότησης για έρευνα και καινοτομία μέσα από τον Ορίζοντα 2020. Ο Peter Friess, εκπρόσωπος της Ευρωπαϊκής Επιτροπής (DG CNECT) αναφέρθηκε διεξοδικά στις λεπτομέρειες των προκηρύξεων σχετικά με το IoT, χαρακτηρίζοντας το IoT ως την επόμενη ψηφιακή επανάσταση. Ο P. Friess υπογράμμισε ότι η Ευρώπη έχει την ικανότητα να είναι πρωτοπόρος στο IoT, καθώς υπάρχουν και οι κατάλληλοι φορείς, όσο η έρευνα και το θεμελιωμένο οικοσύστημα IT. Υπάρχει όμως ο κίνδυνος του κατακερματισμού των προσπαθειών και της καθυστέρησης λόγω και του διεθνούς ανταγωνισμού. Επίσης, παρουσίασε εκτενώς τις ανοικτές προκηρύξεις για πιλοτικά έργα μεγάλης κλίμακας IoT (Large Scale Pilots) στο Horizon 2020, τα οποία έχουν καταληκτική ημερομηνία 12 Απριλίου 2016.

Τα πιλοτικά έργα μεγάλης κλίμακας αφορούν τις περιοχές: Pilot 1: Smart living environments for ageing well (20 εκατ. ευρώ), Pilot 2: Smart Farming and Food Security (30 εκατ. ευρώ), Pilot 3: Wearables for smart ecosystems (15 εκατ. ευρώ), Pilot 4: Reference zones in EU cities (15 εκατ. ευρώ), Pilot 5: Autonomous vehicles in a connected environment (20 εκατ. ευρώ). Ο P. Friess έκλεισε με χρήσιμες οδηγίες για την επιτυχημένη υποβολή προτάσεων και απάντησε στις ερωτήσεις του κοινού.

Ο Κωνσταντίνος Σπυρόπουλος, Διευθυντής Ερευνών στο ΕΚΕΦΕ Δημόκριτος, μίλησε για το Alliance for the IoT Innovation (AIOTI), με την ιδιότητά του ως συντονιστής του AIOTI στην Ελλάδα. Η Συμμαχία για το IoT (AIOTI) ξεκίνησε από την Ευρωπαϊκή Επιτροπή και σημαντικούς οργανισμούς που δραστηριοποιούνται στον χώρο του IoT. Η AIOTI έχει ως στόχο να εξασφαλίσει στην ΕΕ το προβάδισμα

στις σχετικές τεχνολογίες, δημιουργώντας ένα δυναμικό ευρωπαϊκό IoT οικοσύστημα. Ο Κ. Σπυρόπουλος επισήμανε τις βασικές προκλήσεις για την ανάπτυξη του IoT, όπως η γρήγορη τεχνολογική ανάπτυξη, η αποδοχή των υπηρεσιών IoT από τους χρήστες, η ανάγκη για ανάπτυξη σχετικών επιχειρηματικών μοντέλων, το ρίσκο του κατακερματισμού, και ο διεθνής ανταγωνισμός.

Στη συνέχεια παρουσιάστηκαν καλές πρακτικές από έργα που έχουν ήδη επιλεγεί προς χρηματοδότηση στον χώρο του IoT (ICT-30-2015). Ο Σέργιος Σούρσος (Intracom AE) αναφέρθηκε στο SYMBIOTE project, το οποίο και έλαβε την υψηλότερη βαθμολογία στη συγκριτική αξιολόγηση και αφορά τη συμβίωση έξυπνων αντικειμένων σε περιβάλλοντα IoT. Το έργο AGILE (Adoptive Gateways for dIverse MuLtiple Environments) παρουσίασε ο Χάρης Δούκας (Create-net), ενώ ο Θανάσης Τρυφερίδης (ΕΚΕΤΑ), μίλησε για το VICINITY project, το οποίο προσφέρει νέες υπηρεσίες μέσω της διαλειτουργικότητας σε περιβάλλοντα IoT.

Στο δεύτερο μέρος της εκδήλωσης, πραγματοποιήθηκε συζήτηση με πρωτοβουλία επιχειρήσεων και οργανισμών που δραστηριοποιούνται στον χώρο του IoT, αποσκοπώντας στη δημιουργία συνεργειών και συνεργασίας μεταξύ της ακαδημαϊκής/ερευνητικής και επιχειρηματικής κοινότητας, καθώς και στη θεσμοθέτηση ενός ελληνικού οργανισμού για το Internet of Things. Συγκεκριμένα, πήραν θέση οι πιο δραστήριοι οργανισμοί του ελληνικού οικοσυστήματος IoT, ενώ παρουσιάστηκαν εθνικές πρωτοβουλίες που λαμβάνουν χώρα στο εξωτερικό σε επίπεδο συνολικής στρατηγικής για το IoT. Ανάμεσα σε αυτούς, οι εταιρείες Future Intelligence, Intracom AE, Athens Information Technology, ΕΕΛ/ΛΑΚ, PlegmaLabs, Warply, exm. Επιπλέον, παρουσιάστηκαν και συγκεκριμένες καλές πρακτικές από τη χώρα μας, όπως το mi-cluster (cluster μικροηλεκτρονικής corallia), το οποίο έχει οργανώσει πλήθος επιχειρηματικών αποστολών στο εξωτερικό, καθώς και το ανεπίσημο IoT meetup της ελληνικής κοινότητας χρηστών.

Όπως επισημάνθηκε στις τοποθετήσεις των συμμετεχόντων, η ανάγκη συνέργειας μεταξύ των επιχειρήσεων και οργανισμών που δραστηριοποιούνται στον χώρο του IoT μπορεί να συνεισφέρει στην επίτευξη ανταγωνιστικού πλεονεκτήματος και επίτευξη οικονομιών κλίμακας. Παράλληλα, απαιτείται ένα εθνικό πλαίσιο στρατηγικής για το IoT με όραμα, σταθερή ηγεσία και συγκεκριμένες δράσεις που

θα έχουν τον ρόλο καταλύτη και πολλαπλασιαστή προστιθέμενης αξίας και παραγωγικότητας, καταλήγει η ανακοίνωση.

ii) Urban Environments

ToSmartP σε γενικές γραμμές βασίζεται ως επί το πλείστον σε αισθητήρες που τοποθετούνται στο έδαφος της καλλιέργειας και στην συνέχεια μεταβιβάζουν τις πληροφορίες στον κόμβο πίνακα με τον οποίον συνδέονται. Ο τελευταίος συγκεντρώνει τις κατά τόπους μετρήσεις, τις οποίες και στέλνει ασύρματα σε ένα κεντρικό κόμβο που αναλαμβάνει την αποθήκευση και την επεξεργασία των δεδομένων δια μέσου ενός συστήματος απόφασης SmartP DSS και εντέλει την διαχείριση της καλλιέργειας με σκοπό την βελτιστοποίηση των προϊόντων.

Ειδικότερα, μετά την ολοκλήρωση των αναλύσεων, των SPartP DSS μπορεί ή να λάβει κάποια απόφαση και να εκτελέσει μία βελτιωτική εργασία π.χ πότισμα ή και κλείσιμο των σκέπαστρων ή να στείλει μέσω δικτύου τα αποτελέσματα στον τελικό χρήστη-αγρότη, προκειμένου να τον ενημερώσει για την κατάσταση της καλλιέργειάς του.

Ουσιαστικά το συγκεκριμένο σύστημα, είναι εξίσου σημαντικό με τα κλασικά εργαλεία του οργανωμένου σύγχρονου αγρότη, όπως το τρακτέρ, η σπαρτική και τα λιπασματοδιανομέα μιας και το SmartP μετρά, καταγράφει και αναλύει τις συνθήκες διαχείρισης της καλλιέργειας π.χ. κλιματικές συνθήκες, υδατική κατάσταση του εδάφους και του περιβάλλοντος π.χ. “εχθροί” όπως ο Περονόσπορος, ο Βοτρύτης και η Φαιά σήψη.

Πιο συγκεκριμένα, βάσει των πληροφοριών που συλλέγουν οι αισθητήρες και τα αποτελέσματα της ανάλυσης τους από το SmartP DSS, το σύστημα SmartP μπορεί να συμβουλεύει τον τελικό χρήστη, τον αγρότη δηλαδή, για τα εξής:

- Πόσο νερό έχει καταναλωθεί από την καλλιέργεια και πόσο απόθεμα υπάρχει στο έδαφος.

- Πότε και πόσο πρέπει να ποτίσει.

- Ποια είναι η επικινδυνότητα προσβολής της καλλιέργειας από ασθένειες.
- Πότε πρέπει να κάνει ψεκασμό προληπτικά ή θεραπευτικά.
- Ποιες είναι οι τρέχουσες κλιματικές συνθήκες, ενώ υπολογίζει τις ώρες ψύχους, τις ημέρες ζέστης, το σημείο δρόσου κλπ.
- Τυχόν ακραία και επικίνδυνα καιρικά φαινόμενα τα οποία μπορει να βλάψουν την καλλιέργεια (ακραίες θερμοκρασίες, παγετός, ισχυροί άνεμοι, κλπ)
- Τεκμηρίωση προς τους ασφαλιστικούς οργανισμούς απώλειας, ή μείωση παραγωγής λόγο καιρικών συνθηκών

Βασικές εφαρμογές:

Ας υποθέσουμε ότι το SmartP εγκατεστημένο σε έναν αμπελώνα αλλά οι καιρικές συνθήκες ευνοούν τις προσβολές από περονόσπορο σε πρώιμες και όψιμες καλλιέργειες.

Η καταπολέμηση του περονόσπορου γίνεται με καλλιεργητικά μέτρα (καλλιέργεια σε χωράφια που στραγγίζουν καλά, φύτευση υγιούς πολλαπλασιαστικού υλικού, εφαρμογή αμειψισποράς κα) αλλά και με ψεκασμό με εγκεκριμένα για την καλλιέργεια και εκλεκτικά για τον περονόσπορο μυκητοκτόνα.

Η διαδικασία ανάπτυξης ασθένειας δεν είναι ακαριαία αλλά διαρκεί μέρες. Το σύστημα SmartP μπορεί να παρακολουθεί την εξέλιξη της ασθένειας συνεχώς. Μόλις η επικινδυνότητα φτάσει στο όριο που απαιτείται ψεκασμός, τότε το σύστημα, το οποίο επεξεργάζεται τα δεδομένα που συλλέγει κάθε 10 λεπτά, στέλνει email, sms ή ηχητικό μήνυμα στον παραγωγό και τον γεωπόνο με την περιγραφή του συμβάντος αναφέροντας, παραδείγματος χάρη, κάτι σαν το εξής: “Απαιτείται προληπτικός ψεκασμός στο αγροτεμάχιο X”. Το SmartP διαμέσου του SmartP DSS μπορεί να αναλύει διαφορετικά σενάρια τα οποία καλύπτουν διαφορετικές ανάγκες όπως το πότισμα, το ράντισμα, η εκτίμηση παραγωγής και άλλα

Πότισμα:

Ο αγρότης έχει εγκαταστήσει σε ένα απομακρυσμένο κτήμα. Από τους ειδικούς

πίνακες που έχουν εγκατασταθεί στα χωράφια, ο παραγωγός θέτει, παραδείγματος χάρη, τα όρια υγρασίας στο έδαφος για να ελέγχει το πότισμα. Στη συνέχεια το σύστημα μετρά σε διαφορετικά σημεία της καλλιέργειας κάθε 15 λεπτά και τα μεταφέρει στον κεντρικό κόμβο που αναλαμβάνει την ανάλυση και την ενεργοποίηση διεργασιών ή και την αποστολή της ειδοποίησης στον ενδιαφερόμενο. Μόλις η υγρασία του εδάφους πέσει κάτω από το όριο για πάνω από ένα χρονικό διάστημα, ο κεντρικός κόμβος που είναι διασυνδεδεμένος μπορεί να στείλει ένα email ή ένα sms στον αγρότη και να τον ενημερώνει. Αυτός το βλέπει και καταλαβαίνει ότι πρέπει να ποτίσει, ενώ κατά τη διάρκεια μπορεί να παρακολουθεί και το επίπεδο της υγρασίας σε πραγματικό χρόνο για να ξέρει πότε ακριβώς να σταματήσει το πότισμα.

Ράντισμα:

Ας υποθέσουμε τώρα ότι ο αγρότης θέλει να μεταβεί στο ίδιο κτήμα που βρίσκεται εγκατεστημένο το SmartP, με στόχο να ραντίσει την καλλιέργειά του. Σε αυτήν την περίπτωση μπορεί να μπει στο σύστημα μέσω Internet και να δει τις μετρήσεις του μετεωρολογικού σταθμού, προκειμένου να διαπιστώσει εάν το μικρόκλιμα στην περιοχή του ευνοεί κάτι τέτοιο ή όχι. Με αυτόν τον τρόπο γλυτώνει στην άσκοπη μετακίνηση ή την λανθασμένη επέμβαση στην καλλιέργεια.

Εκτίμηση Παραγωγής:

Υποθέτουμε ότι έχουν περάσει τρία χρόνια από την στιγμή της εγκατάστασης του SmartP. Ο αγρότης όλο αυτό το διάστημα έχει δημιουργήσει μία αξιόπιστη βάση δεδομένων με τις κλιματικές συνθήκες της κάθε περιοχής του κτήματος, με αποτέλεσμα να είναι σε θέση να συγκρίνει τα στοιχεία μεταξύ τους, προκειμένου να προβλέψει με ακρίβεια την ποσότητα και ποιότητα της σοδειάς ανά χρονική περίοδο. Συστήματα όπως αυτά μπορούν να εφαρμοστούν σε κάθε είδους καλλιέργεια, είτε πρόκειται για ετήσιες, όπως ντομάτες, πατάτες, μαρούλια, φράουλες, ηλίανθους, σιτηρά και καλαμπόκι είτε για πολυετής όπως αμπέλια, ροδάκινα, μήλα, αχλάδια, ελιές και βερίκοκα. Ωστόσο υπάρχουν και εκείνα τα συστήματα που προορίζονται για πιο «ευαίσθητες» καλλιέργειες, όπου το πότισμα ή η έγκαιρη διάγνωση παγετού είναι θέματα ζωτικής σημασίας. Κατά συνέπεια, όπως εξηγούν οι ειδικοί του χώρου, το κόστος τέτοιον συστημάτων αποσβένεται πολύ πιο γρήγορα σε καλλιέργειες που ασθενούν εύκολα και χρειάζονται έντονη

παρακολούθηση.

Οφέλη – πλεονεκτήματα

- Αύξηση της παραγωγής, καθώς η άρδευση και οι ψεκασμοί γίνονται όταν το ίδιο το φυτό τα έχει ανάγκη και όχι με βάση το ημερολόγιο.

- Βελτίωση της ποιότητας του προϊόντος κυρίως σε καλλιέργειες που απαιτούν μεγάλη ακρίβεια στην άρδευση κατά το τελικό στάδιο ωρίμανσης (πχ Αμπέλι).

- Προστασία του περιβάλλοντος και των φυσικών πόρων. Λιγότεροι ψεκασμοί με φυτοφάρμακα, λιγότερη χρήση νερού.

- Εξοικονόμηση χρόνου: Ο παραγωγός μπορεί να γνωρίζει το ποια είναι η καταλληλότερη στιγμή να αρχίσει το πότισμα ή να μαζέψει την σοδειά του.

- Ο αγρότης έχει στην διάθεσή του μετρήσεις με ποικιλία μετρούμενων μεγεθών, τη δυνατότητα παρακολούθησης του μικροκλίματος σε διαφορετικές περιοχές της καλλιέργειας και πρόσβαση σε ιστορικά δεδομένα.

- Τα δεδομένα των μετρήσεων είναι άμεσα προσβάσιμα από οποιοδήποτε σημείο του κόσμου μέσω «έξυπνων» συσκευών (Έξυπνα κινητά τηλέφωνα, υπολογιστές, tablet).

- Μπορούν να εξυπηρετήσουν στην επίβλεψη μεγάλων εκτάσεων, καθώς κάθε κόμβος καλύπτει απόσταση έως 2.5 χιλιομέτρων.

- Τα συστήματα εγκαθίστανται εύκολα και με σχετικά χαμηλό κόστος, ενώ πολλά τροφοδοτούνται από μπαταρίες που επαναφορτίζονται μέσω φωτοβολταϊκών πάνελ.

Γνώσεις – Εξειδίκευση

Αντίθετα με ότι θα πίστευαν οι αγρότες που δεν είναι εξοικειωμένοι με τις νέες τεχνολογίες, δεν χρειάζονται πτυχία και πανεπιστημιακές γνώσεις για να χρησιμοποιήσει κάποιος τέτοια συστήματα στις καλλιέργειές του. «Τα συστήματα είναι πλέον προσαρμοσμένα στις ανάγκες και τις δυνατότητες των απλών χρηστών

που δεν διαθέτουν εμπειρία σε σύγχρονες τεχνολογίες. Σαφώς απαιτείται μια μικρή εκπαίδευση, η οποία παρέχεται δωρεάν μέσω των συνεργατών. Μάλιστα, οι χρήστες που διαθέτουν μεγαλύτερη εξοικείωση μπορούν να δημιουργήσουν ακόμα και τους δικούς τους τρόπους επεξεργασίας των δεδομένων».

Όταν υπάρχουν ιδιαίτερες ανάγκες περαιτέρω εκπαίδευσης, οι ενδιαφερόμενοι εξετάζονται κατά περίπτωση και πιθανότατα να υπάρξουν επιπλέον χρεώσεις ανάλογα με τις απαιτήσεις τους. « Το σύστημα SmartP, παραδείγματος χάρη προτείνεται σε χρήστες με βασικές γεωπονικές γνώσεις και μέσο επίπεδο χρήσης υπολογιστών, όπως η πλοήγηση στο Διαδίκτυο, κατανόηση προγράμματος Excel και τα λοιπά.

iii) SMART HOME

Όταν ο ηλεκτρικός εξοπλισμός είναι συνδεδεμένος στην πρίζα, αλλά δεν είναι σε χρήση, αλλά όμως υπάρχει ροή ηλεκτρισμού. Αυτό σημαίνει ότι σπαταλάμε ηλεκτρική ενέργεια από πέντε έως δέκα τοις εκατό, με αποτέλεσμα να χρεωνόμαστε ρεύμα χωρίς λόγο. Επίσης, όταν έχουμε ηλεκτρικό εξοπλισμό συνδεδεμένο στην πρίζα μπορεί να προκληθούν και πολλά ατυχήματα όπως πχ το ηλεκτρικό βραχυκύκλωμα. Κατά συνέπεια, πρέπει να μην ξεχνάμε να αποσυνδέουμε την ηλεκτρική συσκευή από την πρίζα. Από την άλλη πλευρά, αν ξεχάσουμε να την αποσυνδέσουμε ενώ έχουμε φύγει από το σπίτι πρέπει να γυρίσουμε πάλι πίσω και να τραβήξουμε το βύσμα, έτσι όμως θα σπαταλήσουμε πολύτιμο χρόνο. Προκειμένου να βρεθεί μια λύση για αυτά τα προβλήματα, δημιουργήθηκε το smart home. Με την πρόοδο της τεχνολογίας, πολλά ερευνητικά έργα σχετικά με το smart home έχουν αναπτυχθεί προκειμένου να διευκολύνουν την ανθρώπινη ζωή και να βελτιώσουν την ποιότητα της. Ένα έξυπνο σπίτι (smart home), απαρτίζεται από την τεχνολογία που χρησιμοποιείται για να κάνει όλες τις ηλεκτρονικές συσκευές του σπιτιού έξυπνες (intelligenat).Η τεχνολογία αυτή είναι αυτοματοποιημένη και αποτελείται από διάφορες έξυπνες συσκευές όπως προηγμένα αυτόματα συστήματα για το φωτισμό, τη θερμοκρασία ελέγχου, ασφάλειας και πολλές άλλες λειτουργίες. Μια έξυπνη συσκευή είναι πολύ εύκολο να εγκατασταθεί και να χρησιμοποιηθεί από όλους έχοντας σκοπό να βελτιώσει πολλές πτυχές της καθημερινότητας μας. Τα

κυρίως μέρη που απαρτίζεται το έξυπνο σπίτι (smart home) είναι τρία (3), το δίκτυο, οι συσκευές ελέγχου και οι συσκευές αυτοματισμού της οικίας. Το δίκτυο που χρησιμοποιείται για τη σύνδεση του αυτοματισμού με τις συσκευές ελέγχου μπορεί να είναι ενσύρματο αλλά και ασύρματο. Οι συσκευές ελέγχου χρησιμοποιούνται για την διαχείριση των συστημάτων, και η συσκευή αυτοματισμού είναι συσκευή που ελέγχει το φυσικό περιβάλλον. Ωστόσο, θα αναλύσουμε αυτά τα τρία μέρη λεπτομερώς στην ενότητα που ακολουθεί.

Τι είναι το Smart Home

Με τον όρο Smart Home θεωρούμε οποιοδήποτε προσωπικό ή εργασιακό περιβάλλον που συμπεριλαμβάνει ένα σύνολο τεχνολογικών εφαρμογών με βασικό χαρακτηριστικό την αυτοματοποίηση και τον έλεγχο των επιμέρους τμημάτων του.

Το επίπεδο αυτοματοποίησης, καθώς επίσης και ο τρόπος ελέγχου διαφέρουν, αφού εξαρτώνται από αρκετές παραμέτρους. Ορισμένες από αυτές τις παραμέτρους είναι το κόστος, οι προσωπικές επιθυμίες των χρηστών, το είδος των αντικειμένων που πρόκειται να ελεγχθούν και ο τύπος του οικοδομήματος στο οποίο η τεχνολογία θα εγκατασταθεί.

Το Smart Home μάς δίνει τη δυνατότητα να ζούμε και να εργαζόμαστε σε απλοποιημένα και αναβαθμισμένα περιβάλλοντα, εξασφαλίζοντας μας παράλληλα τη μείωση των πάγιων εξόδων. Μελλοντικά, το κόστος των ηλεκτρικών και ηλεκτρονικών συσκευών και συστημάτων μειώνεται, έτσι ώστε οι αυτοματισμοί του σπιτιού ή και του Smart Home να μπορούν να αξιοποιηθούν. Γενικότερα η εύκολη εγκατάσταση, το χαμηλό κόστος συντήρησης, η αθόρυβη λειτουργία, η εξοικονόμηση ενέργειας, η άνεση και ο προσωπικός έλεγχος επί του οικιακού περιβάλλοντος από απόσταση αποτελούν μερικά από τα βασικά πλεονεκτήματα της αυτοματοποίησης. Η τεχνολογία του Smart Home, συμβάλλει στην απλοποίηση της καθημερινότητας των χρηστών, πρέπει να πληρεί συγκεκριμένες προϋποθέσεις, όπως:

- Τη διασφάλιση της ανθρώπινης ζωής και περιουσίας,

- Τη γνώση για τη διαχείριση της τεχνολογίας και
- Την επικοινωνία με το εξωτερικό περιβάλλον.

Ένα από τα βασικά χαρακτηριστικά της τεχνολογίας των Smart Home είναι ότι οι περιφερειακές μονάδες χρησιμοποιούνται για πολλαπλές χρήσεις. Παραδείγματος χάρην, οι αισθητήρες παρουσίας μπορούν να χρησιμοποιηθούν για τον έλεγχο του φωτισμού και του συστήματος θέρμανσης, ενώ ταυτόχρονα χρησιμεύουν και για το σύστημα του συναγερμού. Ακόμα ένα παράδειγμα αφορά την οθόνη της τηλεόρασης, η οποία μπορεί να προβάλλει και την εικόνα της θυροτηλεόρασης.

Τα σύγχρονα συστήματα που εφαρμόζονται στα Smart Home δίνουν την δυνατότητα στους ενοίκους για πάρα πολλές διευκολύνσεις και συμβάλλουν στην εξοικονόμηση πολύτιμου χρόνου. Οι παρεχόμενες διευκολύνσεις αυξάνονται καθώς, εκτός από τις βασικές λειτουργίες, δίνεται επίσης και η δυνατότητα στους ιδιοκτήτες των Smart Home να προγραμματίσουν το σύστημα και να δημιουργήσουν τα δικά τους σενάρια, προκειμένου να καλύψουν πλήρως τις δικές τους εξατομικευμένες ανάγκες. Τα σενάρια που μπορούν να εφαρμοστούν είναι άπειρα. Μερικά παραδείγματα, όσον αφορά στις συνήθεις λειτουργίες των Smart Home, παρουσιάζονται παρακάτω.

1. Φωτισμός:

Αυτοματοποιημένος φωτισμός που μειώνεται ή αυξάνεται κατά τη διάρκεια της ημέρας, προκατασκευασμένα σενάρια φωτισμού, αυτόματη απενεργοποίηση και ενεργοποίηση των φώτων.

2. Ασφάλεια:

Προστασία από πυρκαγιά, πλημμύρες, βραχυκυκλώματα,, ή οποιαδήποτε βλάβη. Σε αυτήν την περίπτωση, το Smart Home σημαίνει συναγερμό.

3. Έλεγχος θέρμανσης, κλιματισμού, αερισμού:

Δυνατότητα ρύθμισης εκ των προτέρων ή απομακρυσμένα της επιθυμητής θερμοκρασίας για το σπίτι. Οι ίδιες ρυθμίσεις μπορούν να γίνουν και για τον κλιματισμό - αερισμό, ενώ ακόμα υπάρχει η δυνατότητα αυτόματης ενεργοποίησης του εξαερισμού σε περίπτωση υψηλής συγκέντρωσης αερίων ή καπνού στο χώρο. Επίσης, η θέρμανση μπορεί να απενεργοποιείτε αν υπάρχει ανοιχτό παράθυρο ή

όταν θεωρείται περιττή.

4. Έλεγχος ηλεκτρικών περσίδων και τεντών:

Θα μπορούσαμε να εντάξουμε στην παραπάνω ενότητα, ωστόσο αποτελεί αυτοτελές τμήμα των συστημάτων ελέγχου ενός Smart Home. Οι περσίδες, τα παράθυρα και οι τέντες μπορούν να ανοίγουν και να κλείνουν ανάλογα με το φως, τον αέρα ακόμη και τη θερμοκρασία ρυθμίζοντας απόλυτα τις συνθήκες διαβίωσης.

5. Πολυμέσα:

Δυνατότητα διασύνδεσης ηχοσυστημάτων, τηλεοράσεων, τηλεφώνων είτε μεταξύ τους, είτε με άλλες «έξυπνες» συσκευές στο σπίτι. Συμπερασματικά, στο αυτοματοποιημένο περιβάλλον ενός Smart Home όλα τα συστήματα μπορούν να λειτουργήσουν αρμονικά μεταξύ τους, ρυθμίζοντας αυτόματα τις επιθυμητές συνθήκες διαβίωσης. Το κυριότερο είναι ότι μπορούμε να ελέγξουμε εξ ολοκλήρου την κατανάλωση της ενέργειας, εξοικονομώντας το μέγιστο δυνατόν, εφόσον η λειτουργία των συσκευών, του κλιματισμού, του φωτισμού και της θέρμανσης αποκλειστικά καθορίζεται από το χρόνο που μας είναι αναγκαία.

Το δίκτυο του Smart Home

Η τεχνολογία δικτύου του Smart home μπορεί να ταξινομηθεί σε δύο κύρια είδη, τα οποία είναι το ηλεκτρικό σύστημα και το ασύρματο σύστημα. Στο ηλεκτρικό σύστημα, ο εξοπλισμός θα πρέπει να συνδεθεί στην κύρια τροφοδοσία άμεσα, έτσι ώστε τα δεδομένα που αποστέλλονται στις συσκευές να ενεργοποιούνται ή να απενεργοποιούνται. Υπάρχουν πολλοί τύποι καλωδίων που μπορούμε να εγκαταστήσουμε σε έναν τοίχο. Πολλοί αυτοματισμοί του Smart Home συνδέονται μέσω καλωδίωσης όπως πχ οι οπτικές ίνες. Ένα παράδειγμα εξαιρετικής τεχνολογίας είναι το X10, το οποίο είναι ένα ανοικτό πρότυπο αυτοματισμού οικίας. Το X10 μεταδίδει δυαδικά δεδομένα χρησιμοποιώντας τη διαμόρφωση πλάτους (AM).Οι X10 ελεγκτές στέλνουν σήματα μέσω των υφιστάμενων AC καλωδιώσεων στο δέκτη. Πολλές όμως νέες συσκευές χρησιμοποιούν ασύρματη τεχνολογία και όχι το ηλεκτρικό σύστημα για να επικοινωνήσουν με άλλες συσκευές. Παραδείγματα ασύρματων τεχνολογιών είναι οι υπέρυθρες (IR), οι ραδιοσυχνότητες (RF), το Wi-Fi, το Bluetooth και ούτω καθεξής. Επίσης ορισμένες τεχνολογίες δικτύου smart

home μπορούν να λειτουργήσουν και με τους δύο τρόπους και με ηλεκτρικό άλλα και ασύρματο σύστημα. Ένα παράδειγμα ασύρματης επικοινωνίας για το smart home είναι το Z-κύμα, το οποίο είναι μια αξιόπιστη και προσιτή ασύρματη λύση οικιακού αυτοματισμού. Το Z-κύμα είναι μία ασύρματη RF based μέθοδος για άμεσο τηλεχειρισμό των συσκευών.

Συσκευές ελέγχου του Smart Home

Το έξυπνο σπίτι (Smart home) ελέγχει τις συσκευές που χρησιμοποιούνται για τη διαχείριση των συστημάτων του με την αποστολή δεδομένων ή την αποστολή σήματος στους ελεγκτές. Τα παραδείγματα των ελεγκτών δεν είναι μόνο το τηλεχειριστήριο, αλλά επίσης και κάποια έξυπνα αντικείμενα όπως πχ τα tablet (iPad, Galaxy tab), web browsers και Short Message Service (SMS). Επιπλέον, ορισμένα συστήματα μπορεί να έχουν ενσωματωμένο υπολογιστή που λειτουργεί ως κέντρο αντίληψης για το περιβάλλον ή τη μονάδα αξιολόγησης

Συσκευές αυτοματισμού του Smart Home

Μερικά παραδείγματα Smart συσκευών αναφέρονται στον παρακάτω πίνακα:

Οικιακές Συσκευές	Πόσο έξυπνες;
Ψυγείο	Ρυθμίζει την θερμοκρασία ψύξης με βάση τον όγκο των προϊόντων που περιέχει
Θερμοστάτης	Αλλαγές θερμοκρασίας με βάση τις τρέχουσες και προσεχείς καιρικές συνθήκες

Τηλεόραση	Προτείνει τηλεοπτικά σόου βασισμένα σε προηγούμενες επιλογές του χρήστη. Επίσης με το πρόγραμμα περιήγησης στο Διαδίκτυο θα μπορείς να ελέγχεις άλλες συνδεδεμένες συσκευές πχ θερμοστάτη, φωτισμό του χώρου και τη διανομή του ήχου
Πλυντήριο πιάτων - Στεγνωτήριο	Προσδιορίζει τη θερμοκρασία του νερού καθώς και την πλύση – ξέπλυμα βασισμένο στον όγκο φορτίου, την βρωμιά και την ώρα της ημέρας ενέργειας (Νυχτερινό ρεύμα, ώρες ξεκούρασης)
Εξοπλισμός πισίνας	Καθορίζει τα επίπεδα μόλυνσης και καταργεί τη σωστή ποσότητα χημικών ουσιών προσαρμόζει τη λειτουργία της αντλίας κυκλοφορίας και χλώριο ζωοτροφών με την ώρα της ημέρας και τις καιρικές συνθήκες.

I) Κουζίνα

Η κουζίνα είναι ο χώρος ο οποίος έχει λάβει τις μεγαλύτερες αναβαθμίσεις για ένα έξυπνο σπίτι (Smart Home). Για παράδειγμα, μερικές συσκευές που έχουν αναβαθμιστεί σε έξυπνες είναι τα ψυγεία, οι φούρνοι μικροκυμάτων, οι καφετιέρες και τα πλυντήρια πιάτων. Το smart ψυγείο εφαρμόζει την τεχνολογία του έξυπνου σπιτιού (smart home) και κάνει την καθημερινότητά μας πολύ πιο εύκολη. Συγκεκριμένα, συνδέεται στο Διαδίκτυο και επιτρέπει στους χρήστες να επικοινωνούν μαζί του, έτσι ώστε να είναι δυνατή η λήψη συνταγών και στη συνέχεια να τις εμφανίζει στην οθόνη LCD που διαθέτει. Επιπλέον, το smart ψυγείο κάνει επίσης μια αυτόματη απογραφή των ειδών στο εσωτερικό του και μπορεί να προειδοποιήσει τους χρήστες για το τι υπάρχει διαθέσιμο. Ακόμη υπάρχουν και

φούρνοι μικροκυμάτων που είναι επίσης smart. Οι smart φούρνοι μικροκυμάτων μπορούν να επικοινωνήσουν με το smart ψυγείο και να του προτείνουν συνταγές που βασίζονται στην είδη διατροφής που διατίθενται ήδη μέσα σε αυτό. Επίσης έχουν την δυνατότητα να ενεργοποιηθούν αυτόματα αν το επιλέξει ο χρήστης ενώ βρίσκεται μακριά από το σπίτι.

ii) Σαλόνι

Φεύγοντας από την κουζίνα κατευθυνόμαστε σε ένα άλλο μέρος του έξυπνου σπιτιού (Smart Home) το οποίο έχει λάβει αναβαθμίσεις, το σαλόνι. Έξυπνες συσκευές όπως τηλεοράσεις και ηχοσυστήματα χρησιμοποιούν αυτή την τεχνολογία για να βελτιώσουν την εμπειρία της ψυχαγωγίας. Το Smart TV, έχει πολλές λειτουργίες όπως του προσωπικού επιτραπέζιου υπολογιστή (Personal Computer) με αποτέλεσμα αυτό να οδηγεί στο να έχουμε μια διαδραστική τηλεόραση με διαδραστικό περιεχόμενο που πλέον υπάρχει ως επιλογή. Επιπλέον, το σύστημα ελέγχου φωτισμού μπορεί να χρησιμοποιηθεί για τον έλεγχο στα οικιακά ηλεκτρικά φώτα, χρησιμοποιώντας τους ανιχνευτές κίνησης. Τα φώτα μπορούν να σβήσουν αυτόματα στο δωμάτιο όταν κάποιος φύγει από αυτό και να ενεργοποιηθούν αντίστοιχα όταν κάποιος εισέλθει σε αυτό.

iii) Υπνοδωμάτιο

Το δωμάτιο διαθέτει Smart θερμοστάτη που οι χρήστες μπορούν να ρυθμίσουν την θερμοκρασία με ένα μόλις άγγιγμα. Επίσης μπορούν να επιλέξουν μια μόνιμη νυχτερινή θερμοκρασία και μόνιμο φωτισμό για κάθε υπνοδωμάτιο. Το κρεβάτι είναι επίσης εξοπλισμένο με αισθητήρες που μπορούν να παρακολουθούν την κίνηση του ατόμου στο κρεβάτι και να ανιχνεύουν την κατάσταση της υγείας το σχετικά με τον ύπνο. Ακόμη, οι Smart συσκευές μπορούν να χρησιμοποιηθούν και σε πολλές πτυχές, όπως για παράδειγμα:

- Υγεία: Μια ιατρική συσκευή σχεδιασμένη με ενσωματωμένο λογισμικό που βοηθά τους παρόχους υγείας να παρακολουθούν συνεχώς ασθενείς με εμφυτευμένο τσιπάκι ή άλλες ιατρικές συσκευές στο σπίτι τους χωρίς νοσηλεία στο νοσοκομείο ή ιατρικές επισκέψεις σε ιδιωτικά γραφεία.. Αυτά τα σπίτια με

ηλεκτρονικές συσκευές υγείας μπορούν να συλλέγουν αξιόλογα στοιχεία σχετικά με την τρέχουσα κατάσταση της υγείας για την πρόληψη των ασθενειών και τη συνολική ευεξία αυτών. Οι συσκευές αυτές μπορούν ακόμη και να χρηματοδοτηθούν εν μέρει ή πλήρως από τις ασφαλιστικές εταιρείες και την κυβέρνηση

- Ψυχαγωγία: Ο πλούτος του Internet είναι τώρα διαθέσιμος μέσω της τηλεόρασης, με τον οποίο αλλάζει ριζικά ο ορισμός του "περιεχομένου". Σήμερα οι εταιρείες μπορούν να δημιουργήσουν ανοικτές πλατφόρμες για νέες τηλεοράσεις που διαθέτουν ένα portal το οποίο περιέχει ψυχαγωγικό περιεχόμενο από πολυάριθμους τηλεοπτικούς σταθμούς

- Περιβάλλον: Απομακρυσμένος έλεγχος για τον φωτισμό την θέρμανση και τον κλιματισμό. Επίσης την κατανάλωση ενέργειας και του κόστους

- Ασφάλεια: Το έξυπνο σπίτι (smart home) μπορεί να βελτιώσει την αρχική ασφάλεια και να παρέχει μεγαλύτερη σιγουριά. Για παράδειγμα, οι αισθητήρες μπορούν άμεσα να ενημερώνουν τον ιδιοκτήτη ή την αστυνομία ή και την πυροσβεστική υπηρεσία. Οι υπηρεσίες αυτές μπορούν επίσης να εξουσιοδοτούν τα μέλη της οικογένειας να αποκτήσει έλεγχο της ασφάλειας των παιδιών από μακριά, την ευεξία των ηλικιωμένων. Επίσης μπορεί να ενημερώσει τον ιδιοκτήτη για πιθανές διαρροές αερίου και νερού.

- Υπενθυμίσεις: home ημερολόγιο, υπενθυμίσεις και επικοινωνία μέσα και έξω από το σπίτι

- Πράσινη Ενέργεια: Μείωση της ηλεκτρικής ενέργειας, κατανάλωση καυσίμου για την θέρμανση.

iv) Πόρτα γκαράζ

Ένα από τα πρώτα σημεία εισόδου μέσα σε ένα σπίτι συνήθως είναι το γκαράζ (υποθέτοντας, φυσικά, ότι το σπίτι έχει ένα γκαράζ). Έτσι λοιπόν το γκαράζ αποτελεί μια αρκετά καλή θέση για να τοποθετήσουμε έναν αισθητήρα, επειδή επίσης μπορούμε να εξασφαλίσουμε ότι η πόρτα του γκαράζ δεν είναι ανοικτή. Ο πρώτος αισθητήρας που θα εγκαταστήσουμε είναι ο αισθητήρας

ανοίγματος/κλεισίματος πορτών γκαράζ. Ο διακόπτης επαφής της πόρτας του γκαράζ τοποθετείται στις πόρτες γκαράζ, στα ρολά, ή και σε πύλες όπου είναι δύσκολο να τοποθετηθούν οι κοινές μαγνητικές επαφές. Οι μικρότερες επαφές (όπως αυτές που θα χρησιμοποιήσουμε στις πόρτες και τα παράθυρα στο σπίτι) έχουν ένα μικρό λειτουργικό κενό και πρέπει να είναι μέσα σε μισή ίντσα για να χρησιμοποιηθουν. Αυτές οι επαφές μπορούν να έχουν μέχρι και δύο ίντσες αποσταση και ακόμα να λειτουργούν. Ο αισθητήρας τοποθετείται στο τσιμεντένιο πάτωμα και διαθέτει βάση κατασκευασμένη από αλουμίνιο. Ο διακόπτης επαφών σφραγίζεται εντελώς στο εσωτερικό της βάσης. Ο μαγνήτης τοποθετείται στην πόρτα ή την πύλη σε ένα διευθετήσιμο υποστήριγμα τύπου L για την οριζόντια και κάθετη ρύθμιση. Έτσι ολοκληρώνουμε το σύστημα.. Η βάση των αισθητήρων είναι στρογγυλή ώστε τα οχήματα να μπορούν να την πατήσουν δίχως να προκαλέσουν ζημιά είτε στον αισθητήρα είτε στο όχημα. Ένα εύκαμπτο ανοξείδωτο θωρακισμένο καλώδιο 24-ίντσων χρησιμοποιείτε για την προστασία των καλωδίων καθώς είναι τοποθετημένα κατά μήκος του εδάφους

ν) Θερμοκρασία

Για να ελέγξουμε τη θερμοκρασία μιας περιοχής, χρησιμοποιούμαι τους αισθητήρες θερμοκρασίας. Οι αισθητήρες θερμοκρασίας διαφέρουν από τους θερμοστάτες επειδή οι αισθητήρες λειτουργούν ακριβώς όπως υπονοεί το όνομά τους - ανιχνεύουν δηλαδή τη θερμοκρασία, ενώ ένας θερμοστάτης είναι σε θέση να αντιδράσει στη δεδομένη θερμοκρασία (για παράδειγμα, να ανοίξει τον κλιματισμό όταν αυξάνεται η θερμοκρασία πάνω από ένα προκαθορισμένο όριο).

Οι αισθητήρες θερμοκρασίας επίσης έχουν τη δυνατότητα να συνδυαστούν με άλλους αισθητήρες ως μια ενιαία μμονάδα. Είναι σύνηθες για έναν αισθητήρα υγρασίας να συνδυαστεί με έναν αισθητήρα θερμοκρασίας. Επίσης τους αισθητήρες θερμοκρασίας μπορούμε να τους εγκαταστήσουμε είτε στο εσωτερικό είτε υπαίθρια (στον κήπο σας). Το σημαντικότερο ζήτημα στην εγκατάσταση αισθητήρων θερμοκρασίας είναι η τοποθέτηση τους. Επειδή αυτοί οι αισθητήρες διαβάζουν θερμοκρασίες και είναι ευαίσθητοι στις περιβαλλοντικές αλλαγές, δεν πρέπει να τοποθετήσετε τον αισθητήρα πάρα πολύ ψηλά (θα διαβάσει καυτό, καθώς ανεβαίνει ψηλά ο θερμός αέρας), και δεν πρέπει να τοποθετήσετε τον αισθητήρα πάρα πολύ χαμηλά (θα διαβάσει κρύο, καθώς κατεβαίνει χαμηλά ο κρύος αέρας). Επίσης,

πρέπει να κρατήσετε τον αισθητήρα μακριά από το άμεσο φως του ήλιου. Στο εσωτερικό του γκαράζ μπορούμε να τοποθετήσουμε έναν δεύτερο αισθητήρα θερμοκρασίας, κάτω από το πάτωμα της σοφίτας. Με αυτό τον τρόπο αποφεύγουμε να εκθέσουμε τον αισθητήρα από διάφορα στοιχεία και το άμεσο φως του ήλιου.

vi) Λουτρό

Όπως την έξυπνη κουζίνα, έτσι και το λουτρό δεν έχει πολλά ενσωματωμένα συστήματα εντούτοις, υπάρχουν μερικές έξυπνες συσκευές που εξυπηρετούν και έχουν χρήσιμους αλλά και χρηστικούς σκοπούς.

Τουαλέτα Flow Manager

Το FlowManager, χρησιμοποιείται για να ανιχνεύσει και να αποτρέψει τις υπερχειλίσεις και τις διαρροές στις τουαλέτες. Οι υπερχειλίσεις τουαλετών μπορούν όχι μόνο να είναι ακατάστατες και ενοχλητικές, μπορούν επίσης να προκαλέσουν ζημία στα πατώματα και στους τοίχους. Επιπλέον, οι υπερχειλίσεις μπορούν να προκαλέσουν την αύξηση άσχημων οσμών που μπορουν να οδηγησουν σε αλλεργικες αντιδράσεις,ακόμη και άσθμα.

Το FlowManager αποτρέπει αυτά τα προβλήματα με τη χρηση ενός αισθητήρα, που τοποθετείται στο εσωτερικό του πλαισίου των κυπέλλων της τουαλέτας. Όταν ο αισθητήρας κυπέλλων ανιχνεύει την αύξηση του νερού, στέλνει ένα σήμα σε έναν αισθητήρα στον κύριο ελεγκτή για να κλείσει τη ροή του νερου, και εκπέμπει έπειτα έναν ευδιάκριτο συναγερμό, που μας προειδοποιεί για το πρόβλημα.

Όταν έχουμε διαρροή νερού σε κάποιο σωλήνα ενεργοποιείται ένας αισθητήρας, που έχει τοποθετηθεί μέσα στη δεξαμενή, ο οποιος στέλνει σήμα στον κύριο ελεγκτή όταν ανιχνεύεται μια διαρροή.Μόλις σταλεί ένα σήμα προβλήματος στον κύριο ελεγκτή, το FlowManager αποκλείει το νερό μόνο στην τουαλέτα που υπάρχει το πρόβλημα ενώ οι υπόλοιπες υδραυλικές εγκαταστάσεις του σπιτιού λειτουργούν κανονικά. Όταν το πρόβλημα επιλυθεί, η κανονική ροή του ύδατος στην τουαλέτα αποκαθίσταται απλώς πατώντας ένα κουμπί. Εάν ο συναγερμός είναι ενοχλητικός σε σας και εργάζεστε για να επιδιορθώσετε το πρόβλημα, ο συναγερμός μπορεί να μπει σε αθόρυβη λειτουργία με το πάτημα ενός κουμπιού. Το FlowManager λειτουργεί

πολύ απλά χρησιμοποιώντας τέσσερις μπαταρίες.

Ενεργοποιημένος διανομέας σαπουνιών.

Όταν τα χέρια σας είναι ακάθαρτα και προσπαθείτε να πάρετε σαπούνι από το διανομέα, τα ακάθαρτα χέρια σας αφήνουν κάποιους λεκέδες στο διανομέα. Βέβαια, τα χέρια σας καθαρίζουν, αλλά όμως τώρα ο διανομέας είναι βρώμικος.

Μια λύση στο πρόβλημα είναι η χρήση ενός διανομέα χωρίς τη χρησιμοποίηση των χεριών. Έτσι λοιπόν ο ενεργοποιημένος διανομέας σαπουνιού διανέμει το σαπούνι στα χέρια σας χωρίς να χρειαστεί να έρθετε σε επαφή μαζί του. Απλώς πλησιάζετε τα χέρια σας κάτω από το στόμιο του και ο ενεργοποιημένος διανομέας σαπουνιού διανέμει το σαπούνι στα χέρια σας με μηδενική επαφή.

Αύτη η ιδιαίτερη κατασκευή λειτουργεί με μμπαταρία και είναι χρήσιμο όχι μόνο για το λουτρό του έξυπνου σπιτιού σας, αλλά θα μπορουσαν να τοποθετηθουν και στο γκαράζ ή οπουδήποτε αλλού θέλετε.Τα χαρακτηριστικά γνωρίσματά του περιλαμβάνουν τα παρακάτω: δυνατότητα να διανέμει το υγρό σαπούνι ή τη λοσιόν, χαμηλός δείκτης μπαταριών, παράθυρο για να δει το επίπεδο σαπουνιού ή λοσιόν,υπέρυθρος αισθητήρας, διανομέας διευθετήσιμος μεταξύ μιας έως τεσσάρων πτώσεων του υγρού. Η εγκατάσταση διαθέτει ένα απλό υποστήριγμα που τοποθετείται στον τοίχο, λειτουργεί με μπαταρίες και γεμίζει είτε με υγρό σαπούνι είτε με λοσιόν.

Θερμαινόμενα ράφια πετσετών

Τα θερμαινόμενα ράφια πετσετών, χρησιμοποιούνται στα ξενοδοχεία και στις ιαματικές πηγές εδώ και πολλά χρόνια, αλλά επίσης μπορούν να εγκατασταθούν και στο σπίτι σας.Οι θήκες πετσετών δεν είναι μόνο καλές λόγο ευκολίας, αλλά επίσης και για τη σωματική μας υγιεινή αφού μπορούν και μειώνουν την παρουσία των μικροβίων άλλα και του ιωδίου. Τα ηλεκτρικά θερμαινόμενα ράφια πετσετών χρησιμοποιούν ένα στοιχείο θέρμανσης το οποίο τρέχει το μήκος του ραφιού και επιτρέπει μια ομαλή θερμότητα που φτάνει γρήγορα μέχρι τη θερμοκρασία που

εμείς έχουμε ορίσει. Με σκοπό να κάνουμε αυτή τη συσκευή ακόμα εξυπνότερη, μπορούμε να συνδέσουμε το μαγκάλι πετσετών με μια συσκευή X10 έτσι ώστε το μαγκάλι πετσετών να ενεργοποιείται σε έναν προγραμματισμένο χρόνο.Για παραδείγμα, μπορούμε να προγραμματίσουμε τη συσκευή X10 να αρχίσει να λειτουργεί το ράφι πετσετών όταν ανοίγεται το φως λουτρών. Αυτά τα ράφια πετσετών όχι μόνο ειναι καλά για το έξυπνο σπιτι σας, αλλά επίσης ειναι χρήσιμα στα δωμάτια άσκησης και τα δωμάτια δίπλα στις ιαματικές πηγές, και τις λίμνες.Επίσης μπορούν να χρησιμοποιηθούν για τη θέρμανση των ενδυμάτων,των καλυμμάτων,για τους τήβεννους, ή ακομα και για την ξήρανση των ενδυμάτων που είναι πολύ λεπτά για τον οικιακό στεγνωτήρα.

vii) Δωμάτιο πλυντηρίων

Το δωμάτιο πλυντηρίων αποτελείτε από το πλυντήριο ρούχων και το θερμοσίφωνα. Όταν δημιουργηθεί υπερχείλιση αυτών των συσκευών, θα είμαστε τυχεροί εάν βγει λίγο νερό απλά στο πάτωμα. Σε μία χειροτερη περίπτωση το νερό μπορεί να καταστρέψει τις καλυμμένες με τάπητα περιοχές και να προκαλέσει ζημιά. Σε αυτό το τμήμα εξετάζουμε δύο τύπους αισθητήρων. Ο πρώτος τύπος είναι αυτόνομες μονάδες που αποκλείουν αυτόματα την συσκευή που εχει το προβλημα όταν αυτή προκαλεί διαρροή νερού επάνω στο πάτωμα. Ο δεύτερος χρησιμοποιείται από κοινού με ολόκληρο το σύστημα εσωτερικής αυτοματοποίησής (είτε πρόκειται για ένα έξυπνο σύστημα ασφάλειας, είτε για ένα σύστημα εγχώριας αυτοματοποίησης, ή για X10 συσκευές) και μας ενημερώνει που βρισκεται πρόβλημα.

Ανιχνευτής διαρροών πλυντηρίων ρούχων

Η ζημιά που προκαλείται από το ξεχείλισμα στα πλυντήρια ρούχων μπορεί εύκολα να περιοριστεί με την εγκατάσταση μιας αυτόματης εξυπνης βαλβίδας στη μηχανή. Αυτοί οι αισθητήρες ανιχνεύουν τη διαρροή του υδατος, κατόπιν κλείνουν αυτόματα τις βαλβίδες του νερού. Το FloodStop σύστημα I για παραδειγμα,εγκαθίσταται σε περίπου πέντε λεπτά, χρησιμοποιώντας απλα και μόνο ένα κατσαβίδι.

Εμπόδια στην υλοποίηση του Smart Home

Εμπόδιο Πρώτο: Ασφάλεια

Το έξυπνο σπίτι (Smart home) έρχεται επίσης με ορισμένες ανησυχίες για την ασφάλεια. Για παράδειγμα, οι χάκερ μπορούν να έχουν πρόσβαση στο δίκτυο, έτσι λοιπόν έχουν τη δυνατότητα να ελέγχουν όλες τις έξυπνες συσκευές.

Εμπόδιο Δεύτερο: Προσαρμογή στο νέο περιβάλλον

Όταν κατέχετε ένα έξυπνο σπίτι σημαίνει πως πρέπει να μάθετε πώς να χρησιμοποιείτε το σπίτι σας και ότι απαιτείται για να προσαρμοστείτε στις πολλές καινοτομίες γύρω σας, όπως τα συστήματα ασφαλείας και οι πολλοί αισθητήρες που πάντα θα ανιχνεύουν την κίνησή σας. Κατά συνέπεια, θα πρέπει να διαβάσετε τα εγχειρίδια που θα σας μάθουν πως να χρησιμοποιείτε το σπίτι σας.

Εμπόδιο Τρίτο: Υψηλό κόστος

Αν και τα έξυπνα σπίτια έχουν πολλά πλεονεκτήματα που καθιστούν την ανθρώπινη ζωή πιο άνετη, αυτά τα ίδια όμως πλεονεκτήματα έχουν υψηλό τίμημα. Το κόστος ενός έξυπνου σπιτιού είναι υψηλό, επειδή η τεχνολογία είναι σχετικά νέα.

Εν κατά κλείδι

Η ανάπτυξη των τεχνολογιών αυξάνεται και πολλά ερευνητικά προγράμματα έχουν αναπτυχθεί. Το έξυπνο σπίτι είναι κάτι περισσότερο από απλά ένα σπίτι που ελέγχεται από την κεντρική μονάδα αξιολόγησης ενός υπολογιστή. Με το έξυπνο σπίτι ο τρόπος με τον οποίο οι άνθρωποι ζουν προφανώς θα γίνει πιο αποτελεσματικός και άνετος. Θα έχουμε περισσότερο χρόνο για άλλες ασχολίες μιας που το σπίτι θα μπορεί να κάνει σχεδόν τα πάντα για εμάς. Επίσης, η τεχνολογία ενός έξυπνου σπιτιού (smart home technology) είναι μια καλή επιλογή για τους ανθρώπους που νοιάζονται για την ασφάλεια και την άνεση αλλά και την εξοικονόμηση ενέργειας. Τα έξυπνα σπίτια θα αποτελέσουν το μέλλον, διότι οι νέες τεχνολογίες αυξάνονται με καλπάζων ρυθμούς. Ένα από τα μελλοντικά έργα, είναι η δημιουργία μιας εφαρμογής υπολογιστή tablet ή smart phone με Android λειτουργικό σύστημα για τον έλεγχο των έξυπνων συσκευών με σκοπό την ευκολότερη και πιο άνετη ζωή.

iv) SMART CITY

Οι ‘έξυπνες πόλεις’ δημιουργούνται από τη σύγκλιση δύο μεγάλων ρευμάτων της σύγχρονης σκέψης για την πόλη και την αστική ανάπτυξη: αφενός του επαναπροσδιορισμού της πόλης μέσα από τις τεχνολογίες επικοινωνίας, την ψηφιακή δικτύωση και αναπαράστασή της, και αφετέρου από την κατανόηση της πόλης ως περιβάλλοντος δημιουργικότητας και καινοτομίας.

Ο όρος (intelligent cities / smart cities) χρησιμοποιείται για να χαρακτηρίσουμε περιοχές (πόλεις, περιφέρειες, συνοικίες πόλεων, clusters) στις οποίες το τοπικό σύστημα καινοτομίας υποστηρίζεται και αναβαθμίζεται μέσω ψηφιακών δικτύων και εφαρμογών. Με τη χρήση τεχνολογιών πληροφορικής και επικοινωνίας το σύστημα καινοτομίας αποκτά μεγαλύτερο βάθος και εμβέλεια, ενώ οι λειτουργίες του γίνονται περισσότερο διαφανείς και αποτελεσματικές. Η πόλη κερδίζει σε ικανότητα καινοτομίας, που μεταφράζεται σε ανταγωνιστικότητα και ευημερία. Δύο από τις πιο βασικές συνιστώσες των έξυπνων πόλεων είναι οι εξής:

- Το σύστημα καινοτομίας (τοπικό / περιφερειακό), το οποίο καθοδηγεί την ανάπτυξη γνώσεων και τεχνολογιών στους οργανισμούς της περιοχής (επιχειρήσεις, πανεπιστήμια, τεχνολογικά κέντρα, θερμοκοιτίδες, κ.α.), και

- Οι ψηφιακές εφαρμογές διαχείρισης πληροφορίας και γνώσεων, που διευκολύνουν την πληροφόρηση, την επικοινωνία, τη λήψη αποφάσεων, τη μεταφορά και εφαρμογή τεχνολογιών, τη συνεργασία στην καινοτομία, κ.α.

Παρά τη σαφή διασύνδεση με την κοινωνία της δημιουργικότητας και την κοινωνία της πληροφορίας, η έννοια της “έξυπνης πόλης” είναι ακόμη αμφιλεγόμενη. Σ’ αυτό συμβάλλουν τρεις λόγοι. Ταυτίσθηκε με ψηφιακές αναπαραστάσεις των πόλεων, τις ψηφιακές πόλεις, και χρησιμοποιήθηκε ισοδύναμα και εναλλακτικά με τους όρους “digital city” και “cyber city”. Εντούτοις, είναι βέβαιο ότι δεν αρκεί η επιπλέον δυνατότητα επικοινωνίας που προσφέρει μια ψηφιακή πλατφόρμα ή μια ψηφιακή αναπαράσταση της πόλης για να χαρακτηρισθεί ένα αστικό σύστημα ως ευφυές.

Μια δεύτερη πηγή σύγχυσης δημιουργήθηκε από τη μεταφορική χρήση του όρου ως κοινός τόπος ποικίλων ηλεκτρονικών πληροφοριακών συστημάτων και ψηφιακών

εφαρμογών επί των λειτουργιών των πόλεων. Το MIMOS (Malaysian Institute of Microelectronic Systems) για παράδειγμα, σημειώνει ότι στις μεταφορικές χρήσεις του όρου ‘intelligent city’ συμπεριλαμβάνονται οι έννοιες ‘invisible city', ‘information city’, 'wired city', 'telecity', ‘knowledge-based city', ‘virtual city’, ‘electronic communities’, 'electronic spaces', 'flexicity', ‘teletopia', 'cyberville', etc., στις περισσότερες από τις οποίες λείπουν στοιχεία ευφυΐας. Μια τρίτη πηγή σύγχυσης προέρχεται από την επικάλυψη με εφαρμογές ευφυούς περιβάλλοντος, όρος που χρησιμοποιείται για να χαρακτηρίσει διαδραστικούς χώρους που ενσωματώνουν υπολογιστικά συστήματα στο φυσικό χώρο και στους οποίους η υπολογιστική ισχύς χρησιμοποιείται απρόσκοπτα για να υποβοηθήσει τις καθημερινές δραστηριότητες.

1. Τρία επίπεδα μιας έξυπνης πόλης

Η ευφυής πόλη είναι ένα πολυεπίπεδο περιοχικό σύστημα καινοτομίας. Συνθέτει ανθρώπινες ικανότητες και δραστηριότητες έντασης-γνώσεων, θεσμούς τεχνολογικής μάθησης, και ψηφιακούς χώρους επικοινωνίας, ώστε να μεγιστοποιείται η ικανότητα καινοτομίας της περιοχής αναφοράς της. Αποτελεί την πιο εξελιγμένη μορφή περιοχικών συστημάτων καινοτομίας που γνωρίζουμε σήμερα, ένα σύστημα τρίτης γενιάς, μετά τα καινοτόμα clusters και τις μαθησιακές περιφέρειες. Συγκροτείται από την επαλληλία σειράς επιπέδων, σε αντιστοιχία με την εξέλιξη των διεργασιών της καινοτομίας σε φυσικό, θεσμικό, και ψηφιακό χώρο.

Επίπεδο Ι:

Είναι το επίπεδο βάσης και περιλαμβάνει τις δραστηριότητες έντασης-γνώσεων της πόλης. Πρόκειται για δραστηριότητες μεταποίησης και υπηρεσιών που (συνήθως) αυτόοργανώνονται σε συστάδες και συνοικίες (clusters). Η εγγύτητα στο φυσικό χώρο είναι το άμεσο συνδετικό στοιχείο που ενοποιεί τις επιμέρους μονάδες και οργανισμούς σε ένα ενιαίο σύστημα παραγωγής και καινοτομίας. Η ικανότητα καινοτομίας βασίζεται στην εξειδίκευση, την ατομική δημιουργικότητα, και τη συνεργασία μέσα στο cluster. Το επίπεδο αυτό συνδέεται άμεσα με τους ανθρώπους της πόλης: την ευφυΐα, εφευρετικότητα και τη δημιουργικότητά τους. Ταυτίζεται μ ε ότι περιέγραψε ο Richard Florida ως ‘νέα δημιουργική τάξη’, επιστημόνων,

καλλιτεχνών, επιχειρηματιών, επενδυτών κινδύνου, και άλλων ταλαντούχων και δημιουργικών ατόμων που συγκεντρώνονται σε μια πόλη και καθορίζουν τη διαδρομή ανάπτυξής της.

Επίπεδο ΙΙ:

Ένα δεύτερο επίπεδο περιλαμβάνει τους θεσμικούς μηχανισμούς κοινωνικής συνεργασίας για μάθηση και καινοτομία: θεσμοί και μηχανισμοί στρατηγικής πληροφόρησης, συγκριτικής αξιολόγησης, χρηματοδότησης κινδύνου, μεταφοράς τεχνολογίας, συνεργατικής ανάπτυξης νέων προϊόντων. Το επίπεδο αυτό σχετίζεται μ ε τη συλλογική ευφυΐα του πληθυσμού της πόλης, η οποία απορρέει από τους θεσμούς κοινωνικής συνεργασίας. Είναι η ευφυΐα ενός πληθυσμού, όπως αυτή κωδικοποιείται μέσα σε καθιερωμένες πρακτικές και καθημερινές ρουτίνες εργασίας

Επίπεδο ΙΙΙ:

Ένα τρίτο επίπεδο περιλαμβάνει τα ψηφιακά εργαλεία και εφαρμογές υποστήριξης της καινοτομίας, τα οποία δημιουργούν ένα εικονικό περιβάλλον χειρισμού της πληροφορίας και των γνώσεων. Το επίπεδο αυτό αφορά στο σύστημα τεχνητής ευφυΐας που είναι στη διάθεση του πληθυσμού της πόλης για να υποστηρίξει τόσο τις ατομικές επιλογές του, όσο και τη συλλογική επικοινωνία και συνεργασία. Πρόκειται για το δημόσιο σύστημα ψηφιακής επικοινωνίας, με ψηφιακά δίκτυα και υπηρεσίες, εφαρμογές τεχνητής ευφυΐας, ψηφιακούς χώρους και εργαλεία επίλυσης προβλημάτων, την επικοινωνία σε εικονικό περιβάλλον, το δημόσιο ψηφιακό περιεχόμενο που είναι στη διάθεση του πληθυσμού της πόλης

Η έννοια της ‘έξυπνης πόλης’ και το σχέδιο για την πραγματοποίησή της παραπέμπει και στις τρεις παραπάνω διαστάσεις του φυσικού, θεσμικού, και ψηφιακού χώρου της σύγχρονης πόλης: στους ανθρώπους, στους θεσμούς συνεργασίας, και στα ψηφιακά εργαλεία διαχείρισης γνώσεων και καινοτομίας. Μιλώντας επομένως κυριολεκτικά και όχι μεταφορικά, ο όρος ‘ευφυής πόλη’ χαρακτηρίζει ένα οργανισμό (κοινότητα, συνοικία, πόλη, περιφέρεια):

- Με αναπτυγμένες δραστηριότητες έντασης-γνώσεων, σε σχέση με τις οποίες αυτή μεταβάλλεται, προσαρμόζεται, και εξελίσσεται.

- Με θεσμούς και εμπεδωμένες ρουτίνες κοινωνικής συνεργασίας για την απόκτηση, προσαρμογή και ανάπτυξη γνώσεων και τεχνογνωσίας,

- Με αναπτυγμένο σύστημα επικοινωνίας και διαχείρισης γνώσεων, το οποίο επιτρέπει να συγκεντρώνει πληροφορία από το περιβάλλον, να την επεξεργάζεται, να μαθαίνει, και να προσαρμόζει ανάλογα τη δράση της,

- Με αποδεδειγμένη ικανότητα καινοτομίας, διαχείρισης και επίλυσης προβλημάτων που τίθενται για πρώτη φορά, καθώς η καινοτομία, η διαχείριση της αβεβαιότητας, η επίλυση νέων προβλημάτων, αποτελούν κρίσιμα μέτρα κάθε μορφής ευφυΐας.

2. Εφαρμογές: Κυβερνοπόλεις vs. έξυπνες κοινότητες

Δύο μεγάλες πρωτοβουλίες δημιουργίας έξυπνων πόλεων είναι σε εξέλιξη, υποστηριζόμενες από τα κινήματα για 'Smart Communities' και 'Intelligent Communities'

Το World Foundation for Smart Communities ξεκίνησε το 1997 και αποτέλεσε την πρώτη συστηματική προσπάθεια σύνδεσης των πόλεων με τις τεχνολογίες επικοινωνίας και πληροφορίας. «Μια έξυπνη κοινότητα είναι η κοινότητα που κάνει μια συνειδητή προσπάθεια να χρησιμοποιήσει τεχνολογίες πληροφορικής ώστε να μετασχηματίσει τη ζωή και εργασία στη περιοχή της με σημαντικό και ουσιαστικό τρόπο» (http://www.smartcommunities.org). Τα δομικά στοιχεία μιας Smart Community είναι τέσσερα:

- Ομάδα διοίκησης / χρήστες, που περιλαμβάνει τον συντονιστή, τους managers, και τους χρήστες. Οι ρόλοι τους διαφέρουν, όπως επίσης τα καθήκοντά και τα κίνητρά τους για την υλοποίηση της έξυπνης κοινότητας.

- Τεχνική δικτυακή υποδομή: Το δίκτυο περιλαμβάνει τα στοιχεία που κάνουν την επικοινωνία εφικτή, τις οπτικές ίνες, τις ασύρματες υποδομές, τις συνδέσεις, τα σημεία εισόδου, τις πλατφόρμες για τις εφαρμογές.

- Θεσμοί διαχείρισης, με τους κανονισμούς λειτουργίας της κοινότητας, τους στόχους που κινητοποιούν τα άτομα, τη ρύθμιση των προβλημάτων, τη

συμφωνία στη διαχείριση της υποδομής.

- Εφαρμογές: Είναι ο πυρήνας της έξυπνης πόλης που διευκολύνει / υποστηρίζει τις λειτουργίες της πόλης, τη διακυβέρνησή της, την επιχειρηματικότητα, την τηλε-εργασία, την εκπαίδευση από απόσταση, και άλλες ψηφιακές υπηρεσίες.

Τα Smart Communities είναι τυπικές κυβερνοπόλεις (cyber cities). Δημιουργούν ένα ψηφιακό χώρο, πάνω σε μια δικτυακή υποδομή, που προσφέρει υπηρεσίες διακυβέρνησης στον πληθυσμό της πόλης. Η έμφαση βρίσκεται στην ψηφιακή τεχνολογία και στον τρόπο που συνδέεται με τον φυσικό χώρο της πόλης. Περιγράφοντας τις σχέσεις ανάμεσα σε πόλεις και κυβερνοπόλεις, ο Pierre Levy οριοθετεί τέσσερις αρχές που διέπουν το νέο σύστημα διαδραστικής επικοινωνίας:

- Αναλογία στη μοντελοποίηση της cyber city, που οφείλει να απορρίψει την εύκολη αντιγραφή του φυσικού χώρου προς όφελος μιας αποτελεσματικής οργάνωσης του ψηφιακού χώρου.

- Υποκατάσταση λειτουργιών της πόλης, καθώς στις ψηφιακές πόλεις δεν απαιτείται η φυσική παρουσία των ανθρώπων.

- Ενσωμάτωση των νέων δικτύων μέσα σε παλιές υποδομές (σιδηροδρόμους, οδικές αρτηρίες, ενεργειακά και τηλεφωνικά δίκτυα).

- Άρθρωση πόλης και κυβερνοπόλης, καθώς οι διεργασίες μέσα στους δύο χώρους διαφέρουν ριζικά. «Ο πυρήνας του κυβερνοχώρου δεν είναι η κατανάλωση πληροφορίας και διαδραστικών υπηρεσιών, αλλά η συμμετοχή στις κοινωνικές διεργασίες της συλλογικής ευφυΐας».

Παράλληλη, αλλά και σημαντικά διαφορετική, είναι η πρωτοβουλία των Intelligent Communities. Υποστηρίζεται από το Intelligent Community Forum (ICF) που βραβεύει κάθε χρόνο τις καλύτερες εφαρμογές Ευφυών Πόλεων από όλο τον κόσμο (http://www.intelligentcommunity.org/). Παράλληλα έχει συμβάλλει στη διαμόρφωση ενός συστήματος μέτρησης που επιτρέπει την ποσοτική αξιολόγηση του ‘βαθμού ευφυΐας’ μιας πόλης. Η πιο σημαντική συμβολή του ICF βρίσκεται στη διασύνδεση της έννοιας της ευφυούς κοινότητας αφενός με την κοινωνία της

πληροφορίας και αφετέρου μ ε την οικονομία της γνώσης και της καινοτομίας. Για την επιλογή των καλύτερων περιπτώσεων χρησιμοποιεί πέντε κριτήρια αξιολόγησης:

- Επίπεδο ευρυζωνικών δικτύων.
- Εργασίες που βασίζονται στη γνώση.
- Ικανότητας καινοτομίας.
- Ψηφιακή σύγκλιση
- Προβολή και προώθηση της πόλης.

Τα πέντε κριτήρια κατανέμονται σε δύο κατηγορίες: δύο στο πεδίο της ευρυζωνικότητας, και τρία στο πεδίο της καινοτομίας και κοινωνίας της γνώσης. Με τα κριτήρια αυτά γίνεται σαφές ότι η δημιουργία μιας ευφυούς κοινότητας δεν είναι μόνο θέμα ψηφιακής τεχνολογίας, αλλά ενός συνθετότερου συστήματος γνώσεων και καινοτομίας. Εδώ βρίσκεται και η βασική διαφορά με τα cyber cities. Στην περίοδο 2000-2006 βραβεύθηκαν 23 πόλεις ως 'Intelligent Communities': ένδεκα στην Ασία (Bario, Singapore, Bangalore, Seoul, Taipei, Victoria, Yokosuka, Mitaka, Tianjin, Gangnam District Seoul, Ichikawa), εννέα στην Αμερική (LaGrange, Nevada, New York, Calgary, Florida high tech corridor, Spokane, Pirai, Toronto, Cleveland, Waterloo) και τρεις στην Ευρώπη (Ennis, Sundeland, Issy-les-Moulineux)

Η δημιουργία μιας έξυπνης πόλης είναι θέμα ανθρώπινων ικανοτήτων, θεσμών και ψηφιακών υπηρεσιών στο πεδίο της μάθησης, γνώσης, και καινοτομίας. Η ψηφιακή υποδομή στην οποία επενδύουν πολλές πόλεις είναι προϋπόθεση για την παροχή υπηρεσιών, αλλά δεν είναι απαραίτητο κάθε πόλη να κατασκευάσει το δικό της καλωδιακό ή ασύρματο δίκτυο. Πάνω στην καλωδιακή ή ασύρματη υποδομή τρέχουν οι ψηφιακές υπηρεσίες διαχείρισης γνώσεων. Αυτές συγκροτούν τον πυρήνα της συλλογικής ευφυΐας της πόλης. Στο URENIO έχουμε αναπτύξει πέντε πλατφόρμες για τη οργάνωση ψηφιακών υπηρεσιών για έξυπνες πόλεις σε κρίσιμα πεδία, όπως στρατηγική πληροφόρηση, απόκτηση τεχνολογίας, καινοτομία σε

συνεργασία, νέα επιχειρηματικότητα, προβολή και ψηφιακή παράδοση υπηρεσιών.

Εντέλει η ευφυΐα μιας πόλης βρίσκεται στην ολοκλήρωση των τριών επιπέδων που περιγράψαμε: των ικανοτήτων του πληθυσμού, των θεσμών συνεργασίας, και των ψηφιακών υπηρεσιών διαχείρισης γνώσεων και καινοτομίας. Εδώ τοποθετούνται και οι προκλήσεις σχεδιασμού έξυπνων πόλεων: στις μεθόδους και τεχνικές διασύνδεσης της ανθρώπινης, συλλογικής, και τεχνητής ευφυΐας που διαθέτει μια κοινότητα, με στόχο τη δημιουργικότητα και καινοτομία.

3. Τοπικά Δίκτυα Αισθητήρων στις «Έξυπνες πόλεις»

Πολλοί είναι οι παράγοντες και οι νέες τεχνολογίες που πρέπει να εφαρμοστούν και να συνεργαστούν αρμονικά μεταξύ τους, ώστε να επιτευχθεί η έξυπνη δικτύωση συσκευών. Θα πρέπει να υπάρξει η υλοποίηση σε τοπικό επίπεδο, στη συνέχεια θα πρέπει τα δεδομένα από πολλά τέτοια τοπικά δίκτυα να «βγουν» σε έναν κοινό τόπο (π.χ. cloud) και στη συνέχεια, να ανέβουν στο διαδίκτυο, ώστε να μπορούν να καταλήξουν σε τερματικά ελέγχου και απομακρυσμένης πρόσβασης.

Δικτύωση αισθητήρων

Στο επίπεδο της τοπικής δικτύωσης αισθητήρων, τα δεδομένα προέρχονται κατά κύριο λόγο από αισθητήρες (π.χ. επίπεδο στάθμης σε δεξαμενή), αλλά και από μονάδες ελέγχου προς ενεργοποιητές (π.χ. εντολή από τον κεντρικό πίνακα στην ηλεκτροβάνα για να κλείσει, ώστε να μην πλημμυρίσει η δεξαμενή). Συνεπώς, η ασφαλής μεταφορά των κρίσιμων αυτών δεδομένων, είναι μεγάλης σπουδαιότητας.

Επίσης, πολύ σημαντική απαίτηση είναι και η χαμηλή κατανάλωση. Η έννοια άλλωστε της «έξυπνης» πόλης, εμπεριέχει σίγουρα και αυτήν της «πράσινης» πόλης. Οι μη επαναφορτιζόμενες μπαταρίες για παράδειγμα, θα πρέπει να κρατάνε για χρόνια πριν ανακυκλωθούν. Επιπλέον τα «έξυπνα πλέγματα» (smartgrids), που εφαρμόζονται ολοένα και περισσότερο τα τελευταία χρόνια, όχι μόνο δίνουν μεγάλη βαρύτητα στη χαμηλή κατανάλωση, αλλά προχωράνε και ένα βήμα παραπάνω, στην παραγωγή δηλαδή ενέργειας (energy harvesting) χαμηλής ισχύος, από διάφορες πηγές (φως, δονήσεις, θερμοηλεκτρικές γεννήτριες κτλ). Η ενέργεια αυτή καταλήγει

σε μέσα αποθήκευσης όπως μπαταρίες ή πυκνωτές. Σε πολλές περιπτώσεις μάλιστα, κάποιοι αισθητήρες μπορεί να τροφοδοτούνται αποκλειστικά από τέτοιες πηγές ενέργειας. Επίσης, η ευελιξία είναι ακόμα ένα χαρακτηριστικό, το οποίο είναι απαιτητό στα δίκτυα αυτά και επιτυγχάνεται μέσω τεχνικών δικτύωσης που περιγράφονται παρακάτω. Τα ασύρματα δίκτυα αισθητήρων λοιπόν WSN (Wireless Sensor Networks), ενσωματώνουν μέσω κατάλληλων μηχανισμών τις παραπάνω απαιτήσεις, σχηματίζοντας τα λεγόμενα WPAN (Wireless Personal Area Networks). Πρόκειται δηλαδή για ένα δίκτυο αισθητήρων και ενεργοποιητών, οι οποίοι επικοινωνούν ασύρματα μεταξύ τους, αλλά και με την κεντρική μονάδα που υπάρχει συνήθως και η οποία διαθέτει σίγουρα επεξεργαστική ισχύ.

Τεχνολογία Plug-in

Μία σημαντική ικανότητα των δικτύων αυτών, είναι η χρήση της τεχνολογίας “plugging in”, όπου όταν δύο τοπικά δίκτυα βρίσκονται εντός εμβέλειας μεταξύ τους, μπορούν (ιδανικά) να επικοινωνούν, σαν να ήταν συνδεμένα με καλώδιο. Αυτό το επιτυγχάνουν περιορίζοντας ή ακόμα και διακόπτοντας κάποιες επικοινωνίες σε τοπικό επίπεδο, δίνοντας έτσι προτεραιότητα στην επικοινωνία μεταξύ των δικτύων. Πολύ γνωστά WPANs είναι τα Bluetooth, ZigBee, Mi-Wi, wireless USB, IrDA, Z-Wave, τα οποία συμμορφώνονται με το πρότυπο IEEE 802.15. Τα low rate WPANs (LR-WPANs), όπως είναι τα δίκτυα αισθητήρων, συμμορφώνονται με το πρότυπο IEEE 802.15.4, το οποίο καθορίζει το φυσικό επίπεδο (physical layer -PHY-) και το επίπεδο ελέγχου πρόσβασης μέσων (media access control -MAC- layer), των LR-WPANs. Τα υψηλότερα επίπεδα (πχ δικτύωση κόμβων) καθορίζονται από την εκάστοτε προδιαγραφή (πχ Bluetooth, ZigBee κτλ). Ως κρίσιμα χαρακτηριστικά μπορούμε να διακρίνουμε την ευελιξία, το χαμηλό κόστος, το χαμηλό επίπεδο πολυπλοκότητας και τη χαμηλή κατανάλωση.

Τεχνικά χαρακτηριστικά

Σε ό,τι αφορά τα τεχνικά χαρακτηριστικά, έχουμε χαμηλό data rate έως 250Kbps και διάφορες επιτρεπτές μπάντες λειτουργίας για Ευρώπη (868MHz), Αμερική (915MHz) και παγκόσμια χρήση (2400MHz), πρόσφατα δε και για Κίνα και Ιαπωνία. Επίσης οι κωδικοποιήσεις δεδομένων ποικίλλουν ανάλογα με την μπάντα και το κανάλι και μπορεί να είναι BPSK, ASK, O-QPSK, GFSK. Επίσης για να αποφευχθούν οι συγκρούσεις δεδομένων (και άρα η καταστροφή τους),

χρησιμοποιείται το πρωτόκολλο CSMS/CA (collision avoidance), όπου κάποιος κόμβος στέλνει μόνο εάν ανιχνεύσει ελεύθερη γραμμή, αλλιώς περιμένει κάποιο τυχαίο χρονικό διάστημα και ξαναπροσπαθεί. Η διευθυνσιοδότηση των κόμβων μπορεί να επιτευχθεί είτε με την 16-bit διεύθυνσή τους (short address), είτε με την 64-bit διεύθυνση (MAC address). Οι τοπολογίες του δικτύου μπορεί να είναι star, cluster tree ή mesh και επίσης οι κόμβοι χωρίζονται σε κόμβους πλήρους λειτουργικότητας (FFD), ή μειωμένης λειτουργικότητας (RFD). Άλλα χαρακτηριστικά που προβλέπονται από το IEEE 802.15.4: beaconing, εγγυημένα time slots, ED (Energy Detection), LQI (Link Quality Indication), δομή των πακέτων, τρόποι επικύρωσης ή απόρριψης των πακέτων, διαδικασίες εισαγωγής/εξαγωγής των κόμβων προς/από το δίκτυο (association) κ.α.

Κόμβοι

Οι κόμβοι διακρίνονται, όπως αναφέρθηκε, σε FFDs και RFDs. Σε ό,τι αφορά στον ρόλο του κάθε κόμβου στο δίκτυο, θα μπορούσε να είναι:

- COORDINATOR. Μία FFD συσκευή, ικανή να αναμεταδίδει μηνύματα.

- PAN COORDINATOR. Ο κυρίαρχος COORDINATOR του δικτύου. Είναι μοναδικός σε κάθε δίκτυο και είναι υπεύθυνος για να αρχικοποιήσει το δίκτυο κατά την εκκίνησή του. Χωρίς PAN COORDINATOR δεν μπορεί να γίνει εκκίνηση του δικτύου.

- DEVICE. Μία συσκευή FFD ή RFD, η οποία δεν συμπεριφέρεται ως COORDINATOR.

Από τις τρεις τοπολογίες (star, cluster tree και mesh), μεγάλο ενδιαφέρον παρουσιάζει η τοπολογία mesh, όπου όλες οι FFDs μπορούν να επικοινωνήσουν απευθείας μεταξύ τους, ενώ οι RFDs μπορούν να επικοινωνήσουν μόνο με FFDs. Οι coordinators μπορούν να αναμεταδώσουν τόσο unicast, όσο και broadcast. Σημαντικότατο χαρακτηριστικό είναι επίσης η χρήση της τεχνικής δρομολόγησης δεδομένων (routing), όπου τα μηνύματα αναπαράγονται επάνω σε ένα μονοπάτι, αναπηδώντας από κόμβο σε κόμβο (hopping), έως ότου φτάσουν στον προορισμό τους. Άρα, μπορούν με αυτόν τον τρόπο να ανταλλάξουν δεδομένα, δύο συσκευές

που μεταξύ τους είναι εκτός εμβέλειας. Άλλη μία πολύ σημαντική δυνατότητα είναι αυτή του συνεχούς επαναπροσδιορισμού του δρόμου μεταφοράς μηνυμάτων, μέσω αλγόριθμων «αυτοθεραπείας» (self healing algorithms), για κατεστραμμένους ή μπλοκαρισμένους για αναμετάδοση κόμβους. Τέλος τα ασύρματα mesh δίκτυα είναι "multihop", που σημαίνει ότι δεν υπάρχει ανάγκη για καλώδιο σε κανένα σημείο του δικτύου, σε αντίθεση με άλλα ασύρματα δίκτυα, τα οποία χρειάζονται οπωσδήποτε καλώδιο σε κάποιες βαθμίδες του δικτύου.

Δεδομένα σε cloud

Επομένως βάσει όλων των παραπάνω, μπορούμε να έχουμε ασύρματα δίκτυα αισθητήρων χαμηλής κατανάλωσης, τα οποία μέσω κατάλληλης δικτύωσης, να μπορούν να επικοινωνούν και μεταξύ τους, ακόμα και εάν πολλοί κόμβοι είναι εκτός εμβέλειας μεταξύ τους. Τα δεδομένα από αυτά τα δίκτυα μπορούν μέσω πυλών (gateways) να «βγουν» στο cloud. Τα δεδομένα από πολλά clouds και αυτά με τη σειρά τους, μπορούν μέσω routers να ανέβουν στο διαδίκτυο, ώστε όλα αυτά τα τοπικά δίκτυα να μπορούν να μιλάνε με μία ή περισσότερες απομακρυσμένες μονάδες, είτε απλά για εποπτεία, είτε και για απομακρυσμένο έλεγχο. Άρα καθίσταται προφανές ότι η δυναμική και οι δυνατότητες είναι πολύ μεγάλες, με τις προοπτικές επεκτασιμότητας να αποτελούν πραγματική πρόκληση. Τα smart grids για παράδειγμα, εφαρμόζονται ήδη σε αεροδρόμια, πάρκα, ΜΜΜ, τηλεπικοινωνίες κτλ.

Τέλος, σημαντικό είναι το ερώτημα πώς μπορούμε να καταλήξουμε στις έξυπνες πόλεις. Θα μπορούσε να υπάρξει τοπική δικτύωση σε επίπεδο κάποιου νοσοκομείου, εκπαιδευτικού ιδρύματος κ.λ.π. Στη συνέχεια, οι πληροφορίες από τα δίκτυα αυτά συνδυάζονται, ώστε να χρησιμοποιηθούν και σε ευρύτερες εφαρμογές. Για παράδειγμα, σε κάποιες πόλεις παρακολουθείται η κίνηση στους δρόμους και η πληρότητα των κάδων απορριμμάτων, ώστε τα απορριμματοφόρα να βγουν για αποκομιδή τις κατάλληλες ώρες όπου και όταν χρειάζεται, εξοικονομώντας έτσι καύσιμα, μην επιβαρύνοντας την κυκλοφορία και επιμηκύνοντας το χρόνο ζωής των οχημάτων. Άλλωστε στην «έξυπνη πόλη», θα υπάρχει σίγουρα συνετή διαχείριση των φυσικών πόρων, καθώς και δυνατότητα επίλυσης προβλημάτων με τη χρήση της τεχνολογίας πληροφοριών και επικοινωνιών, μέσω των οποίων υπάρχει σαφής βελτίωση του επιπέδου διαβίωσης των πολιτών. Αρκεί και ο πολίτης να

ανταποκριθεί και να είναι ώριμος να αξιοποιήσει στο έπακρο όλες αυτές τις δυνατότητες που του δίνονται και να αλληλεπιδράσει κατάλληλα, βοηθώντας με οικολογική ευσυνειδησία, ώστε να λειτουργήσει το σύστημα ακόμα πιο αποδοτικά.

4. Smart Parking

Το έργο SmartParking αναφέρεται σε μια εφαρμογή καθοδήγησης στάθμευσης σε πραγματικό χρόνο για τα smartphones. Το έργο αυτό στοχεύει στο σχεδιασμό, την ανάπτυξη και την εγκατάσταση μιας πλατφόρμας που αποτελείται από αισθητήρες, ενεργοποιητές, κάμερες και οθόνες για να προσφέρει χρήσιμες πληροφορίες σχετικά με ελεύθερες θέσεις στάθμευσης, μέσω διασκορπισμένων κόμβων λήψης σημάτων σε μια ευρύτερη περιοχή μιας πόλης. Η περιοχή αυτή χωρίζεται σε ζώνες, όπου σε κάθε ζώνη εγκαθίσταται μια πύλη (gateway) για να συγκεντρώσει τα δεδομένα. Κάθε πύλη έχει παραμετροποιημένες ρυθμίσεις που λειτουργούν σε διαφορετικές συχνότητες ώστε να μην αλληλεπιδρούν μεταξύ τους. Πειραματικά ένα σετ αισθητήρων εγκαταστάθηκε σε δρόμο της Πάτρας, για τη μέτρηση του μαγνητικού πεδίου για να ανιχνεύσει αν υπάρχουν ελεύθερες θέσεις στάθμευσης. Αισθητήρες ανίχνευσης μαγνητικού πεδίου (Σχήμα 1) μεταφέρουν δεδομένα μέσω της πύλης στο cloud server. Δυνητικά, η εγκατάσταση ενός πίνακα σε διάφορα σημεία της πόλης θα μπορούσε να παρουσιάζει και να ενημερώνει τους οδηγούς για τις ελεύθερες θέσεις πάρκινγκ, όπως αυτά ενημερώνονται ανά ορισμένο χρονικό διάστημα από το σύστημα.

Αρχή Λειτουργίας:

Το έξυπνο σύστημα SmartParking για έξυπνες πόλεις, είναι χτισμένο με τρία στρώματα: Αισθητήρες-, επίπεδο Επικοινωνίας και στρώμα εφαρμογής.

Ένας τρόπος για να επιτευχθεί αυτό είναι να έχει κάθε χώρο στάθμευσης αυτοκινήτων εξοπλισμένο με έναν αισθητήρα ο οποίος είναι σε θέση να ανιχνεύει την παρουσία ενός αυτοκινήτου σε αυτό. Ένας σταθμός πληροφόρησης (Gateways), που δραστηριοποιούνται στο χώρο στάθμευσης αυτοκινήτων, περιοδικά συλλέγει και αθροίζει τις πληροφορίες παρουσίας αυτοκίνητου από όλους τους αισθητήρες που αναπτύσσονται στην περιοχή, π.χ. μέσω Wi - Fi, ZigBee, ή άλλες ασύρματες τεχνολογίες μικρής εμβέλειας.

Μαγνητικοί αισθητήρες ανιχνεύουν αλλαγές στο μαγνητικό πεδίο όταν σε ένα χώρο στάθμευσης, σταθμεύσει ένα αυτοκίνητο. Εκείνη τη στιγμή ο αισθητήρας καταγράφει το γεωγραφικό μήκος και πλάτος και στέλνει το δεδομένο στην πύλη που βρίσκεται σε κοντινό σημείο εμβέλειας. Πρωτόκολλο IEEE 802.15.4 χρησιμοποιείται για τη διεξαγωγή πειραμάτων εντός του δικτύου.

Όταν η κατάσταση ενός πάρκινγκ αυτοκινήτων έχει αλλάξει, πληροφορίες σχετικά με αυτή προωθούνται από την πύλη στο χώρο στάθμευσης αυτοκινήτων στο σύννεφο και τον κεντρικό κόμβο. Συγκεντρωτικά δεδομένα συλλέγονται συνεχώς από τις τοποθετημένες πύλες και μέσω του cloud server, ενημερώνουν τον χάρτη πάνω στον οποίο αποτυπώνονται οι διαθέσιμες αλλά και κατειλημμένες θέσεις στάθμευσης.

Για να μπορεί να γίνει η λήψη δεδομένων από τον αισθητήρα, ο αισθητήρας πρέπει να είναι τοποθετημένος σταθερά κάτω από την επιφάνεια του δρόμου μέσα σε ένα αδιάβροχο περίβλημα. Σε αυτή την περίπτωση έχουν προταθεί και χρησιμοποιηθεί δυο λύσεις. Η μια λύση προβλέπει την τοποθέτηση του αισθητήρα κάτω από την επιφάνεια του δρόμου μέσα σε μια προστατευμένη οπή, γεγονός που σημαίνει αυξημένο κόστος, και εναλλακτικά την τοποθέτηση του αισθητήρα μέσα σε προστατευμένη πλαστική θήκη πάνω από την επιφάνεια του δρόμου. Στην πρώτη περίπτωση η λύση είναι πιο μόνιμη, με αυξημένο κόστος αλλά και πιο περίπλοκη διαδικασία αλλαγής των μπαταριών λειτουργίας, στη δεύτερη περίπτωση η τοποθέτηση και συντήρηση είναι γρήγορη, απλή, οικονομική, αλλά υπόκεινται πιθανώς σε περισσότερες μελλοντικές φθορές. Για την ανίχνευση της ακριβής θέσης ενός αισθητήρα, τοποθετείται ένας πομπός GPS (παγκόσμιο σύστημα εντοπισμού θέσης) που παρέχει ακριβή θέση και πληροφορίες για την ώρα. Στα πλαίσια βελτίωσης μεταφοράς του σήματος αλλά και για λόγους εφεδρείας, τα δεδομένα μπορεί να διαβιβάζονται τα μέσω GPRS / 3G. Κάθε πύλη συγκεντρώνει τα δεδομένα από όλους τους αισθητήρες εντός της ζώνης του, τα αποθηκεύει σε μια βάση δεδομένων MySQL και στέλνει τις πληροφορίες στο cloud server μέσω μιας σύνδεσης 3G. Οι πύλες, ιδεατά θα πρέπει να τοποθετούνται σε υψηλά σημεία για να μεγιστοποείται η περιοχή που καλύπτεται.

Το cloud αποθηκεύει τα δεδομένα και παρέχει υπολογιστικούς πόρους για την

υπηρεσία στάθμευσης αυτοκινήτων. Αποθηκεύει τα «big data» των χώρων στάθμευσης των αυτοκινήτων, των περιοχών που ελέγχονται για τις θέσεις αυτές, την ακριβή θέση των αυτοκινήτων, την τοποθεσία των χρηστών, κ.λπ. Η βαθμίδα του σύννεφου περιλαμβάνει, ένα υπολογιστικό μέρος που καταγράφει και πραγματοποιεί real-time updating της συμπεριφορά των χρηστών σε πραγματικό χρόνο, ενημερώνοντας συνεχώς το σύστημα για τα χαρακτηριστικά του χρήστη αλλά και ένα ασύγχρονο υπολογιστικό μέρος για τη μοντελοποίηση της εξόρυξης δεδομένων. Το μέρος συλλογή κατανεμημένων δεδομένων καταγραφής λειτουργεί ως αγωγός δεδομένων υψηλής ταχύτητας στο σύστημα.

Για τις ανάγκες της χωροθετικής ανάλυσης / παρουσίασης, έχει χρησιμοποιηθεί το QGIS, ένα ανοιχτού κώδικα λογισμικό GIS, ώστε η πληροφορία να αποτυπώνεται γεωγραφικά σε ένα πολύ εύκολο και εύχρηστο περιβάλλον και να διευκολύνει έτσι τους χρήστες μέσα από μια απλή εφαρμογή να παρακολουθούν την κατάσταση των χώρων στάθμευσης, αναζητώντας κάθε φορά με τα δικά τους προσωπικά κριτήρια, μέσα από τα layers που ενεργοποιούνται από τον χρήστη. Για την βελτιστοποίηση πόρων, ένας έξυπνος αλγόριθμός έχει αναπτυχθεί και ενσωματωθεί στο QGIS, που επεξεργάζεται τα εισερχόμενα δεδομένα και προτείνει τις «καλύτερες» θέσεις στάθμευσης αυτοκινήτων για τους χρήστες. Βασισμένο στο προφίλ κάθε χρήστη ο αλγόριθμος «εκπαιδεύεται» μέσω του εργαλείου KNIME, να μελετά παραμέτρους από το καταγεγραμμένο ιστορικό κινήσεων κάθε χρήστη και ανάλογα με τα δεδομένα της στιγμής να προτείνει τις βέλτιστες θέσεις σε κάθε χρήστη.

Εφαρμογή:

Όταν ένας χρήστης προσεγγίζει την περιοχή που έχει προεπιλέξει και στην οποία υπάρχουν εγκατεστημένοι αισθητήρες, μια αυτόματη αίτηση αποστέλλεται από την εφαρμογή (για λογαριασμό του χρήστη) στον κεντρικό κόμβο, ζητώντας ένα πάρκινγκ αυτοκινήτων. Ο διακομιστής βρίσκει το «καλύτερο» διαθέσιμο χώρο στάθμευσης αυτοκινήτων για το συγκεκριμένο χρήστη, με βάση τις προτιμήσεις του / της που ορίζονται στο προφίλ του χρήστη. Οι οδηγίες κατεύθυνσης στη συνέχεια αποστέλλονται στο χρήστη μαζί με ένα λεπτομερή χάρτη, π.χ., μέσω του API Android. Οι χρήστες μπορούν να αλληλεπιδρούν με το σύστημα εγκαθιστώντας την

αντίστοιχη εφαρμογή του χώρου στάθμευσης αυτοκινήτων στις κινητές συσκευές τους. Για μια κινητή συσκευή που δεν υποστηρίζει τεχνολογία GPS, μια υπηρεσία σύντομων μηνυμάτων (SMS) εμφανίζει τις πληροφορίες πάρκινγκ αυτοκινήτων στον χρήστη, έτσι ώστε να βρίσκεται συνεχώς ενημερωμένος ο χρήστης.

Στο επίπεδο εφαρμογών, ο κεντρικός κόμβος παρέχει cloud-based υπηρεσίες, διαχειρίζοντας μια πόλη μέσω ενός ολοκληρωμένου portal υπηρεσιών IoT. Αξιοποιώντας πλήρως τις χρήσεις των αισθητήρων και την πλατφόρμα επικοινωνίας, ένα πλήθος εφαρμογών θα μπορούσε να παρέχεται μέσω αυτού του συστήματος, στους χρήστες, που δεν περιορίζεται μόνο στην ανίχνευσης θέσης. Σε ένα πιο αυτοματοποιημένο σύστημα στάθμευσης, οι πληρωμές θα μπορούν να γίνονται ηλεκτρονικά, και η χρέωση ουσιαστικά να προκύπτει από την ανίχνευση της πινακίδας, και χαρακτηριστικών του κάθε αυτοκινήτου, με τη βοήθεια αισθητήρων εικόνας. Η παραπάνω χρήση θα μπορούσε να συνδυαστεί και με περιπολίες οχημάτων πινακίδα κυκλοφορίας, υπηρεσίες εντοπισμού αυτοκινήτων, κ.λ.π.

An IoT intelligent car parking system for a Smart City.

Διαφορετικές τεχνολογίες ανίχνευσης μπορούν να χρησιμοποιηθούν στο επίπεδο των αισθητήρων για ενσωματωμένες λύσεις στάθμευσης, όπως η αναγνώριση ραδιοσυχνοτήτων (RFID) για τον έλεγχο της πρόσβασης στάθμευσης αυτοκινήτων, λέιζερ, υπέρυθρες, ραντάρ μικροκυμάτων, υπέρηχοι, κλειστό κύκλωμα τηλεόρασης (CCTV) με επεξεργασία εικόνας βίντεο για την ανίχνευση της κατάστασης των χώρων στάθμευσης αυτοκινήτων, κ.α.

Μερικά παραδείγματα σημερινών έξυπνων πόλεων:

Σαν Φρανσίσκο

Στην καρδιά της πιο ζωντανής βιομηχανίας τεχνολογίας στον κόσμο, το Σαν Φρανσίσκο έχει υιοθετήσει τις καλύτερες δημιουργίες από τοπικές επιχειρήσεις, όπως Uber, Airbnb και Twitter. Επίσης έχει ήδη ψηφιστεί σε πολλές λίστες ως ένα από τα καλύτερα μέρη για να ζει κανείς. Ο δήμος έχει βάλει τα δυνατά του για να πετύχει τους αισιόδοξους στόχους του, η απασχολισιμότητα έχει ανέβει τρομερά. Χρησιμοποιούν όλες τις μορφές ενέργειας, κάνουν ανακύκλωση, βελτιώνουν κάθε τόσο τα μέσα μεταφοράς τους, μεγαλώνουν τα πεζοδρόμια και έχουν δωρεάν

εφαρμογές για τους πολίτες που τους ενημερώνουν για το πού υπάρχει κίνηση, ποια είναι η καλύτερη διαδρομή για συγκεκριμένους προορισμούς, ακόμη και το πρόγραμμα των δρομολογίων.

Open City Data: Η πόλη έχει διαθέσει σχεδόν 200 σύνολα δεδομένων στους προγραμματιστές, από τη δημόσια ασφάλεια έως και την υποδομή και εκείνοι έχουν δημιουργήσει περισσότερες από 60 εφαρμογές μέσων μεταφοράς. Οι εφαρμογές δημόσιας ασφάλειας περιλαμβάνουν την παρακολούθηση των πιο επικίνδυνων σημείων για τους πεζούς και χάρτη καθημερινής εγκληματικότητας.

Το *Connected Renewable Energy SF Energy Map Tool* συνδέεται με τις εγκαταστάσεις ηλιακής και αιολικής ενέργειας στην πόλη. Τα δεδομένα μεταφέρονται σε μια ιστοσελίδα που βοηθά τους ιδιοκτήτες κτιρίων να αντλήσουν στοιχεία και δεδομένα.

Smart Charging Station: Στην πόλη λειτουργούν 110 δημόσιοι σταθμοί φόρτισης ηλεκτρικών οχημάτων. Οι δικτυωμένοι σταθμοί επιτρέπουν στην πόλη να παρακολουθεί τη χρήση και την κατάσταση των φορτιστών. Οι χρήστες συνδέονται σε ειδική εφαρμογή για να βρουν τον πλησιέστερο σταθμό και να παρακολουθήσουν τα στατιστικά στοιχεία χρήσης.

Άμστερνταμ

Ο δήμος συνεργάζεται με κορυφαίες εταιρείες για να γίνει όσο το δυνατόν πιο οικολογικός! Τα σκουπίδια ανακυκλώνονται, οι στάσεις των λεωφορείων και τα φώτα των δρόμων φορτίζονται από τον ήλιο και πολλά σπιτικά και επιχειρήσεις χρησιμοποιούν πλέον την ηλιακή ενέργεια. Δισεκατομμύρια ευρώ έχουν εξοικονομηθεί και τα καλύτερα έρχονται...

Τόκιο

Το Τόκιο ετοιμάζεται να φυτέψει 1 εκατομμύρια δέντρα, να χρησιμοποιήσει στο μέγιστο την ηλιακή και την αιολική ενέργεια, ενώ όλο και περισσότεροι κάτοικοί του αγοράζουν υβριδικά ηλεκτρικά αυτοκίνητα. Δίπλα στο Τόκιο χτίζεται ένα οικολογικό χωριό από την Panasonic, στο οποίο οι κάτοικοι χρησιμοποιούν όλες τις μεθόδους εξοικονόμησης ενέργειας και έχουν μέχρι και εφαρμογή που τους

προτείνει την καλύτερη μέρα για να πλύνουν τα ρούχα τους έτσι ώστε να τα απλώσουν στον ήλιο...

Σινγιάνγκ

Η Σινγιάνγκ μας αφήνει άφωνους με τις καινοτομίες της. Αφήνοντας στην άκρη την απίστευτη ενημέρωση των κατοίκων για τις ώρες δρομολογίων λεωφορείων, μετρό, τρένων, του καιρού και της κίνησης, ο δήμος πηγαίνει ένα βήμα πιο πέρα. Ενισχύοντας την κοινωνική πρόνοια, τοποθετεί στα σπίτια των ηλικιωμένων κουμπί το οποίο μπορεί να το πατήσουν και άμεσα να βρεθεί εκεί κάποιος κοινωνικός λειτουργός. Επίσης υπάρχουν "έξυπνοι χάρτες" που δείχνουν σε ποιες περιοχές υπάρχουν περισσότερα περιστατικά εγκληματικότητας ή ανεργίας, έτσι ώστε ο δήμος να επέμβει...

Σιάτλ

Κάνει τεράστιες εκπτώσεις στη φορολογία σε όσες επιχειρήσεις γίνονται "green". Και αν δεν μπορεί κάποιος επιχειρηματίας να αντέξει τη μετάβαση από τον συμβατικό εξοπλισμό σε οικολογικό, το κράτος χρηματοδοτεί τα πάντα. Ενισχύονται οι πράσινες στέγες, τα οικολογικά κτήρια και επιδοτούνται όσοι αποφασίζουν να ασχοληθούν με τις κατασκευές τέτοιων κτηρίων ή να εργαστούν προς αυτή την κατεύθυνση.

Κοπεγχάγη

Η Δανία ασχολείται με αυτό που λέμε "urban planning" εδώ και 100 χρόνια, οπότε είναι λογικό οι πόλεις της να είναι μπροστά. Ένα τεράστιο κομμάτι της πόλης δόθηκε σε εταιρείες που ασχολούνται με την οικολογική τεχνολογία για να κάνουν τις δοκιμές τους! Επίσης, όταν δεν υπάρχει κίνηση στους δρόμους, τα φώτα σβήνουν. Υπάρχουν δίκτυα για τους ποδηλάτες, υπάρχουν εφαρμογές που ενημερώνουν για ελεύθερες θέσεις πάρκινγκ στους δρόμους και γενικώς ζηλεύουμε πολύ.

Στοκχόλμη

Γιατί χρηματοδοτεί οποιαδήποτε προσπάθεια για οικολογικότερες μεθόδους και γιατί μειώνει τους φόρους σε όσες επιχειρήσεις για παράδειγμα αντικαθιστούν τα φώτα τους με φώτα με σένσορες που κλείνουν όταν δεν υπάρχει κίνηση στο χώρο

(κι έτσι γίνεται εξοικονόμηση ενέργειας). Υπάρχουν 1.000 πάρκα (και αυξάνονται) και οι κάτοικοι ανακυκλώνουν τουλάχιστον 100 κιλά σκουπιδιών κάθε χρόνο.

Βιέννη

Θεωρείται από τους περισσότερους ως η πόλη με την καλύτερη ποιότητα ζωής, όχι μόνο στην Ευρώπη, αλλά γενικώς στον κόσμο. Κάτοικοι συνειδητοποιημένοι, οικολόγοι, που εξοικονομούν ενέργεια και ως επί το πλείστον χρησιμοποιούν τα μέσα μαζικής μεταφοράς.

Νέα Υόρκη

Η πιο πυκνοκατοικημένη πόλη στις ΗΠΑ, αγκάλιασε τα τελευταία χρόνια την έξυπνη τεχνολογία. Το Hudson Yards, η μεγαλύτερη ανάπτυξη ακινήτων στη Νέα Υόρκη από την εποχή του Rockefeller Centre, θα διαθέτει αισθητήρες που θα παρακολουθούν τα δεδομένα σχετικά με την κυκλοφορία, τα απορρίμματα, την ενέργεια και άλλους παράγοντες, καθιστώντας το μία από τις πιο «μετρήσιμες» κοινότητες που κατασκευάστηκαν ποτέ. Επίσης μπορείς να συνδεθείς στο Internet σχεδόν από παντού, γιατί έχουν τοποθετηθεί τεράστιες οθόνες σε κεντρικούς δρόμους που ενημερώνουν τους κατοίκους για την κίνηση, τον καιρό, ακόμη και τις εκδηλώσεις και γιατί ο δήμος χρηματοδοτεί τις εφαρμογές που κάνουν καλύτερη τη ζωή των κατοίκων της πόλης.

Networked Streetlights: Η πόλη μετατρέπει και τα 250.000 φώτα στο δρόμο σε LEDS, εξοικονομώντας με αυτό τον τρόπο $14 εκατομμύρια το χρόνο στον τομέα της ενέργειας. Τα LEDs μπορούν να δικτυωθούν ώστε τα φώτα να παρακολουθούνται, να απενεργοποιούνται ή να ενεργοποιούνται όταν ανιχνεύεται κίνηση.

Smart Bikes: Το πρόγραμμα Citi Bike διπλασιάζεται σε μέγεθος και έχει γίνει αναπόσπαστο κομμάτι της ζωής της Νέας Υόρκης. Οι σταθμοί ποδηλάτων συνδέονται με εφαρμογές κινητού που επιτρέπουν στους χρήστες να δουν πόσα ποδήλατα είναι διαθέσιμα σε κάθε σταθμό. Το GPS σε κάθε ποδήλατο ανιχνεύει την τοποθεσία του ποδηλάτου και συγκεντρώνει στοιχεία για κάθε διαδρομή.

Βαρκελώνη

Η Βαρκελώνη, με το Barri Gotic, τις παραλίες και την περίφημη ομάδα ποδοσφαίρου, υπήρξε μία από τις πιο επιθετικές πόλεις στον κόσμο όσον αφορά την υιοθέτηση έξυπνων τεχνολογιών και του Internet of Everything. Η Ευρωπαϊκή Ένωση ανέφερε τη Βαρκελώνη ως την πιο καινοτόμο πόλη της Ευρώπης.

Smart Lighting: Τα φώτα LED που διαθέτουν αισθητήρες μπορούν να ανιχνεύσουν την κίνηση, τον καιρό, τη ρύπανση και το θόρυβο. Τα φώτα μπορούν να ελέγχονται εξ αποστάσεως, να ενεργοποιούνται ή να απενεργοποιούνται. Τα δεδομένα από τους αισθητήρες μπορούν να βοηθήσουν στον εντοπισμό αυξημένης κυκλοφοριακής κίνησης καθώς και στη βελτίωση της ασφάλειας.

Smart Parking: Ανιχνευτές φωτός και μετάλλων εγκατεστημένοι σε κάθε θέση στάθμευσης του δρόμου γνωρίζουν εάν ο χώρος είναι κατειλημμένος. Οι οδηγοί λαμβάνουν πληροφορίες σε πραγματικό χρόνο σχετικά με τις διαθέσιμες θέσεις στάθμευσης σε έναν έξυπνο χάρτη τηλεφώνου. Δεδομένα σχετικά με τα μοτίβα πάρκινγκ, βοηθούν την πόλη να σχεδιάσει καλύτερους δρόμους και χώρους στάθμευσης.

Smart Bus Stops: Οθόνες αφής που τροφοδοτούνται με ηλιακή ενέργεια δείχνουν τους χρόνους άφιξης και τις διαθέσιμες θέσεις του επόμενου λεωφορείου. Επιπλέον προσφέρουν τουριστικές πληροφορίες και δωρεάν Wi-Fi. Τα λεωφορεία διαθέτουν GPE, αισθητήρες θέσεων, και στέλνουν πληροφορίες στη στάση του λεωφορείου.

Ριο Ντε Τζανέιρο

Το Κέντρο Επιχειρήσεων της πόλης του Ρίο ενσωματώνει δεδομένα από 30 φορείς της πόλης, δημιουργώντας ένα εικονικό Ρίο που δείχνει την κίνηση του μετρό και των οχημάτων, διακοπές ρεύματος και τις καιρικές συνθήκες σε όλη την πόλη. Καθώς το Ρίο πλησιάζει τους Θερινούς Ολυμπιακούς Αγώνες του 2016, οι υπεύθυνοι ευελπιστούν πως οι έξυπνες τεχνολογίες θα βοηθήσουν στην αντιμετώπιση των περισσότερων προβλημάτων της πόλης.

Smart Carnaval: Δεδομένα από 18 φορείς της πόλης και χάρτες συνδυάστηκαν για να προγραμματίσουν 425 κινητά συγκροτήματα σάμπα σε 350 τοποθεσίες κατά τη

διάρκεια του ετήσιου Καρναβαλιού. Δεδομένα σε πραγματικό χρόνο συνδυάζουν ασφάλεια, καθαρισμό των δρόμων και έλεγχο του πλήθους. City Data Feeds: Καθώς το Κέντρο Λειτουργίας αναλύει τον καιρό και την κίνηση, στέλνει ειδοποιήσεις στις φορητές συσκευές των πολιτών. Αυτό θα υποστηρίξει την κίνηση εκατομμυρίων επισκεπτών κατά τη διάρκεια των Ολυμπιακών Αγώνων. Micro-Weather Prediction: Το μαθηματικό μοντέλο του Ρίο συλλέγει δεδομένα από το ποτάμι και τα ιστορικά αρχεία καταγραφής βροχοπτώσεων και προβλέπει πλημμύρες και επιπτώσεις του καιρού στην κυκλοφορία και το ηλεκτρικό δίκτυο.

Σιγκαπούρη

Η Σιγκαπούρη έχει εγκαταστήσει ένα δίκτυο αισθητήρων, καμερών και συσκευών που παρακολουθούν από την ποσότητα του διοξειδίου του άνθρακα που απορροφούν τα δέντρα, έως την κυκλοφοριακή συμφόρηση και την κατάσταση των κτιρίων.

Super Wi-Fi: Η Σιγκαπούρη δημιουργεί ασύρματα δίκτυα που έχουν μεγαλύτερη κάλυψη, αλλά απαιτούν λιγότερη ισχύ από ένα καθιερωμένο Wi-Fi. Το ασύρματο δίκτυο θα χρησιμοποιηθεί επίσης για τη μετάδοση των δεδομένων που θα παράγει η πόλη.

Air Quality Monitors: Δικτυωμένοι αισθητήρες ανιχνεύουν ρύπους, υγρασία, επίπεδα διοξειδίου του άνθρακα και άλλους ατμοσφαιρικούς παράγοντες. Τα στοιχεία αποστέλλονται πίσω στα κεντρικά συστήματα για ανάλυση. Building Sensors: Αισθητήρες σε δημόσια κτήρια ανιχνεύουν σεισμικές δονήσεις και στέλνουν μηνύματα σε πραγματικό χρόνο στους μηχανικούς της πόλης, για να ζητήσουν επιθεωρήσεις συγκεκριμένων κτιρίων.

Τρίκαλα

Τα Τρίκαλα αποτελούν την πρώτη ψηφιακή πόλη της Ελλάδας, υλοποιώντας νέες τεχνολογίες με επιτυχία στα διάφορα Δημοτικά έργα. Βασικοί στόχοι της πόλης είναι, η βελτίωση της καθημερινότητας των πολιτών σε μία μεσαίου μεγέθους πόλη, η απλούστευση των καθημερινών τους συναλλαγών, η μείωση στα τηλεπικοινωνιακά κόστη και η προσφορά νέων υπηρεσιών. Λεωφορεία χωρίς οδηγό: Το Ευρωπαϊκό πρόγραμμα CityMobil2, αφορά στη διερεύνηση των δυνατοτήτων

κυκλοφορίας οχήματος χωρίς οδηγό σε Αστικό Περιβάλλον με πραγματικές συνθήκες κυκλοφορίας. Η πρόταση της πόλης των Τρικάλων για συμμετοχή στο πρόγραμμα, συγκέντρωσε την υψηλότερη βαθμολογία ανάμεσα στις 11 υποψήφιες πόλεις ανά την Ευρώπη. Η πόλη αποτελεί πλέον Ευρωπαϊκό πιλότο για την κυκλοφορία των οχημάτων χωρίς οδηγό. Η επίσημη παρουσίαση και έναρξη κυκλοφορίας των οχημάτων είναι στις ΧΧ Σεπτεμβρίου 2015.

Υποδομές:

- 35 χλμ. εγκατεστημένης οπτικής ίνας.
- 34 ασύρματοι κόμβοι δωρεάν πρόσβασης στο διαδίκτυο για περισσότερους από 10.000 κατοίκους και επισκέπτες.
- 900 θέσεις e-parking.
- 5 επαγωγικοί βρόγχοι μέτρησης κυκλοφοριακών δεδομένων.
- 20 δημοτικά οχήματα και 25 αστικά λεωφορεία εξοπλισμένα με Σύστημα Γεωγραφικών Πληροφοριών (GIS).
- Ασύρματη ζεύξη 4 σχολικών συγκροτημάτων.
- 200 επωφελούμενοι από το πρόγραμμα τηλεπρόνοιας.
- 31 καθετοποιημένες εφαρμογές σε λειτουργία.

Santander

Στο Santander μέχρι το τέλος του έργου τον Δεκέμβριο του 2013, θα έχουν εγκατασταθεί περίπου 20.000 αισθητήρες διαφόρων τύπων: στάθμευσης σε δρόμους, έντασης κίνησης στις εισόδους της πόλης, θορύβου, ποιότητας του αέρα (CO, όζον, σωματίδια) πάνω σε λεωφορεία, θερμοκρασίας, υγρασίας σε πάρκα, κλπ. Σημαντική συμβολή έχουν και οι ίδιοι οι πολίτες που με εφαρμογές στα κινητά τους τηλέφωνα, μπορούν και ενημερώνουν τους άλλους συμπολίτες τους και τις δημοτικές αρχές σχετικά με συμβάντα ή συνθήκες που έχουν ενδιαφέρον.

Πρόβλεψη ελεύθερων θέσεων στάθμευσης: Η αυτοματοποιημένη παρακολούθηση θέσεων στάθμευσης σε δρόμο (on-street parking) αποτελεί μια υπηρεσία που μέχρι πρόσφατα δεν ήταν εύκολο να υλοποιηθεί. Στο Santander έχουν εγκατασταθεί στο οδόστρωμα εκατοντάδες ασύρματοι αισθητήρες στάθμευσης

«Έξυπνη πόλη» της Bosch

Κατά τη διάρκεια του φετινού Consumer Electronics Show η Bosch παρουσίασε τις τεχνολογίες εκείνες που φέρνουν συνδεσιμότητα όχι μόνο για τα διαμερίσματα και τα σπίτια, αλλά και για ολόκληρες πόλεις. Πιο αναλυτικά, η Bosch παρέχει τη δυνατότητα της πραγματοποίησης των οραμάτων του μέλλοντος μέσω πέντε πιλοτικών έργων. Μέχρι το 2050 έξι δισεκατομμύρια άνθρωποι θα ζουν στις πόλεις. «Οι έξυπνες πόλεις βελτιώνουν την ποιότητα ζωής των κατοίκων τους, καθώς και την οικονομική αποδοτικότητα των ίδιων των πόλεων. Γι' αυτό, θέλουμε να καταστήσουμε τις πόλεις πιο ευφυείς», είπε ο Διευθύνων Σύμβουλος της Bosch Dr. Volkmar Denner, μιλώντας σε συνέντευξη Τύπου της εταιρίας στο CES 2016 στο Λας Βέγκας. Οι προσπάθειες αυτές θα δώσουν έμφαση στην κινητικότητα, υποδομή, ενέργεια, και ασφάλεια. Είτε πρόκειται για τη σύνδεση διαφόρων τρόπων μεταφοράς – όπως τα τρένα, τα λεωφορεία, και η συλλογική χρήση των Ι.Χ. – είτε για τη διαχείριση των σημάτων κυκλοφορίας και του φωτισμού των πόλεων, ο στόχος, είπε, είναι η παροχή καλύτερης ποιότητας ζωής στους κατοίκους των πόλεων, και κατά συνέπεια μεγαλύτερη ευκολία και ασφάλεια, εξασφαλίζοντας ταυτόχρονα τη διατήρηση των πόρων. Το καλύτερο παράδειγμα αποτελεί ο αυτόματος φωτισμός: αν ο δρόμος είναι άδειος οι φωτεινοί σηματοδότες χαμηλώνουν, αλλά μόλις εμφανίζεται κόσμος τα φώτα γίνονται πιο έντονα. Αυτή η αρχή είναι παρόμοια με το μηχανισμό που διαθέτουν ορισμένες κυλιόμενες σκάλες, οι οποίες αρχίζουν να κινούνται μόνο μόλις πατήσει κάποιος επάνω τους. Αναμένεται επίσης ότι τα έξυπνα κτίρια που προσαρμόζουν αυτόματα τη θερμοκρασία, την ποιότητα αέρα και το φωτισμό τους θα καταστούν ο κανόνας σε όλο τον κόσμο. Με τη μορφή της IoT Suite της Bosch, η εταιρεία προσφέρει ένα από τα δομικά στοιχεία για την έξυπνη πόλη. Πρόκειται για μια πλατφόρμα λογισμικού που ενσωματώνει όλες τις λειτουργίες που είναι απαραίτητες για τη σύνδεση συσκευών, χρηστών και υπηρεσιών – συμπεριλαμβανομένων των ηλεκτρικών δικτύων, φωτισμών, σημάτων κυκλοφορίας και οχημάτων. Είναι επίσης δυνατόν να συνδεθεί το σύνολο της υποδομής, όπως τα μέσα μαζικής μεταφοράς ή κλειστοί χώροι στάθμευσης, ώστε να

υπάρχει η δυνατότητα του έξυπνου ελέγχου μέσω της IoT Suite.

Ένα κλικ και το όχημα θα βρίσκει το δικό του χώρο στάθμευσης

Η κινητικότητα είναι ο παλμός της κάθε πόλης. Αλλά όλο και περισσότερα αστικά κέντρα βρίσκονται σε κίνδυνο αδιεξόδου – όπως μπορεί να επιβεβαιώσει κάθε οδηγός που έχει περάσει ώρες κολλημένος σε μποτιλιάρισμα ή που προσπαθεί να βρει χώρο στάθμευσης. Η Bosch βοηθά τις έξυπνες πόλεις και τα συνδεδεμένα οχήματα στην εύρεση δωρεάν χώρων στάθμευσης της προσέγγισής τους. Η εταιρεία απαλλάσσει επίσης τους οδηγούς από τη διαδικασία της στάθμευσης των αυτοκινήτων τους. Σύντομα το μόνο που θα χρειάζεται είναι το πάτημα ενός κουμπιού ώστε τα αυτοκίνητα να βρίσκουν το δικό τους χώρο στάθμευσης. Εφόσον βρεθούν σε κάποιο πάρκινγκ, τα οχήματα θα εισέρχονται στις θέσεις στάθμευσης και θα εξέρχονται από αυτές αυτόνομα. Το μόνο που θα πρέπει να κάνουν οι οδηγοί είναι ακουμπήσουν με το δάχτυλό τους τη σχετική εφαρμογή κινητού τηλεφώνου.

Οι θέσεις φόρτισης αποτελούν μέρος του IoT

Οι οδηγοί ηλεκτρικών ή plug-in υβριδικών οχημάτων χρησιμοποιούν ήδη εφαρμογές κινητού τηλεφώνου για τον εντοπισμό μιας δωρεάν θέσης φόρτισης όπου θα μπορούν να επαναφορτίσουν τις μπαταρίες τους. Και όχι μόνο αυτό: μόλις ένα κλικ ακόμα και μπορούν να πληρώσουν επίσης για την ηλεκτρική ενέργεια που καταναλώνουν. Η Bosch έχει συνεργαστεί με μια αυτοκινητοβιομηχανία για την ανάπτυξη μιας τέτοιας εφαρμογής κινητού τηλεφώνου και τώρα την παρέχει στους οδηγούς ηλεκτρικών οχημάτων. Η εφαρμογή καλύπτει σχεδόν όλες τις δημόσιες θέσεις φόρτισης στη Γερμανία, με την τακτή προσθήκη θέσεων φόρτισης σε άλλες χώρες.

ΚΕΦΑΛΑΙΟ 3

ΠΡΟΒΛΗΜΑΤΑ ΠΟΥ ΠΡΟΚΥΠΤΟΥΝ ΜΕ ΤΟ IoT

Είναι αδύνατον να καλύψουμε το ευρύ πεδίο φάσματος των προβλημάτων γύρω από το IoT σε ένα ενιαίο έγγραφο. Θα προσπαθήσουμε όμως, να κάνουμε μια γενική επισκόπηση γύρω από τα πέντε πιο συχνά συζητημένα θέματα σε σχέση με το IoT. Σε αυτά μέσα περιλαμβάνονται τα εξής:

- Εγγύηση.
- Απόρρητο.
- Διαλειτουργικότητα προτύπων.
- Νομικά ζητήματα.
- Αναπτυσσόμενες οικονομίες.

Ξεκινήσαμε να εξετάζουμε αυτά τα θέματα μέσα από τις «ικανότητες» του IoT. Η δήλωση των θεμελιωδών αρχών που καθοδηγούν εργασίες του ISOC όσον αφορά τις δυνατότητες, θέλουμε να πιστεύουμε όλοι οι χρήστες του Διαδικτύου ότι πρέπει να προστατεύονται. Αυτές περιλαμβάνουν τη δυνατότητα να συνδεόμαστε, να μιλάμε, να μοιραζόμαστε, να επιλέγουμε και να εμπιστευόμαστε. Με τις αρχές αυτές ως οδηγό, σας παρουσιάζουμε σημαντικές πτυχές της κάθε έκδοσης και προτείνουμε αρκετές ερωτήσεις για συζήτηση.

ΠΡΟΒΛΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Προκλήσεις ασφαλείας του IoT

Όπως διαπιστώνουμε από τις αρχές που καθοδηγούν την πτυχιακή μας, εξασφαλίζοντας την ασφάλεια, την αξιοπιστία, την ανθεκτικότητα και τη σταθερότητα των εφαρμογών Internet και υπηρεσιών, είναι απαραίτητα μέτρα για την προώθηση της εμπιστοσύνης και της χρήσης του Διαδικτύου. Ως χρήστες του Διαδικτύου, θα πρέπει να έχουμε έναν υψηλό βαθμό εμπιστοσύνης ότι το Διαδίκτυο, οι εφαρμογές και οι συσκευές που συνδέονται σε αυτό, είναι αρκετά ασφαλής για τα

είδη των δραστηριοτήτων που θέλουμε να κάνουμε σε αυτό. Το IoT δεν διαφέρει πολύ από την άποψη αυτή, καθώς η ασφάλεια του συνδέεται άμεσα με την ικανότητα των χρηστών να εμπιστεύονται το περιβάλλον χρήσης του. Εάν οι άνθρωποι δεν εμπιστεύονται τις συνδεδεμένες συσκευές και νομίζουν ότι οι πληροφορίες τους δεν είναι αρκετά ασφαλής (είτε από κακή χρήση είτε επειδή προσπαθεί κάποιος να τους βλάψει), αυτό έχει ως αποτέλεσμα τη διάβρωση της εμπιστοσύνης και προκαλείτε μια απροθυμία να χρησιμοποιούν το Διαδίκτυο. Αυτό φυσικά έχει παγκόσμιες συνέπειες για το ηλεκτρονικό εμπόριο, την τεχνολογική καινοτομία, την ελευθερία του λόγου, και σχεδόν κάθε άλλη πτυχή online δραστηριότητας. Έτσι λοιπόν σίγουρα η διασφάλιση της ασφάλειας των «έξυπνων» προϊόντων και υπηρεσιών θα πρέπει να θεωρείται προτεραιότητα για τον τομέα.

Όσο συνδέουμε όλο και περισσότερες συσκευές στο Διαδίκτυο, δημιουργούνται νέες ευκαιρίες για την παραβίαση ευπαθών συστημάτων ασφαλείας, έτσι τα ποσοστά του πιθανού κινδύνου αυξάνονται. «Έξυπνες» συσκευές που εχουν εσωματωμενα χαμηλα συστηματα ασφαλείας θα μπορούσαν να χρησιμεύσουν ως σημεία εισόδου για cyberattack επιτρέποντας σε κακόβουλα άτομα να επαναπρογραμματίσουν μια συσκευή ή ακόμα και να προκαλέσουν την δυσλειτουργία της. Επίσης οι ελλιπώς σχεδιασμένες συσκευές μπορούν να εκθέσουν τα δεδομένα χρήστη σε κλοπή αφήνοντας ροές δεδομένων χωρίς να προστατεύονται επαρκώς. Ακόμα οι δυσλειτουργικές συσκευές μπορούν επίσης να δημιουργήσουν ευπαθή συστήματα ασφάλειας. Τα προβλήματα αυτά είναι εξίσου μεγάλα και για τις μικρές, φθηνές, και ευρείας κατανάλωσης «έξυπνες» συσκευές που διαθέτουν παραδοσιακά τα τερματικά που συνδέονται στο Internet. Το ανταγωνιστικό κόστος και οι τεχνικοί περιορισμοί των «έξυπνων» συσκευών αποτελούν πρόκληση στους κατασκευαστές να σχεδιάσουν επαρκώς τα χαρακτηριστικά ασφάλειας των συσκευών, προκαλώντας ενδεχομένως την ασφάλεια και τη μακροπρόθεσμη διατηρησιμότητα ευπάθειας σαφώς μεγαλύτερη από την ήδη υπάρχουσα στους υπολογιστές.

Λόγω της αύξησης του αριθμού των «έξυπνων» συσκευών αυξάνονται και οι επιθέσεις σε πιθανώς ευπαθή λογισμικά. Μερικές «έξυπνες» συσκευές λόγο του ελαττωματικού σχεδιασμού τους ενδέχεται να επηρεάζουν την ασφάλεια και την αντοχή του Διαδικτύου παγκοσμίως, όχι μόνο τοπικά. Για παράδειγμα, ένα κακώς προστατευμένο «έξυπνο» ψυγείο ή μια «έξυπνη» τηλεόραση στις ΗΠΑ που είναι

μολυσμένα με κακόβουλο λογισμικό μπορεί να στείλουν χιλιάδες επιβλαβή spam emails σε αποδέκτες παγκοσμίως που χρησιμοποιούν την οικιακή τους Wi-Fi σύνδεση στο Internet.

Συμπερασματικά, η ικανότητά μας να λειτουργούμε σε καθημερινές μας δραστηριότητες χωρίς τη χρήση «έξυπνων» συσκευών ή συστημάτων που βρίσκονται συνδεδεμένα στο Internet, είναι πιθανόν να μειωθεί σε hyperconnected κόσμο. Στην πραγματικότητα όμως, είναι όλο και πιο δύσκολο να αγοράσουμε συσκευές που δεν έχουν την δυνατότητα σύνδεσης στο Internet, επειδή οι περισσότεροι κατασκευαστές παράγουν πλέον μόνο έξυπνα προϊόντα. Μέρα με τη μέρα, όλα θα γίνουν συνδεδεμένα στο Διαδίκτυο και οι περισσότερες καθημερινές μας δραστηριότητες θα εξαρτώνται από τις «έξυπνες» συσκευές, οι οποίες πρέπει να έχουν άμεσα την προϋπόθεση να είναι ασφαλείς. Δυστυχώς όμως γνωρίζουμε ότι καμία συσκευή δεν γίνεται να είναι απολύτως ασφαλής. Αυτή η αύξηση της εξάρτησης από τις «έξυπνες» συσκευές και υπηρεσίες Internet αλληλεπιδρά αυξάνοντας τα πιθανά κενά ασφαλείας που πιθανόν μπορεί να εκμεταλλευτούν οι παραβάτες με σκοπό να αποκτήσουν πρόσβαση στις «έξυπνες» συσκευές. Θα μπορούσαμε ίσως στη περίπτωση μιας cyber επίθεσης να αποσυνδέσουμε τις «έξυπνες» συσκευές από το Διαδίκτυο, αλλά όμως δεν μπορούμε να απενεργοποιήσουμε έναν «έξυπνο» μετρητή ισχύος ή ελέγχου της εναέριας κυκλοφορίας ή ακόμη και ένα άτομο με εμφύτευμα στο βηματοδότη, εάν πέσουν θύματα κακόβουλης cyber επίθεσης. Αυτός είναι ο λόγος που η ασφάλεια των «έξυπνων» συσκευών και υπηρεσιών είναι μια μεγάλη συζήτηση και πρέπει να θεωρείται ως ένα κρίσιμο ζήτημα. Μελλοντικά θα εξαρτάται όλο και περισσότερο από αυτές τις «έξυπνες» συσκευές οι καθημερινές μας δραστηριότητες, καθώς η συμπεριφορά τους μπορεί να έχει παγκόσμια εμβέλεια και παγκόσμιο αντίκτυπο.

Το Φάσμα των προβλημάτων Ασφαλείας

Όταν σκεφτόμαστε σχετικά με τις έξυπνες συσκευές είναι σημαντικό να λαμβάνουμε υπόψη μας ότι η ασφάλεια αυτών των συσκευών δεν είναι κάτι δεδομένο. Οι ασφάλεια μιας «έξυπνης» συσκευής δεν έχει δυαδικό διακόπτη όπως οι υπολογιστές που να γράφει ασφαλές ή μη ασφαλές. Αντιθέτως, είναι σημαντικό να σκεφτόμαστε το φάσμα της ασφάλειας των «έξυπνων» συσκευών ως ένα φάσμα τρωτών συσκευών. Η εμβέλεια του φάσματος από εντελώς μη προστατευμένες

συσκευές μέχρι υψηλά προστατευμένες συσκευές περιέχει πολλά στάδια ενδιάμεσα. Σε ένα φαύλο κύκλο, νέες πιθανές απειλές ασφαλείας εξελίσσονται και οι κατασκευαστές καθώς επίσης και οι χειριστές του Διαδικτύου πρέπει συνεχώς να ανταποκρίνονται σε αυτές τις νέες απειλές.

Η γενική εικόνα της ασφάλειας του IoT λειτουργεί κατά κύρια βάση με το πως εκτιμούμε και διαχειριζόμαστε τα προβλήματα που προκύπτουν. Η ασφάλεια μιας συσκευής λειτουργεί βάση: του ρίσκου του οποίου η συσκευή εκτίθεται, η ζημία στην οποία εκτίθεται και ο χρόνος και οι πόροι οι οποίοι χρειάζονται για να επιτύχουμε ένα συγκεκριμένο επίπεδο ασφάλειας. Αν ένας χρήστης δεν μπορεί να ανεχτεί ένα υψηλό βαθμό ρίσκου ασφαλείας στην περίπτωση που ο διαχειριστής του συστήματος ελέγχου κίνησης (traffic control system) ή ένας άνθρωπος ο οποίος έχει ενσωματωμένη μια «έξυπνη» συσκευή υγείας στο σώμα του, τότε δικαιολογείτε το να διαθέσει ένα λογικό ποσό πόρων για να προστατέψει το σύστημα ή την «έξυπνη» συσκευή του από μια πιθανή επίθεση. Διαφορετικά, αν δεν κάνει αυτό πιθανόν να του χακάρουν το σύστημα και να του στέλνουν spam emails ή ακόμα και να κλονιστεί η υγεία του.

Διάφοροι παράγοντες επηρεάζουν την αξιολόγηση και τον υπολογισμό του κινδύνου ασφαλείας. Οι παράγοντες αυτοί περιλαμβάνουν σαφή κατανόηση των σημερινών κινδύνων ασφάλειας αλλά και τις δυνατότητες μελλοντικών κινδύνων. Εκτιμώντας το κόστος της ζημίας αλλά και το κόστος των κινδύνων που ακόμα δεν έχουν πραγματοποιηθεί, καταφέρνουν να υπολογίσουν το εκτιμώμενο κόστος για τον μετριασμό των κινδύνων. Αυτά τα είδη ασφάλειας trade-offs συχνά γίνονται από ένα μεμονωμένο χρήστη. Επίσης σημαντικό είναι να εξεταστεί επαρκώς η κάθε «έξυπνη» συσκευή ως μέρος ενός μεγαλύτερου «έξυπνου» οικοσυστήματος. Η δικτυακή συνδεσιμότητα των «έξυπνων» συσκευών σημαίνει ότι οι αποφάσεις που λαμβάνονται για μια μεμονωμένη «έξυπνη» συσκευή μπορεί να έχει παγκόσμιες επιπτώσεις και σε άλλες «έξυπνες» συσκευές.

Ως θέμα αρχής, οι προγραμματιστές των «έξυπνων» συσκευών για το IoT έχουν την υποχρέωση να διασφαλίσουν ότι αυτές οι συσκευές δεν εκτίθονται είτε μέσω της δικής τους χρήσης ή της χρήσης τρίτων για ενδεχόμενη ζημία. Το θέμα των επιχειρήσεων και της οικονομίας είναι ότι οι κατασκευαστές ενδιαφέρονται για τη

μείωση του κόστους τους, την πολυπλοκότητα και το χρόνο διάθεσης στην αγορά. Για παράδειγμα, «έξυπνες» συσκευές που είναι υψηλής έντασης, χρησιμοποιούν δαπανηρά εξαρτήματα που προστίθενται στο μεγάλο ποσοστό του κόστους, προσθέτοντας περισσότερη μνήμη και ταχύτερους επεξεργαστές για να εφαρμόσουν τα μέτρα ασφάλειας θα μπορούσε εύκολα να το προϊόν να μην είναι εύκολα εμπορικώς ανταγωνιστικό.

Από οικονομικής απόψεως, η έλλειψη ασφάλειας στις «έξυπνες» συσκευές οδηγεί σε οικονομικά αδιέξοδα, όπου το κόστος που επιβάλλεται από μια εταιρία εμποδίζει και σε άλλες εταιρίες. Ένα κλασικό παράδειγμα είναι η μόλυνση του περιβάλλοντος, όπου οι περιβαλλοντικές ζημιές και το κόστος εκκαθάρισης αναλαμβάνονται από άλλες εταιρίες. Το θέμα είναι ότι το κόστος των εξωγενών επιδράσεων που επιβλήθηκαν σε άλλους, συνήθως δεν συνυπολογίζεται στην διαδικασία λήψης αποφάσεων, εκτός εάν, όπως είναι η περίπτωση της ρύπανσης, που ο φόρος επιβάλλεται από την αρχή. Στην περίπτωση της ασφάλειας των πληροφοριών, το κόστος προκύπτει όταν ο κατασκευαστής, δημιουργώντας το προϊόν, δεν φέρει ευθύνη για το κόστος που προκαλείται από οποιαδήποτε ευπαθές σύστημα ασφαλείας- στην περίπτωση αυτή, η νομοθεσία περί αστικής ευθύνης μπορεί να επηρεάσει τους κατασκευαστές, ώστε να ληφθούν υπόψη οι εξωτερικές ζημίες με σκοπό να αναπτύξουν περισσότερο την ασφάλεια των προϊόντων.

Αυτά τα θέματα ασφάλειας δεν είναι κάτι καινούριο στο πλαίσιο της τεχνολογίας των πληροφοριών, αλλά στην κλίμακα των μοναδικών προκλήσεων που μπορούν να προκύψουν σχετικά με την ασφάλεια των «έξυπνων» συσκευών, όπως περιγράφεται κατωτέρω, τα καθιστούν σημαντικά.

Unique Security Challenges of IoT Devices

Οι «έξυπνες» συσκευές τείνουν να διαφέρουν από τις παραδοσιακές συσκευές υπολογιστών και συσκευές πληροφορικής σχετικά με τα θέματα ασφάλειας:

- Πολλές «έξυπνες» συσκευές, όπως οι αισθητήρες και τα καταναλωτικά είδη, έχουν σχεδιαστεί ώστε να αναπτυχθούν σε μαζική κλίμακα της τάξεις του μεγέθους πέραν των απλών συσκευών που συνδέονται στο Διαδίκτυο. Ως αποτέλεσμα, το δυναμικό της ποσότητας των διασυνδεδεμένων δεσμών μεταξύ

αυτών των συσκευών είναι πρωτοφανής. Επιπλέον, πολλές από αυτές τις συσκευές, θα μπορούσαν να δημιουργήσουν δεσμούς με σκοπό να επικοινωνήσουν με άλλες συσκευές με τους δικούς τους απρόβλεπτους και δυναμικούς τρόπους. Επομένως, τα υπάρχοντα εργαλεία, οι μέθοδοι και οι στρατηγικές που σχετίζονται με ασφάλεια του IoT μπορεί να χρειάζονται να επανεξεταστούν.

- Πολλές υλοποιήσεις του IoT θα αποτελούνται από συλλογές όμοιες ή παραπλήσιες με πανομοιότυπες συσκευές. Η ομοιογένεια μεγεθύνει τις δυνητικές επιπτώσεις των μεμονωμένων ευπαθών συστημάτων ασφαλείας. Τεράστιος αριθμός των «έξυπνων» συσκευών έχουν τα ίδια χαρακτηριστικά. Για παράδειγμα, ένα πρωτόκολλο επικοινωνίας μιας εταιρείας του «έξυπνων» λαμπτήρων μπορεί να επεκταθεί σε κάθε μάρκα και κάθε μοντέλο της συσκευής που χρησιμοποιεί το ίδιο πρωτόκολλο ή έχει παρόμοια χαρακτηριστικά.

- Πολλές «έξυπνες» συσκευές θα αναπτυχθούν με αναμενόμενη διάρκεια ζωής πολλών ετών, περισσότερο από ότι συνήθως καθώς συνδέονται με εξοπλισμό υψηλής τεχνολογίας. Περαιτέρω, οι συσκευές αυτές θα μπορούσαν να αναπτυχθούν σε περιστάσεις που καθιστούν δύσκολο ή αδύνατο να επαναρυθμιστούν ή να αναβαθμιστούν ή και ακόμη οι συσκευές αυτές μπορούν να συνεχίσουν να λειτουργούν περισσότερο ακόμα και από την εταιρεία που τα δημιούργησε, αφήνοντας “ορφανές” αυτές συσκευές με κανένα μέσο για μακροπρόθεσμη υποστήριξη. Τα σενάρια αυτά δείχνουν ότι η ασφάλεια των μηχανισμών που είναι κατάλληλες για ανάπτυξη ενδέχεται να μην είναι επαρκής για την πλήρη διάρκεια ζωής της συσκευής, όμως οι απειλές για την ασφάλεια τους εξελίσσονται. Συνεπώς δημιουργείτε ρήγμα στο πρωτόκολλο ασφαλείας που δίνει την δυνατότητα σε τρίτους εγκαταστήσουν κάποιο κακόβουλο λογισμικό στην «έξυπνη» συσκευή καθώς και να κλέψουν αρχεία του χρήστη. Αυτό έρχεται σε αντίθεση με τα παραδείγματα των κοινών συστημάτων υπολογιστών που συνήθως έχουν αναβαθμιστεί με λειτουργικό σύστημα και ενημερώσεις λογισμικού για όλη τη διάρκεια ζωής του υπολογιστή με σκοπό την αντιμετώπιση των απειλών της ασφαλείας του. Η μακροπρόθεσμη στήριξη και διαχείριση των «έξυπνων» συσκευών αποτελεί μια σημαντική πρόκληση ασφαλείας.

- Πολλές έξυπνες συσκευές σκόπιμα σχεδιάστηκαν χωρίς καμία δυνατότητα να αναβαθμιστούν, ή ακόμα και να είχαν τη δυνατότητα να αναβαθμιστούν η διαδικασία της αναβάθμισης είναι δύσκολη ως και αδύνατη. Για παράδειγμα, σκεφτείτε το 2015 που η Fiat και η Chrysler πραγματοποίησε ανάκληση 1.4 εκατομμυρίων οχημάτων για να καθορίσει μια ευπάθεια που επέτρεπε σε έναν εισβολέα να παραβιάσει ασύρματα το αυτοκίνητο. Τα αυτοκίνητα αυτά θα έπρεπε οι ιδιοκτήτες τους να τα πάνε σε μια αντιπροσωπία της Fiat η της Chrysler για να αναβαθμιστούν χειροκίνητα, ή ο ιδιοκτήτης τους έπρεπε να εκτελέσετε την αναβάθμιση τους με ένα κλειδί USB που απαιτούσε πολλές γνώσεις πληροφορικής τις οποίες αρκετοί δεν κατείχαν. Η πραγματικότητα λοιπόν είναι ότι ένα υψηλό ποσοστό των εν λόγω αυτοκίνητα πιθανότατα δεν θα αναβαθμιστεί καθόλου διότι η διαδικασία της αναβάθμισης ταλαιπωρούσε με τον έναν η τον άλλο τρόπο τους ιδιοκτήτες, αφήνοντας τους μονίμως ευάλωτους σε πιθανές απειλές της ασφάλειας του οχήματος τους.

- Πολλές «έξυπνες» συσκευές λειτουργούν με έναν τρόπο όπου ο χρήστης έχει λίγη ή και καμία ορατότητα της εσωτερικής λειτουργίας της συσκευής ή την ακρίβεια των ροών δεδομένων που παράγουν. Αυτό δημιουργεί μια ευπάθεια ασφαλείας όταν ένας χρήστης πιστεύει πως η «έξυπνη» συσκευή του εκτελεί ορισμένες λειτουργίες, όταν στην πραγματικότητα μπορεί να εκτελεί το ανεπιθύμητο κακόβουλο πρόγραμμα ή τη συλλογή περισσότερων δεδομένων από ότι σκόπευε ο χρήστης. Οι λειτουργίες της συσκευής μπορούν ακόμα να αλλάξουν χωρίς ειδοποίηση όταν ο κατασκευαστής διάθετε μια νέα ενημέρωση, αφήνοντας τον χρήστη ευάλωτο στις όποιες αλλαγές του κατασκευαστή.

- Ορισμένες «έξυπνες» συσκευές είναι πιθανό να αναπτυχθούν σε μέρη όπου η φυσική ασφάλεια είναι δύσκολο ή αδύνατο να επιτευχθεί. Οι εισβολείς μπορούν να έχουν άμεση πρόσβαση στις «έξυπνες» συσκευές. Σαφώς βέβαια οι χρήστες μπορούν να διαθέτουν αντικλεπτικό σύστημα και άλλες καινοτομίες σχεδιασμού με σκοπό να εξασφαλίσει την ασφάλεια της συσκευής τους.

- Πολλές «έξυπνες» συσκευές, όπως πολλοί αισθητήρες περιβάλλοντος, έχουν σχεδιαστεί διακριτικά να τοποθετούνται και να ενσωματώνονται στο περιβάλλον, όπου ο χρήστης δεν επιδρά άμεσα στη συσκευή ούτε παρακολουθεί την

κατάσταση λειτουργίας της. Επιπλέον, οι συσκευές αυτές μπορούν να έχουν σαφής τρόπους για να προειδοποιήσουν το χρήστη όταν ένα πρόβλημα ασφάλειας ανακύπτει, καθιστώντας δύσκολο για τον χρήστη να γνωρίζει ότι μια παραβίαση ασφαλείας της «έξυπνης» συσκευής προέκυψε. Μια παραβίαση ασφάλειας μπορεί να συνεχιστεί για πολύ καιρό πριν να την παρατηρήσει χρήστης και να διορθωθεί αν και εφόσον φυσικά η διόρθωση ή ο μετριασμός της είναι ακόμα δυνατός. Ομοίως, ο χρήστης ενδέχεται να μην γνωρίζει ότι ένας αισθητήρας υπάρχει στο περιβάλλον, επιτρέποντας μία παραβίαση ασφάλειας να παραμείνει για μεγάλα χρονικά διαστήματα χωρίς ανίχνευση.

- Κάποια αρχικά μοντέλα του IoT υπέθεταν πως αυτά θα χρησιμοποιούταν σε μεγάλες ιδιωτικές και ή δημόσιες επιχειρήσεις τεχνολογίας, αλλά στο μέλλον το σύνθημα "Δημιουργήστε το δικό σας IoT" (BY IoT) μπορεί να γίνει πιο κοινότυπο όπως αποδεικνύεται και από τις αυξανόμενες Arduino και *Raspberry* PI60 developer κοινότητες.

Ερωτήματα για την Ασφάλεια του IoT

Αυτά τα ζητήματα ιδιοτηκότητας θα δημιουργούσαν προκλήσεις ακόμα κι αν τα συμφέροντα και τα κίνητρα όλων των συμμετεχόντων στο οικοσύστημα του IoT ήταν κοινά. Εντούτοις, γνωρίζουμε ότι μπορούν να υπάρξουν άνισες ή άδικες σχέσεις και ενδιαφέροντα μεταξύ εκείνων που εκτίθενται στη συλλογή προσωπικών δεδομένων και εκείνων που συνολικά, αναλύουν και χρησιμοποιούν τα στοιχεία. Η πηγή δεδομένων μπορεί να διαπιστώσει μια ανεπιθύμητη εισχώρηση στο ιδιωτικό περιβάλλον, συχνά χωρίς τη συγκατάθεση, τον έλεγχο, την επιλογή, ή ακόμα και χωρίς να είναι εις γνώσιν του χρήστη. Παρόλα αυτά ο συλλέκτης δεδομένων, μπορεί να θεωρήσει αυτήν ως έναν πόρο προς αξιοποίηση που μπορεί να προσθέσει αξία στα προϊόντα και τις υπηρεσίες καθώς επίσης και να παρέχει τις νέες ροές εισοδήματος.

Επειδή οι προκλήσεις ασφαλείας του IoT μπορούν να προκαλέσουν την έννοια της ασφάλειας με καινούριους τρόπους, οι ερωτήσεις κλειδιά πρέπει να υποβληθούν κατά τον επαναξιολόγηση των σε απευθείας σύνδεση προτύπων ασφαλείας στα πλαίσια του IoT. Μερικές ερωτήσεις που έχουν τεθεί περιλαμβάνουν:

A) Fairness in Data Collection and Use:

Πώς επιλύουμε τη σχέση των αγορών μεταξύ των πηγών δεδομένων και των συλλεκτών δεδομένων στα πλαίσια του IoT; Το προσωπικό στοιχείο έχει την προσωπική και εμπορική αξία που οι πηγές και οι συλλέκτες εκτιμούν διαφορετικά, και χωριστά αλλά και στο σύνολο και τα δύο μέρη έχουν τα νόμιμα ενδιαφέροντα που μπορούν να συγκρουστούν. Πώς μπορούν εκείνα τα ευδιάκριτα ενδιαφέροντα να εκφραστούν με τέτοιο τρόπο ώστε να οδηγηθούν στους δίκαιους και συνεπείς κανόνες για τις πηγές αλλά και για τους συλλέκτες που αφορούν την πρόσβαση, τον έλεγχο, τη διαφάνεια, και την προστασία;

B) Transparency, Expression, and Enforcement of Privacy Preferences:

Πώς μπορούν οι πολιτικές και οι πρακτικές ιδιωτικότητας να γίνουν εύκολα διαθέσιμες και κατανοητές στα πλαίσια του IoT; Ποιες είναι οι εναλλακτικές λύσεις στο παραδοσιακό πρότυπο ιδιωτικότητας «ειδοποίησης και συγκατάθεσης» που θα απευθύνονται στις μοναδικές πτυχές του IoT; Τι είναι ένα αποτελεσματικό πρότυπο για την έκφραση, την εφαρμογή, και την επιβολή των μεμονωμένων προτιμήσεων ιδιωτικότητας και των πολυμερών προτιμήσεων; Θα μπορούσε ένα τέτοιο πολυμεριστικό πρότυπο να κατασκευαστεί, και σε αυτή την περίπτωση, πως θα έμοιαζε αυτό; Πώς θα μπορούσε να εφαρμοστεί στις συγκεκριμένες περιστάσεις που περιλαμβάνουν τις μεμονωμένες προτιμήσεις ιδιωτικότητας; Υπάρχει μια αγορά για τη μεταφορά της διαχείρισης των ήδη τοποθετημένων επιλογών ιδιωτικότητας στις εμπορικές υπηρεσίες με σκοπό να εφαρμόσουν τις προτιμήσεις των χρηστών; Υπάρχει ένας ρόλος για ένα πληρεξούσιο ιδιωτικότητας που να εκφράζει και να επιβάλει τις προτιμήσεις ενός χρήστη σε μια σειρά συσκευών, εξαλείφοντας την ανάγκη για την άμεση αλληλεπίδραση με την καθεμία;

C) Wide-Ranging Privacy Expectations:

Οι κανόνες και οι προσδοκίες ιδιωτικότητας είναι στενά συνδεδεμένοι στο κοινωνικό και πολιτιστικό πλαίσιο του χρήστη, το οποίο θα ποικίλει από μια ομάδα ή ένα έθνος σε ένα άλλο. Πολλά σενάρια του IoT περιλαμβάνουν τις επεκτάσεις συσκευών και τις δραστηριότητες συλλογής δεδομένων με πολυεθνικό ή σφαιρικό φάσμα που θα διασχίζει τα κοινωνικά και πολιτιστικά όρια. Τι θα σήμαινε αυτό για την ανάπτυξη μιας ευρέως εφαρμόσιμης προστασίας της ιδιωτικότητας για το IoT;

Πώς μπορούν οι συσκευές και τα συστήματα του IoT να προσαρμοστούν για να αναγνωρίσουν και να τιμήσουν τη σειρά των προσδοκιών ιδιωτικότητας των χρηστών και των διαφορετικών νόμων;

D) Privacy by Design:

Πώς μπορούμε να ενθαρρύνουμε τους κατασκευαστές «έξυπνων» συσκευών για να ενσωματώσουμε τις αρχές ιδιωτικότητας-από-σχεδίου στις βασικές τιμές τους; Πώς ενθαρρύνουμε το συνυπολογισμό των εκτιμήσεων της καταναλωτικής ιδιωτικότητας σε κάθε φάση ανάπτυξης προϊόντος και λειτουργίας; Πώς συμφιλιώνουμε τις απαιτήσεις λειτουργικότητας και ιδιωτικότητας; Κατ 'αρχήν, οι κατασκευαστές πρέπει να προσδοκούν ότι η ιδιωτικότητα -σεβόμενη τα προϊόντα και τις πρακτικές- χτίζει τη μακροπρόθεσμη εμπιστοσύνη πελατών, την ικανοποίηση, και την πίστη στα εμπορικά σήματα. Είναι αυτό ένα αρκετά εξαναγκάσιμο κίνητρο, όταν αντιστοιχείται ενάντια στον ανταγωνισμό για την κατασκευαστική απλότητα και την ταχύτητα διαθεσιμότητάς του στην αγορά; Θα έπρεπε οι «έξυπνες» συσκευές να σχεδιαστούν με προεπιλεγμένες ρυθμίσεις που διαμορφώνονται για τον πιο συντηρητικό τρόπο συλλογής δεδομένων.

E) Identification:

Πώς θα έπρεπε να προστατέψουμε τα στοιχεία που συλλέγονται από το IoT που εμφανίζεται να μην είναι προσωπικά στο σημείο της συλλογής ή είναι μη προσδιορίσιμα, αλλά μπορούν σε κάποιο βαθμό στο μέλλον να γίνουν προσωπικά στοιχεία.

IoT Interoperability / Standards Background

Στο παραδοσιακό Διαδίκτυο, η διαλειτουργικότητα είναι η πιο βασική αξία. Η πρώτη απαίτηση της συνδεσιμότητας του Διαδικτύου είναι ότι «συνδεδεμένα» συστήματα να είναι σε θέση «να μιλήσει την ίδια γλώσσα» των πρωτοκόλλων και των κωδικοποιήσεων. Η διαλειτουργικότητα είναι τόσο θεμελιώδης που τα πρόωρα εργαστήρια για τους προμηθευτές εξοπλισμού Διαδικτύου αποκαλέστηκαν «Interops» και είναι ο ρητός στόχος των ολόκληρων συσκευών προτύπων Διαδικτύου που κεντροθετούνται στην IETF (Internet Engineering Task Force).

Η διαλειτουργικότητα είναι επίσης ένας ακρογωνιαίος λίθος του ανοικτού Διαδικτύου. Τα εμπόδια που δημιουργούνται σκοπίμως για να εμποδίσουν την ανταλλαγή των πληροφοριών μπορούν να αρνηθούν στους χρήστες του Ιντερνέτ τη δυνατότητα να συνδέσουν, να μιλήσουν, να μοιραστούν, και να καινοτομήσουν, τα οποία είναι οι τέσσερις θεμελιώδεις αρχές του ISOC. Οι αποκαλούμενοι «περιτοιχισμένοι κήποι» στους οποίους οι χρήστες επιτρέπονται να επικοινωνήσουν με μόνο το α υποσύνολο των περιοχών και υπηρεσιών, μπορούν ουσιαστικά να μικρύνουν τα κοινωνικά, πολιτικά, και οικονομικά οφέλη της πρόσβασης σε ολόκληρο Διαδίκτυο.

Σε ένα πλήρως διαλειτουργικό περιβάλλον, οποιαδήποτε «έξυπνη» συσκευή θα ήταν σε θέση να συνδεθεί με οποιεσδήποτε πληροφορίες συσκευών ή συστημάτων και ανταλλαγής όπως επιδιώκονται. Στην πρακτικότητα, η διαλειτουργικότητα είναι πιο σύνθετη. Η διαλειτουργικότητα μεταξύ των συσκευών και των συστημάτων IoT συμβαίνει στις ποικιλίες βαθμών στα διαφορετικά στρώματα μέσα στη λίστα πρωτοκόλλου επικοινωνιών μεταξύ των συσκευών. Επιπλέον, η πλήρης διαλειτουργικότητα πέρα από κάθε πτυχή ενός τεχνικού προϊόντος είναι όχι πάντα εφικτή, απαραίτητη, ή επιθυμητή και, εάν το επιβάλλουν οι περιστάσεις (όπως μέσω των κυβερνητικών εξουσιοδοτήσεων), θα μπορούσε να παρέχει τα αντικίνητρα για την επένδυση και την καινοτομία. Η τυποποίηση και η υιοθέτηση των πρωτοκόλλων που διευκρινίζουν αυτές τις λεπτομέρειες επικοινωνίας, είναι βέλτιστη για να έχει τα πρότυπα και να είναι στην καρδιά της συζήτησης της διαλειτουργικότητας του IoT.

Πέρα από τις τεχνικές πτυχές, η διαλειτουργικότητα έχει σημαντική επιρροή στον πιθανό οικονομικό αντίκτυπο του IoT. Με καλή λειτουργία και καθορισμένη με σαφήνεια διαλειτουργικότητα «έξυπνων» συσκευών, μπορεί να ενθαρρύνει την καινοτομία και να παρέχει τις αποδοτικότερες λύσεις για τους κατασκευαστές «έξυπνων» συσκευών, που αυξάνουν τη γενική οικονομική αξία της αγοράς. Επιπλέον, η εφαρμογή των υπαρχόντων προτύπων και η ανάπτυξη των νέων ανοιχτών προτύπων βοηθούν όπου είναι απαραίτητο τα χαμηλότερα εμπόδια στην είσοδο, διευκολύνουν τα νέα επιχειρησιακά πρότυπα, και χτίζουν τις κλίμακες της οικονομίας.

Οι εκθέσεις αναφοράς του ιδρύματος McKinsey για το 2015, βασισμένες στον μέσο

όρος, δηλώνουν ότι «η διαλειτουργικότητα είναι απαραίτητη για να δημιουργήσουν το 40 τοις εκατό της πιθανής αξίας που μπορεί να παραχθεί από το IoT σε διάφορες ρυθμίσεις». Καθώς η έκθεση συνεχίζεται, αναφέρει: «η διαλειτουργικότητα απαιτείται για να ξεκλειδώσει περισσότερα από $4 τρισεκατομμύρια το χρόνο στον πιθανό οικονομικό αντίκτυπο για τη χρήση του IoT έως το 2025, από έναν συνολικό αντίκτυπο $11.1 τρισεκατομμυρίων στις εννέα ρυθμίσεις που McKinsey ανέλυσε». Μερικές επιχειρήσεις αντιλαμβάνονται τα ανταγωνιστικά πλεονεκτήματα και τα οικονομικά κίνητρα στην οικοδόμηση των ιδιόκτητων συστημάτων και στις γενικές οικονομικές ευκαιρίες που μπορούν να περιοριστούν σε μια αγορά των σιλό.

Επίσης, η διαλειτουργικότητα είναι πλήρως πολύτιμη από την προοπτική και του μεμονωμένου καταναλωτή και του οργανωτικού χρήστη αυτών των συσκευών. Διευκολύνει τη δυνατότητα να επιλεχτούν οι συσκευές με τα καλύτερα χαρακτηριστικά γνωρίσματα, στην καλύτερη τιμή και να ενσωματωθούν για να τις κάνει την εργασία από κοινού. Οι αγοραστές μπορούν να είναι διστακτικοί στο να αγοράσουν τα προϊόντα και τις υπηρεσίες του IoT εάν υπάρχει υψηλή πολυπλοκότητα ιδιοκτησίας, ανησυχία σχετικά για τον προμηθευτή, ή φόβος παλιού συστήματος ασφαλείας λόγω των μεταβαλλόμενων πρωτοκόλλων.

Key Considerations and Challenges in IoT Interoperability / Standards

Η διαλειτουργικότητα, τα πρότυπα, τα πρωτόκολλα, και οι συμβάσεις είναι ένα αρχικό ζήτημα στην πρόωρη ανάπτυξη και υιοθέτηση των «έξυπνων» συσκευών. Ενώ διάφορες βασικές εκτιμήσεις και προκλήσεις περιλαμβάνουν:

Proprietary Ecosystems and Consumer Choice:

Μερικοί κατασκευαστές συσκευών βλέπουν ένα πλεονέκτημα αγοράς στη δημιουργία ενός ιδιόκτητου οικοσυστήματος των συμβατών προϊόντων του IoT, αποκαλούμενου μερικές φορές «περιτοιχισμένους κήπους», οι οποίοι περιορίζουν τη διαλειτουργικότητα μόνο σε εκείνα τα συσκευές και συστατικά μέσα στη γραμμή παραγωγής εμπορικών σημάτων. Αυτοί οι κατασκευαστές μπορούν να δημιουργήσουν ένα ασφαλές περιβάλλον για το χρήστη στο ιδιαίτερο οικοσύστημα συσκευών τους με το να αυξήσουν το κόστος μετατροπής για τον καταναλωτή με σκοπό την αλλαγή σε μια διαφορετική εταιρία στο μέλλον ή τα τμήματα υποκατάστατων από έναν άλλο προμηθευτή. Παραδείγματος χάριν, στην αγορά

εγχώριας αυτοματοποίησης, οι λάμπες φωτός από έναν προμηθευτή μπορούν να μην είναι διαλειτουργικές με έναν διακόπτη ή ένα σύστημα ελέγχου που κατασκευάζεται από έναν άλλον προμηθευτή.

Οι υποστηρικτές διαλειτουργικότητας βλέπουν αυτές τις πρακτικές ως εμπόδιο στην επιλογή χρηστών επειδή αποτρέπει τους χρήστες από την αγορά εναλλακτικών προϊόντων. Βλέπουν επίσης αυτήν την πρακτική ως εμπόδιο στην καινοτομία και τον ανταγωνισμό επειδή περιορίζει τη δυνατότητα των ανταγωνιστών να δημιουργήσουν τα νέα προϊόντα βασισμένα στη θεμελιώδη υποδομή του οικοσυστήματος. Μερικοί κατασκευαστές συσκευών, εντούτοις, βλέπουν μια κλειστή προσέγγιση του οικοσυστήματος ως όφελος των χρηστών με την παροχή ενός πρωτοκόλλου που μπορεί να προσαρμοστεί γρηγορότερα και ευκολότερα όταν απαιτείται αλλαγή στην τεχνική ή στην ζήτηση της αγοράς.

Οι εκτιμήσεις της διαλειτουργικότητας επεκτείνονται επίσης στα στοιχεία που συλλέγονται και που υποβάλλονται σε επεξεργασία από τις υπηρεσίες του IoT. Μια από τις αρχικές έλξεις των συνδεδεμένων συσκευών είναι η δυνατότητα να διαβιβαστούν και να παραληφθούν στοιχεία από τις υπηρεσίες «στο cloud», οι οποίες παρέχουν με τη σειρά τους πολύτιμες πληροφορίες ή υπηρεσίες που εδρεύουν επάνω σε εκείνο το δεδομένο. Ενώ αυτό είναι εξαιρετικά χρήσιμο, μπορεί επίσης να παρουσιάσει προκλήσεις για έναν χρήστη που θέλει να κινηθεί προς μια ανταγωνιστική υπηρεσία. Ακόμα κι αν η πρόσβαση στα δεδομένα που παράγονται από τις συσκευές τίθεται στην διάθεση των χρηστών, η λήψη των δεδομένων θα είναι άχρηστη εάν το δεδομένο είναι με ένα ιδιόκτητο σχήμα. Μόνο εάν το στοιχείο πηγής είναι ελεύθερα διαθέσιμο στο δημιουρμένο χρήστη, με ένα σχήμα ανοιχτών προτύπων, οι χρήστες θα είναι ελεύθεροι να κινηθούν προς έναν άλλο φορέα παροχής υπηρεσιών, ή να εκτελέσουν τις αναλύσεις μόνοι τους.

Technical and Cost Constraints.

Δεδομένου ότι οι κατασκευαστές αναπτύσσουν τις «έξυπνες» συσκευές, υπάρχει χρόνος στην αγορά, και περιορισμοί δαπανών στους παράγοντες στη διαλειτουργικότητας και στο σχέδιο των «έξυπνων» συσκευών. Μερικές «έξυπνες» συσκευές περιορίζονται από τους τεχνικούς παράγοντες όπως τους περιορισμένες εσωτερικές πόρους επεξεργασίας, τη μνήμη, ή τις ζητήσεις κατανάλωσης ισχύος.

Επομένως, οι κατασκευαστές τίθονται υπό πίεση με σκοπό να μειώσουν το κόστος μονάδας της συσκευής με την ελαχιστοποίηση των δαπανών του σχεδιασμού των μερών και των προϊόντων. Οι κατασκευαστές κάνουν τις αναλύσεις κόστους-κέρδους για να αποφασίσουν εάν οι συμπληρωματικές δαπάνες και η ενδεχομένως μειωμένη απόδοση προϊόντων αξίζουν τα πρόσθετα οφέλη για τα πρότυπα. Βραχυπρόθεσμα, μπορεί να είναι περισσότερο δαπανηρό για να σχεδιάσει τα χαρακτηριστικά γνωρίσματα διαλειτουργικότητας σε ένα προϊόν και τη δοκιμή για τη συμμόρφωση με μια προδιαγραφή προτύπων. Σε μερικά πλαίσια, η μικρότερη σε κόστος πορεία στην αγορά μπορεί να είναι να χρησιμοποιηθούν ιδιόκτητα πρωτόκολλα και συστήματα.

Αυτό πρέπει να συγκριθεί, εντούτοις, ενάντια στα μακροπρόθεσμα κέρδη του κύκλου ζωής των προϊόντων που διατίθενται από τη διαλειτουργικότητα.

Schedule Risk.

Σε μια παγκοσμίως ανταγωνιστική αγορά, υπάρχει συχνά ένα πλεονέκτημα καινοτομίας να φέρει ένα προϊόν στην αγορά γρήγορα και να καθιερώσει το μερίδιό του σε αυτήν, και αυτό ισχύει βεβαίως για τους κατασκευαστές «έξυπνων» συσκευών. Ένα πρόβλημα προκύπτει για τη διαλειτουργικότητα «έξυπνων» συσκευών όταν ξεπερνά το πρόγραμμα σχεδίου προϊόντων του κατασκευαστή «έξυπνων» συσκευών και τη διαθεσιμότητα των προτύπων διαλειτουργικότητας. Ένας κατασκευαστής συσκευών του IoT που είναι πρόθυμος να φέρει ένα προϊόν στην αγορά μπορεί να δει την έλλειψη βεβαιότητας στα προγράμματα και τις διαδικασίες ανάπτυξης προτύπων ως επιχειρησιακό κίνδυνο που ελαχιστοποιείται ή που αποφεύγεται. Αυτό μπορεί να κάνει τις εναλλακτικές λύσεις στα ανοικτά πρότυπα διαλειτουργικότητας ελκυστικότερες, ιδιαίτερα βραχυπρόθεσμες.

Technical Risk.

Όταν ένας κατασκευαστής ή ένας χρήστης «έξυπνων» συσκευών προγραμματίζει την ανάπτυξη ενός προϊόντος, πρέπει να αξιολογήσουν τους τεχνικούς κινδύνους σχεδίου πρωτοκόλλων στη αναπτυξιακή διαδικασία. Η ενσωμάτωση των υπαρχόντων και αποδεδειγμένων προτύπων στα σχέδια προϊόντων ή συστημάτων μπορεί να αντιπροσωπεύσουν έναν χαμηλότερο τεχνικό κίνδυνο έναντι της ανάπτυξης και της χρήσης των ιδιόκτητων πρωτοκόλλων. Η χρήση των γενικών,

ανοικτών και ευρέων διαθέσιμων προτύπων (όπως η ακολουθία πρωτοκόλλου Διαδικτύου) ως δομικές μονάδες για τις συσκευές και τις υπηρεσίες μπορούν να φέρουν άλλα οφέλη, όπως η πρόσβαση στις μεγαλύτερες ομάδες του τεχνικού ταλέντου, το αναπτυγμένο λογισμικό, και φτηνότερες δαπάνες ανάπτυξης. Αυτοί οι παράγοντες συζητούνται στον Internet Architechture Board (IAB).

Devices Behaving Badly.

Η έλλειψη προτύπων και οι τεκμηριωμένες καλύτερες πρακτικές ασκούν μεγαλύτερη επίδραση από την περιοριστική δυνατότητα των «έξυπνων» συσκευών. Με έναν παθητικό τρόπο, η απουσία αυτών των προτύπων μπορεί να επιτρέψουν την κακή συμπεριφορά από τις «έξυπνες» συσκευές. Με άλλα λόγια, χωρίς πρότυπα για να καθοδηγήσουν τους κατασκευαστές, οι υπεύθυνοι για την ανάπτυξη αυτών των συσκευών σχεδιάζουν μερικές φορές τα προϊόντα που λειτουργούν με τους αποδιοργανωτικούς τρόπους στο διαδίκτυο χωρίς πολύ σεβασμό στον αντίκτυπό τους. Αυτές οι συσκευές είναι χειρότερες από απλά μην όντας διαλειτουργικές. Εάν είναι κακοσχεδιασμένες και διαμορφωμένες λάθος, μπορούν να έχουν αρνητικές συνέπειες για τους πόρους δικτύωσης που συνδέονται και με το ευρύτερο Διαδίκτυο.

Σε μια έκθεση, ο ειδικός στο Διαδίκτυο Geoff Huston περιγράφει τον πολλαπλασιασμό τέτοιων συσκευών όπως το “Διαδίκτυο των Ηλίθιων Πραγμάτων”. Ο Huston περιγράφει ένα παράδειγμα ενός καλωδιακού μόντεμ κάποιου καταναλωτή που παράγεται από έναν κατασκευαστή που είναι κωδικοποιημένος με την διεύθυνση IP του κεντρικού υπολογιστή του χρονικού πρωτοκόλλου δικτύων (NTP) που χρησιμοποιείται από το πανεπιστήμιο του Ουισκόνσιν, το οποίο είναι μια παραβίαση των συνήθως αποδεκτών πρακτικών του σχεδίου. Όπως Huston εξηγεί, “οι περισσότερες μονάδες που πωλήθηκαν, όσο μεγαλύτερος ο συνολικός όγκος κυκλοφορίας που εστάλη στον κεντρικό υπολογιστή του πανεπιστημίου.” Όχι μόνο αυτές οι συσκευές συμπεριφέρονταν άσχημα με τη διοχέτευση όλων των αιτημάτων NTP σε έναν ενιαίο κεντρικό υπολογιστή, αλλά το φτωχό σχέδιο του προμηθευτή συνέθεσε στη δυσκολία επειδή δεν παρείχε κανέναν αποτελεσματικό μηχανισμό για να καθορίσει το πρόβλημα.

Υπάρχει μια ευκαιρία για την επέκταση των προτύπων και των καλύτερων πρακτικών του IoT με σκοπό να μειώσουν σημαντικά αυτή η κατηγορία

προβλημάτων με τον καιρό.

Legacy Systems.

Η τυποποίηση διαλειτουργικότητας είναι μια πρόκληση για τις νέες «έξυπνες» συσκευές που πρέπει να διασυνδεθούν με τα συστήματα που επεκτάθηκαν ήδη και που λειτουργούν. Αυτό είναι σχετικό με πολλά συγκεκριμένα και οριζόμενα από εφαρμογές σε περιβάλλοντα βιομηχανίας που έχουν καθιερώσει τα δίκτυα των συσκευών. Οι μηχανικοί του IoT βρίσκονται αντιμέτωποι με τις ανταλλαγές σχεδίου για να διατηρήσουν τη συμβατότητα με τα συστήματα κληρονομιών ακόμα προσπαθώντας να επιτύχουν τη μεγαλύτερη διαλειτουργικότητα με άλλες συσκευές μέσω της χρήσης των πρωτοκόλλων.

Configuration.

Οι χρήστες θα αντιμετωπίσουν τις αυξανόμενες προκλήσεις στη διαχείριση των μεγαλύτερων αριθμών των «έξυπνων» συσκευών. Μια τέτοια πρόκληση είναι η ανάγκη γρήγορα και εύκολα τροποποιεί τις τοποθετήσεις διαμόρφωσης πολλών συσκευών IoT σε ένα δίκτυο. Κατά την αντιμετώπιση της αποθαρρυντικής προοπτικής της διαμόρφωσης των εκατοντάδων ξεχωριστών συσκευών, θα ήταν απαραίτητο να έχουν στοχαστικά σχέδια και τυποποίηση των εργαλείων διαμόρφωσης, των μεθόδων, και του Interface.

Proliferation of Standards Efforts.

Πολλοί νέοι βιομηχανικοί συνασπισμοί έχουν δημιουργηθεί παράλληλα με τα παραδοσιακά Standards Developing Organizations (SDOs) για να αυξήσουν τις προσπάθειες να αξιολογηθούν, να αναπτυχθούν, να τροποποιηθούν, ή να εναρμονιστούν τα πρότυπα και τα πρωτόκολλα σχετικά με το IoT. Αυτό περιλαμβάνει, παραδείγματος χάριν, από μακρού υφιστάμενο SDOs όπως το IETF, η ITU, και IEEE, και οι συγκριτικά νέες προσπάθειες όπως η Industrial Internet Consortium, Open Interconnection Consortium, ZigBee Alliance και η AllSeen Alliance, μεταξύ πολλών άλλων.

Ο χρόνος και η επένδυση που απαιτούνται από τη βιομηχανία και άλλους συμμέτοχους για να συμμετάσχουν στο ευρύ φάσμα για την τυποποίηση οι προσπάθειες θα είναι πιθανώς δαπανηρές. Περαιτέρω, είναι πιθανό να υπάρξει

επικάλυψη και ακόμα και συγκρουόμενες στρατηγικές τυποποίησης μεταξύ μερικών προσπαθειών. Εκτός από την αύξηση των δαπανών της ανάπτυξης των προτύπων, η απουσία συντονισμού στις προσπάθειες θα μπορούσε τελικά να παραγάγει συγκρουόμενα πρωτόκολλα και την καθυστέρηση της επέκτασης προϊόντων.

Ιδιωτικότητα

Τι είναι ιδιωτικότητα;

Δεν είναι εύκολο να απαντήσει κανείς τι είναι ιδιωτικότητα και είναι μάλλον ένα ερώτημα περισσότερο φιλοσοφικό παρά τεχνολογικό. Γενικότερα, είναι η δυνατότητα ενός ατόμου ή μιας ομάδας ατόμων να απομονώνουν τους ιδίους ή πληροφορίες σχετικές με αυτούς και έτσι να «αποκαλύπτονται» επιλεκτικά. Τα όρια και το περιεχόμενο του τι θεωρείται ιδιωτικό διαφέρει μεταξύ πολιτισμών, ατόμων, ηλικιών και εποχών, αλλά μοιράζεται βασικά κοινά θέματα. Μερικές φορές η ιδιωτικότητα σχετίζεται με την ανωνυμία, δηλαδή την επιθυμία να παραμείνει κάποιος απαρατήρητος ή μη αναγνωρισθείς στο κοινό. Ο βαθμός με τον οποίο ιδιωτικές πληροφορίες εκτίθενται εξαρτάται από το πως το κοινό θα εκλάβει αυτές τις πληροφορίες. Η ιδιωτικότητα είναι ευρύτερη από την ασφάλεια και περιλαμβάνει τις έννοιες της κατάλληλης χρήσης και προστασίας των πληροφοριών [1].

Προσωπικά δεδομένα

Στα δεδομένα προσωπικού χαρακτήρα (μερικές φορές ονομάζονται και *προσωπικά στοιχεία*) περιλαμβάνεται κάθε δεδομένο που μπορεί πιθανώς να χρησιμοποιηθεί αυτόνομο ή σε συνδυασμό με άλλες πηγές, για να ταυτοποιήσεις μοναδικά, να σχετίσει ή να εντοπίσει ένα μόνο πρόσωπο. Παραδείγματα προσωπικών δεδομένων είναι:

- Πληροφορίες επικοινωνίας (όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, τηλέφωνο, ταχυδρομική διεύθυνση)
- Μορφές ταυτοποίησης (δίπλωμα οδήγησης, διαβατήριο, δαχτυλικά αποτυπώματα)
- Δημογραφικές πληροφορίες (ηλικία, φύλο, εθνικότητα, θρησκευτικές πεποιθήσεις, σεξουαλικές προτιμήσεις, ποινικό μητρώο)

- Επαγγελματικές πληροφορίες (θέση, όνομα εταιρείας)

- Πληροφορίες υγειονομικής περίθαλψης (πάροχοι, ασφάλιση, γενετικές πληροφορίες)

- Χρηματοοικονομικές πληροφορίες (τραπεζικούς και πιστωτικούς/ χρεωστικούς αριθμούς λογαριασμών, ιστορικό αγορών)

- Online δραστηριότητα (διεύθυνση IP, cookies, τα cookies flash, log-in credentials)

Ένα υποσύνολο των προσωπικών δεδομένων ορίζεται ως *ευαίσθητα προσωπικά δεδομένα* και απαιτεί ένα μεγαλύτερο επίπεδο ελέγχου όσο αφορά την συλλογή, χρήση, γνωστοποίηση και προστασία. Παραδείγματα πληροφοριών που αποτελούν ευαίσθητα προσωπικά δεδομένα είναι: 1) θρησκευτικές πεποιθήσεις 2) πολιτικές ιδέες και 3) πληροφορίες που αφορούν την υγεία. Τα ευαίσθητα προσωπικά δεδομένα περιλαμβάνουν και κάποιες μορφές ταυτοποίησης, όπως ο αριθμός κοινωνικής ασφάλισης, ορισμένα δημογραφικά δεδομένα, και πληροφορίες που μπορούν να χρησιμοποιηθούν για να αποκτήσει κάποιος πρόσβαση σε χρηματοοικονομικούς λογαριασμούς, όπως αριθμοί πιστωτικών καρτών και αριθμοί λογαριασμών σε συνδυασμό με οποιονδήποτε απαιτούμενο κωδικό ασφαλείας ή κωδικό πρόσβασης.

Ιδιωτικότητα και νομοθεσία

Από μια πιο νομική σκοπιά, σύμφωνα με τον δικηγόρο Νίκο Φραγκάκη *«η ιδιωτικότητα είναι σημείο ρήξης ανάμεσα στην ελευθερία και την ασφάλεια, λόγω της ανασφάλειας που καλλιεργείται με αφορμή την τρομοκρατία και την εγκληματικότητα, ωθώντας σε μέτρα που συρρικνώνουν τα ατομικά δικαιώματα γενικά και την ιδιωτικότητα ειδικότερα»*.

Στην Ελλάδα, η νομοθεσία διαχωρίζει τις πληροφορίες που αφορούν καθένα από εμάς σε προσωπικά δεδομένα και σε ευαίσθητα προσωπικά δεδομένα με τα δεύτερα να προστατεύονται με ποιον αυστηρό τρόπο από τον νόμο. Αξίζει να αναφερθεί πως το 2007 η χώρα μας κέρδισε μια πρωτιά που δεν πήρε τη δημοσιότητα που της αξίζει: στη «Διεθνή Κατάταξη Ιδιωτικότητας για το 2007» (καταρτίζεται κάθε χρόνο από το αμερικανικό Electronic Privacy Information Center και το αγγλικό Privacy

International, βλ. http://www.privacyinternational.org και «Ελευθεροτυπία» στις 2.1.2008) η Ελλάδα είναι πρώτη στην προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων ανάμεσα στις 27 χώρες της ΕΕ και σε άλλες 20 χώρες.[2]

Πολλές χώρες έχουν θεσπίσει νόμους για την προστασία της ιδιωτικότητας των ατόμων, όπως ο Personal Information Protection and Electronic Documents Act (PIPEDA) στον Καναδά, η οδηγία της Ευρωπαϊκής Επιτροπής σχετικά με το απόρρητο των δεδομένων και ο Swiss Federal Data Protection Ordinance. Στις Ηνωμένες Πολιτείες Αμερικής το δικαίωμα των ατόμων για ιδιωτικότητα προστατεύεται και από ρυθμιστικές αξιώσεις που αφορούν τον επιχειρηματικό τομέα όπως το Health Insurance Portability and Accountability Act (HIPAA), το Gramm-Leach-Bliley Act (GLBA), και το FCC Customer Proprietary Network Information (CPNI).

Ιδιωτηκότητα και Πληροφορική

Όσο αφορά τον χώρο της Πληροφορικής, ιδιωτικότητα *της πληροφορίας* (information privacy) ή *Ιδιωτικότητα των δεδομένων* (data privacy) είναι η συσχέτιση ανάμεσα στην συλλογή και διάδοση των δεδομένων, στην τεχνολογία, στην προσδοκία της κοινωνίας για ιδιωτικότητα και στα νομικά ζητήματα που περιβάλλουν όλα αυτά [3]. Πρόκληση στην ιδιωτικότητα των δεδομένων αποτελεί η κοινή χρήση δεδομένων προστατεύοντας ταυτόχρονα τις προσωπικές πληροφορίες που μπορούν να χρησιμοποιηθούν για να ταυτοποιηθεί κάποιο άτομο. Τα πεδία της ασφάλειας δεδομένων και της ασφάλειας πληροφοριών σχεδιάζουν και χρησιμοποιούν υλικό, λογισμικό και ανθρώπινους πόρους για να αντιμετωπίσουν αυτό το ζήτημα. Η δυνατότητα να ελέγχει κάποιος ποιες πληροφορίες αποκαλύπτονται για τον ίδιον μέσω του Διαδικτύου, και ποιος μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες, αποτελεί ένα ζήτημα αυξανόμενης ανησυχίας.

Η ιδιωτικότητα αποτελεί σημαντικό ζήτημα και για τις επιχειρήσεις. Επικεντρώνεται στην διασφάλιση ότι τα προσωπικά δεδομένα προστατεύονται από μη εξουσιοδοτημένη και ανάρμοστη συλλογή, χρήση και αποκάλυψή τους, και σε τελική ανάλυση στην διαφύλαξη της εμπιστοσύνης των πελατών και την παρεμπόδιση δόλιας δραστηριότητας, όπως κλοπή ταυτότητας, αποστολή ανεπιθύμητης αλληλογραφίας (spamming) και ηλεκτρονικό «ψάρεμα» (phishing)[1].

Οι πληροφορίες των πελατών μπορεί να είναι «δεδομένα χρήστη» ή/και «προσωπικά δεδομένα». Τα δεδομένα χρήστη είναι πληροφορίες που συλλέγονται από τον πελάτη και συμπεριλαμβάνουν:

- Δεδομένα που συλλέγονται απευθείας από κάποιον πελάτη (π.χ. συμπληρώνονται από τον πελάτη μέσω της διαπεφής μιας εφαρμογής)
- Δεδομένα σχετικά με κάποιον πελάτη που συγκεντρώνονται έμμεσα (π.χ. μεταδεδομένα σε έγγραφα)
- Δεδομένα σχετικά με την συμπεριφορά χρήσης του πελάτη
- Δεδομένα που σχετίζονται με το σύστημα του πελάτη (π.χ διεύθυνση IP)

Να σημειωθεί πως τα δεδομένα χρήστη μπορεί να είναι και προσωπικά δεδομένα

Παραδείγματα παραβίασης της ιδιωτικότητας

Παράδειγμα σημαντικής απειλής της ιδιωτικότητας αποτελούν τα κοινωνικά δίκτυα, τα οποία τα τελευταία χρόνια γνωρίζουν μεγάλη ανάπτυξη. Μια από τις πιο γνωστές σελίδες κοινωνικής δικτύωσης είναι και το Facebook. Σύμφωνα με στοιχεία που παρουσίασε η ελληνική μη κυβερνητική οργάνωση N.E.O.I., κατά το 2010 δέχτηκε 218 καταγγελίες, εκ των οποίων το 72% αφορούσε παραβιάσεις προσωπικών δεδομένων στο Facebook, το 16% πορνογραφικά μηνύματα στο ηλεκτρονικό ταχυδρομείο των χρηστών του διαδικτύου, το 2% σεξουαλική παρενόχληση σε προσωπικό ιστολόγιο ή ιστοσελίδα, ενώ έγιναν 6 αναφορές γονέων για εθισμό των παιδιών τους με ηλεκτρονικά παιχνίδια και αυξημένη χρήση του διαδικτύου και άλλες που αφορούσαν οικονομικές απάτες. [4]. Ενδεικτικό της έκτασης και της σοβαρότητας της κατάστασης είναι το γεγονός πως η επίτροπος της Ευρωπαϊκής Ένωσης για θέματα δικαιοσύνης προειδοποίησε εταιρείες όπως το Facebook ότι «μία εταιρεία κοινωνικής δικτύωσης που εδρεύει στις ΗΠΑ η οποία έχει εκατομμύρια ενεργών χρηστών στην Ευρώπη πρέπει να συμμορφώνεται με τους κανόνες της Ε.Ε.». Το συνολικό «πακέτο» των προτάσεων θα ανακοινωθεί το καλοκαίρι. Η επίτροπος δήλωσε πως σκοπεύει να αναγκάσει το Facebook και άλλους παρεμφερείς δικτυακούς τόπους να καθιερώσουν υψηλά standard προστασίας προσωπικών δεδομένων και να δώσουν στο χρήστη πλήρη έλεγχο σχετικά με το υλικό που διατίθεται online.[5]

Μια γνωστή εταιρεία που επανειλημμένως έχει δεχθεί καταγγελίες για παραβιάσεις της ιδιωτικότητας των χρηστών είναι η Google. Πρόσφατα η Γαλλία μήνυσε την Google με το ποσό των €100,000 για την συλλογή δεδομένων από ιδιωτικά Wi-Fi δίκτυα κατά την διάρκεια συγκέντρωσης εικόνων για την Google Street View. Η Google Street View είναι μια υπηρεσία των Google Maps και Google Earth που προσφέρει πανοραμική θέα από διάφορες θέσεις κατά μήκος πολλών δρόμων ανά τον κόσμο. Ξεκίνησε στις 25 Μαΐου του 2007, αρχικά μόνο σε κάποιες πόλεις στις Ηνωμένες Πολιτείες, και έκτοτε βαθμιαία επεκτάθηκε ώστε να περιλαμβάνει περισσότερες πόλεις και αγροτικές περιοχές απ' όλο τον κόσμο. Η Google Street View εμφανίζει εικόνες που λαμβάνονται από ειδικά εξοπλισμένα αυτοκίνητα. Σε κάθε ένα από αυτά τα αυτοκίνητα υπάρχουν 9 ειδικές κάμερες, GPS και 3G/GSM/Wi-Fi κεραίες για την ανίχνευση 3G/GSM και Wi-Fi hotspots. Η Google Street View αμφισβητήθηκε από την αρχή της λειτουργίας της. Σε πολλούς δεν άρεσε το γεγονός πως η Google μπορούσε να συγκεντρώνει εικόνες από κτήρια, πινακίδες και πρόσωπα. Η εταιρεία απάντησε αποκρύπτοντας ευαίσθητα κομμάτια των εικόνων. Όμως τον Μάιο του 2010 αποκαλύφθηκε πως τα ειδικά εξοπλισμένα αυτοκίνητα που χρησιμοποιούνται για την υπηρεσία, συνέλλεξαν και αποθήκευσαν δεδομένα από ιδιωτικά κρυπτογραφημένα Wi-Fi δίκτυα. Το γεγονός αποδόθηκε σε λάθος. Τον Αύγουστο του 2010, η γαλλική αστυνομία σταμάτησε ένα από τα αυτοκίνητα της Google Street View ύστερα από εντολή της Εθνικής Επιτροπής για την Πληροφορική και τις Ατομικές Ελευθερίες (National Commission for Computing and Civil Liberties-CNIL) για να επιθεωρήσει το κατά πόσον η Google εξακολουθεί να συλλέγει Wi-Fi δεδομένα. Η CNI δήλωσε πως η εταιρεία δεσμεύτηκε να διαγράψει τα δεδομένα που είχε συλλέξει, αλλά διαπίστωσε πως δεν απέτρεψε τελικά την χρήση των δεδομένων που συλλέχτηκαν, χωρίς όμως οι χρήστες να το γνωρίζουν. Τον Ιούλιο του 2010 η Google δήλωσε πως τα αυτοκίνητα δεν θα συλλέγουν πλέον καθόλου πληροφορίες, αλλά οι επιπτώσεις από το ατύχημα υπενθυμίζουν πόσο δυσάρεστες μπορεί να γίνουν οι συνέπειες από τον μη σεβασμό της ιδιωτικότητας των χρηστών, ειδικά για εταιρείες του βεληνεκούς της Google. [6]

Ένα από τα πιο πρόσφατα τεχνολογικά επιτεύγματα είναι το iPhone4. Διατέθηκε στην αγορά στις 24 Ιουνίου του 2010. Τον Απρίλιο του 2011 έγινε γνωστό πως η συσκευή κατέγραφε δεδομένα σχετικά με την θέση των χρηστών της χωρίς οι ίδιοι να το γνωρίζουν. Η καταγραφή έγινε μέσω του αρχείου με την ονομασία "consolidated.db",

και αφορούσε σημεία ασύρματης πρόσβασης (Wi-Fi hotspot) και κεραίες του δικτύου κινητής τηλεφωνίας στην ακτίνα του κατόχου του smartphone (όχι τα ακριβή σημεία όπου βρισκόταν, αφού όπως υποστηρίζει η Apple μπορεί να είναι πολύ μακριά) επί έναν ολόκληρο χρόνο. Μάλιστα τα στοιχεία αυτά χρησιμοποίησαν οι ερευνητές Alasdair Allan και Pete Warden για να αναπαράγουν ζωντανά σε χάρτη τις μετακινήσεις ενός κατόχου iPhone επί ένα χρόνο. Σύμφωνα με την εταιρεία, η καταγραφή ήταν αποτέλεσμα λάθους στο σχεδιασμό του λειτουργικού της συστήματος και επιφυλάχτηκε να το διορθώσει. Πράγματι, μέσα σε μια εβδομάδα διατέθηκε η ενημέρωση 4.3.3 του iOS για iPhone και το iPad 3G (μέσω σύνδεσης στο iTunes). Η Apple είχε απαντήσει σε ερωτήματα σχετικά με τις υπηρεσίες εντοπισμού θέσεως ενώπιον του αμερικανικού Κογκρέσου. Συγκεκριμένα, είχε δικαιολογήσει την καταγραφή των Wi-Fi hotspot και των κεραιών καθώς την αξιοποιούσε ώστε οι εφαρμογές πλοήγησης να ανταποκρίνονται ταχύτερα στα αιτήματα του χρήστη, σε σχέση με την αναζήτηση δορυφόρων (GPS). Εντούτοις, δεν είχε απαντήσει στο ερώτημα γιατί κατέγραφε την ημερομηνία και την ώρα κατά την οποία «πέρασε» ο κάτοχος του κινητού από κάθε σημείο (εξάλλου, η εμβέλεια των Wi-Fi δεν είναι τόσο μεγάλη). Μετά την ενημέρωση του λειτουργικού με την πρώτη διόρθωση, τα δεδομένα θα καταγράφονται μόνο για επτά ημέρες. Μετά τις διαμαρτυρίες αγανακτισμένων χρηστών, η Apple είχε υποσχεθεί ότι δεν θα επιτρέπεται η λήψη αντιγράφων ασφαλείας του επίμαχου αρχείου με τα δεδομένα θέσης σε ηλεκτρονικό υπολογιστή (που θεωρούνται επιρρεπή σε κακόβουλες επιθέσεις). Μια άλλη διόρθωση είναι η κρυπτογράφηση του αρχείου (και στο iPhone4) και η απενεργοποίηση της καταγραφής των σημάτων στα διαθέσιμα σημεία πρόσβασης όταν οι χρήστες έχουν επιλέξει να απενεργοποιήσουν πλήρως όλες τις υπηρεσίες που χρειάζονται δεδομένα θέσης. Σε κάθε περίπτωση, η εταιρεία υποστηρίζει ότι τα δεδομένα θέσης των χρηστών που επιστρέφουν σε αυτή είναι ανώνυμα. Επίσης, τα δεδομένα θέσης μπορεί να είναι διαθέσιμα σε εταιρείες που παρέχουν τοπικές υπηρεσίες μέσω εφαρμογών για το iPhone4, αν και, για να συμβεί αυτό, απαιτείται η συναίνεση του χρήστη. Το ίδιο ισχύει και για τη διάθεση των στοιχείων θέσης σε διαφημιζόμενους μέσω της πλατφόρμας της Apple, iAd. Πάντως ανησυχίες για το ίδιο θέμα εκφράζονται και για τα κινητά με Android, με την Google Inc. να παραδέχεται ότι πράγματι αποθηκεύονται δεδομένα θέσης για σύντομο χρονικό διάστημα από χρήστες που έχουν επιλέξει να χρησιμοποιούν υπηρεσίες GPS. [7]

Η προστασία της ιδιωτικότητας είναι ένα σύνθετο πρόβλημα. Η λύση του προϋποθέτει συνδυασμό τεχνολογικών επιτευγμάτων και υιοθέτηση κατάλληλου ρυθμιστικού πλαισίου. Καθώς το Διαδίκτυο και η χρήση του ενσωματώνεται όλο και περισσότερο στην καθημερινότητά μας, τα προβλήματα ιδιωτικότητας θα αυξάνονται ποσοτικά αλλά και ποιοτικά, καθώς θα προκύπτουν και νέες είδους απειλές. Στο πλαίσιο αυτό μία από αυτές τις νέες απειλές αποτελεί και το «νέφος».

Με την εξάπλωση των εφαρμογών του νέφους μεγαλώνουν και τα προβλήματα ιδιωτικότητας. Η σημασία των προβλημάτων αυτών είναι ανάλογη της σημασίας των εφαρμογών «νέφους» για τους χρήστες. Ένα σημαντικό όπλο για την προστασία της ιδιωτικότητας αποτελούν οι νέες μορφές των ηλεκτρονικών ταυτοτήτων διότι αν δεν ληφθούν κατάλληλα μέτρα το γεγονός πως ένας χρήστης έχει όλα τα στοιχεία του σε μια κάρτα ίσως να είναι επικίνδυνο. Έχουν γίνει διάφορες προσπάθειες για να υλοποιηθεί η προσέγγιση της «ελάχιστης αποκάλυψης». Πριν λίγους μήνες άρχισε σε ερευνητικό επίπεδο το έργο ABC4Trust. Πριν όμως αναφερθούμε αναλυτικότερα στο ABC4Trust θα περιγράψουμε τα Attribute Based Διαπιστευτήρια.

Attribute Based Διαπιστευτήρια

Ο αριθμός των ηλεκτρονικών συναλλαγών που πραγματοποιούμε καθημερινά αυξάνεται διαρκώς. Από ηλεκτρονικό εμπόριο και e-banking μέχρι δοσοληψίες με κυβερνητικούς φορείς. Σχεδόν όλες οι εφαρμογές και οι υπηρεσίες που βασίζονται σε συστήματα ηλεκτρονικών υπολογιστών απαιτούν κάποια αυθεντικοποίηση (authentication) για την δημιουργία έμπιστων σχέσεων, είτε μόνο για το ένα άκρο της επικοινωνίας είτε και για τα δύο. Ορισμένες χώρες έχουν ήδη θεσπίσει ή πρόκειται να θεσπίσουν τις ηλεκτρονικές ταυτότητες (electronic Identity). Ηλεκτρονικά εισιτήρια και συστήματα διοδίων χρησιμοποιούνται ευρέως σε όλο τον κόσμο. Καθώς οι ηλεκτρονικές συσκευές που απαιτούν ταυτοποίηση και αυθεντικοποίηση έχουν εξαπλωθεί ευρέως σε ένα ευρύ χάσμα σεναρίων, η ιδιωτικότητα του χρήστη θα απειλείται όλο και περισσότερο στην μελλοντική κοινωνία του Διαδικτύου.

Ποια όμως είναι τα μέσα για την προστασία της ιδιωτικότητας των χρηστών; Τα ηλεκτρονικά διακριτικά ελέγχου ταυτότητας (authentication tokens) [1] καθώς και οι μηχανισμοί που παρέχουν είναι πολύ γνωστά επειδή δεν χρησιμοποιούνται μόνο στο Ίντερνετ αλλά και αλλού. Πράγματι, οι ηλεκτρονικές ταυτότητες, η αυθεντικοποίηση

από κινητά τηλέφωνα και τα RFID διακριτικά [2] εξαπλώνονται γρήγορα. Αυτοί οι μηχανισμοί αυθεντικοποίησης δυστυχώς έχουν την αδυναμία πως χρησιμοποιούν μοναδικά αναγνωριστικά τα οποία παρουσιάζουν τον κίνδυνο ότι μπορούν να συνδέσουν διάφορες συναλλαγές με τον ίδιο τον χρήστη, με αποτέλεσμα να απειλείται σοβαρά η ιδιωτικότητα του. Ένας άλλος διαδεδομένος μηχανισμός είναι η αυθεντικοποίηση με την χρήση κωδικών πρόσβασης που όμως παρουσιάζει πολλές αδυναμίες. Τα κρυπτογραφικά πιστοποιητικά (cryptographic certificates) παρόλο που μπορούν να προσφέρουν επαρκή ασφάλεια για αρκετούς σκοπούς, δεν καλύπτουν τις ανάγκες της ιδιωτικότητας γιατί συνδέονται μ' ένα υπαρκτό πρόσωπο. Οποιαδήποτε χρήση ενός τέτοιου πιστοποιητικού εκθέτει την ταυτότητα του κατόχου στο μέρος που ζητά την αυθεντικοποίηση. Υπάρχουν πολλά σενάρια όπου η χρήση τέτοιων πιστοποιητικών αποκαλύπτει την ταυτότητα του κατόχου χωρίς να είναι απαραίτητο, για παράδειγμα σενάρια όπου η πλατφόρμα μιας υπηρεσίας χρειάζεται μόνο να εξακριβώσει την ηλικία ενός χρήστη και όχι την πραγματική του/της ταυτότητα. Η αποκάλυψη περισσότερων πληροφοριών από τις απαραίτητες όχι μόνο ζημιώνει την ιδιωτικότητα των χρηστών αλλά αυξάνει και το ρίσκο κακής χρήσης των πληροφοριών του, όπως κλοπή ταυτότητας, όταν οι πληροφορίες πέσουν σε λάθος χέρια.

Τα κλασσικά διαπιστευτήρια (credentials) λοιπόν δεν σέβονται την ιδιωτικότητα. Κατά κανόνα αποκαλύπτουν την ταυτότητα του κατόχου του διαπιστευτηρίου, παρόλο που συχνά η εφαρμογή απαιτεί λιγότερη πληροφορία, για παράδειγμα μόνο την επιβεβαίωση ότι ο κάτοχος είναι έφηβος ή δικαιούται κοινωνικές παροχές. Σε αντίθεση με αυτό, τα Attribute-based Διαπιστευτήρια (Attribute Based Credentials – ABC) επιτρέπουν στον κάτοχο να αποκαλύψει μόνο την ελάχιστη πληροφορία που απαιτείται από την εφαρμογή, χωρίς να αποκαλύπτουν μια πλήρη ταυτότητα. Αυτά τα διαπιστευτήρια διευκολύνουν έτσι την υλοποίηση μιας αξιόπιστης ψηφιακής κοινωνίας που ταυτόχρονα προστατεύει την ιδιωτικότητα. Τα τελευταία 25 χρόνια έχουν αναπτυχθεί μια σειρά από τεχνολογίες για την κατασκευή ABC συστημάτων με έναν τρόπο ώστε να είναι έμπιστα, όπως τα κρυπτογραφικά πιστοποιητικά, ενώ ταυτόχρονα να προστατεύουν την ιδιωτικότητα του κατόχου τους (π.χ. αποκρύπτοντας την πραγματική ταυτότητα του κατόχου τους). Τέτοια Attribute-based Διαπιστευτήρια εκδίδονται όπως τα κρυπτογραφικά διαπιστευτήρια (π.χ. τα X.509 διαπιστευτήρια) χρησιμοποιώντας ένα ψηφιακό (μυστικό) κλειδί υπογραφής

(signature key). Ένα Attribute Based Διαπιστευτήριο επιτρέπει στον κάτοχό του να το μετατρέψει σ' ένα νέο διαπιστευτήριο που περιέχει μόνο ένα υποσύνολο των χαρακτηριστικών (attributes) που περιέχονται στο αρχικό διαπιστευτήριο. Αυτά τα διαπιστευτήρια μπορούν να επαληθευτούν όπως τα κοινά κρυπτογραφικά διαπιστευτήρια (χρησιμοποιώντας το δημόσιο κλειδί επαλήθευσης του εκδότη) και προσφέρουν την ίδια ασφάλεια .Οι τεχνολογίες ABC, που συχνά ονομάζονται στην βιβλιογραφία ανώνυμα συστήματα διαπιστευτηρίων, επιτρέπουν σ' έναν πάροχο υπηρεσιών ταυτότητας (identity service provider) να εκδώσει ένα διαπιστευτήριο (ή πιστοποιητικό) σ' έναν χρήστη. Αυτό το διαπιστευτήριο περιέχει χαρακτηριστικά του χρήστη όπως διεύθυνση ή ημερομηνία γέννησης αλλά και τα δικαιώματα του χρήστη ή ρόλους του ως χαρακτηριστικά. Χρησιμοποιώντας το διαπιστευτήριο, ο χρήστης μπορεί να αποδείξει σ' ένα τρίτο μέρος (a third party) ότι έχει στην κατοχή του ένα διαπιστευτήριο που περιέχει ένα συγκεκριμένο χαρακτηριστικό ή ρόλο χωρίς να αποκαλύπτει άλλες πληροφορίες που είναι αποθηκευμένες στο διαπιστευτήριο. Για παράδειγμα, ο χρήστης μπορεί να χρησιμοποιήσει ένα ανώνυμο ID διαπιστευτήριο που έχει εκδοθεί από την κυβέρνηση για να αποδείξει πως είναι ενήλικας, δηλαδή πως έχει ένα διαπιστευτήριο που περιέχει μια ημερομηνία γέννησης που είναι μεγαλύτερη από 18 χρόνια πριν. Ως εκ τούτου, τα ανώνυμα διαπιστευτήρια (anonymous credentials) υπόσχονται να είναι ο ακρογωνιαίος λίθος για την προστασία της ιδιωτικότητας του χρήστη σ' ένα ηλεκτρονικό περιβάλλον.

Βιβλιογραφία

[1] http HYPERLINK "http://en.wikipedia.org/wiki/Privacy":// HYPERLINK "http://en.wikipedia.org/wiki/Privacy"en HYPERLINK "http://en.wikipedia.org/wiki/Privacy". HYPERLINK "http://en.wikipedia.org/wiki/Privacy"wikipedia HYPERLINK "http://en.wikipedia.org/wiki/Privacy". HYPERLINK "http://en.wikipedia.org/wiki/Privacy"org HYPERLINK "http://en.wikipedia.org/wiki/Privacy"/ HYPERLINK "http://en.wikipedia.org/wiki/Privacy"wiki HYPERLINK "http://en.wikipedia.org/wiki/Privacy"/ HYPERLINK "http://en.wikipedia.org/wiki/Privacy"Privacy

[2]http HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ ΤΕΥΧΟΣ&spid=1478&cs=1":// HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ ΤΕΥΧΟΣ&spid=1478&cs=1"www HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ ΤΕΥΧΟΣ&spid=1478&cs=1". HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ ΤΕΥΧΟΣ&spid=1478&cs=1"vimaideon HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ ΤΕΥΧΟΣ&spid=1478&cs=1". HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ ΤΕΥΧΟΣ&spid=1478&cs=1"gr HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ ΤΕΥΧΟΣ&spid=1478&cs=1"// HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ ΤΕΥΧΟΣ&spid=1478&cs=1"Article HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ ΤΕΥΧΟΣ&spid=1478&cs=1". HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=ΚΥΠΙΟ

TEYXOΣ&spid=1478&cs=1"aspx HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"? HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"d HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"=20080201 HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"& HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"nid HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"=7342365 HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"& HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"sn HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"=KYPIO%20TEYXOΣ HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"& HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"spid HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"=1478 HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"& HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"cs HYPERLINK "http://www.vimaideon.gr/Article.aspx?d=20080201&nid=7342365&sn=KYPIO TEYXOΣ&spid=1478&cs=1"=1

[3] http://en.wikipedia.org/wiki/Information_privacy, retrieved 28 Feb 2009.

[4] http://news.pathfinder.gr/scitech/681381.html

[5] http://www.mediasoup.gr/node/28381

[6] http://mashable.com/2011/03/21/france-fine-google-street-view/

[7] http://tech.in.gr/news/article/?aid=1231106844