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

Πτυχιακή Εργασία

ΤΟ INTERNET ΤΩΝ ΠΡΑΓΜΑΤΩΝ – INTERNET OF THINGS

Παπαγρίβας Ελευθέριος & Φραγκουλάκης Γεώργιος
Επιβλέπων καθηγητής: Μιχαήλ Παρασκευάς

Αντίρριο, Νοέμβριος 2016

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή
Αντίρριο, 4 Νοεμβρίου 2016

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ
1. Παρασκευάς Μιχαήλ
2. Ασάφης Ηλίας
3. Τσακανίκας Βασίλειος

Ευχαριστίες

Για τις συμβουλές του και την καθοδήγησή του καθ' όλη την διάρκεια των σπουδών μου καθώς και την για την επίβλεψη της παρούσας πτυχιακής εργασίας οφείλω να ευχαριστήσω τον καθηγητή μου κ. Μιχαήλ Παρασκευά.

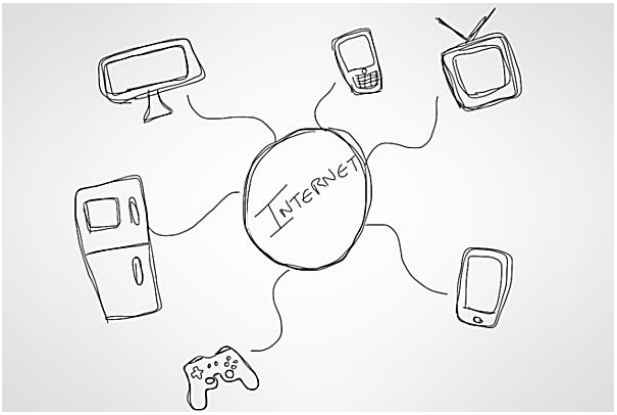
Αφιέρωση

Στην τεχνολογία, στην επιστήμη, στο μέλλον.

Πίνακας Περιεχομένων

1. Εισαγωγή στο Internet Of Things

Σύμφωνα με την έκθεση της McKinsey «Επαναστατικές τεχνολογίες : Οι πρόοδοι που θα μεταμορφώσουν τη ζωή, τις επιχειρήσεις και την παγκόσμια οικονομία» , **το Internet of Things (IOT) είναι μία από τις τρεις κορυφαίες τεχνολογικές εξελίξεις της επόμενης δεκαετίας** (μαζί με το Mobile Internet και την αυτοματοποίηση του knowledge work). Η έκθεση επισημαίνει ότι «το Internet of Things» είναι μια σαρωτική έννοια που αποτελεί πρόκληση ακόμα και να φανταστείς όλους τους πιθανούς τρόπους με τους οποίους θα οι επιχειρήσεις, οι οικονομίες ή και η κοινωνία θα επηρεαστούν. Κάποιες από τις αλλαγές που θα φέρει το IOT είναι: η επικοινωνία της μηχανής με μηχανή (MTM), η επικοινωνία της μηχανής με μία ολόκληρη υποδομή συστημάτων, η επικοινωνία της μηχανής με το περιβάλλον καθώς και η επικοινωνία με οποιαδήποτε εν δυνάμει «έξυπνη» συσκευή μέσω αισθητήρων.

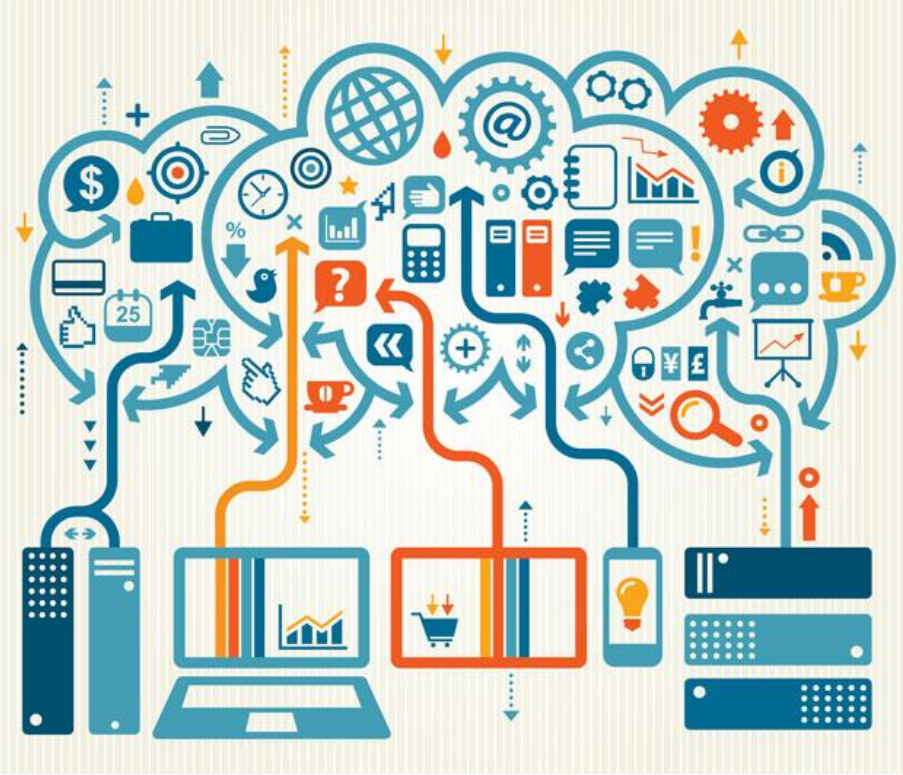


Ένα παράδειγμα επικοινωνίας μέσω αισθητήρων, είναι η ενσωμάτωση αισθητήρων στα φυσικά αντικείμενα, συνδέοντας μέσω ενσύρματων και ασύρματων δικτυών, χρησιμοποιώντας συχνά το ίδιο πρωτόκολλο Internet (IP) που συνδέει το Διαδίκτυο, καθιστά την δυνατότητα όλα τα αντικείμενα μπορούν να επικοινωνήσουν μεταξύ τους αλλά και με άλλα αντικείμενα. Με αυτό το παράδειγμα διαφοροποιούμαστε από την ιδέα ότι η επικοινωνία μπορεί να επιτευχθεί μόνο μέσω υπολογιστή και ενός έξυπνου κινητού τηλεφώνου. Με αυτόν το νέο τρόπο επικοινωνίας – μέσω αισθητήρων –, η συνδεσμολογία ποικίλει από συνδεδεμένα σπίτια και πόλεις μέχρι συνδεδεμένα αυτοκίνητα και μηχανήματα. **Οι συσκευές που θα παρακολουθούν τη συμπεριφορά ενός ατόμου θα χρησιμοποιούν τα δεδομένα που συλλέγονται για ένα νέο είδος υπηρεσιών.**

«**Συσκευές «ινκόγκνιτο» σε δημόσιους και ιδιωτικούς χώρους θα αναγνωρίζουν τους κατοίκους μιας έξυπνης πόλης και θα προσαρμόζονται στις απαιτήσεις αυτών για την άνεση, την ασφάλεια, το βελτιωμένο εμπόριο, την ψυχαγωγία, την εκπαίδευση, τη εξοικονόμηση των πόρων, τη λειτουργική αποδοτικότητα και την προσωπική ευημερία**», σύμφωνα με την έκθεση της Intel, "Rise of the Embedded Internet".

Αναμφίβολα το Internet of Things δημιουργείται και αναπτύσσεται ταχύτατα και οι δυνατότητες που προσφέρει είναι τεράστιες καθώς το δίκτυο για την επικοινωνία αυτόν τον έξυπνων συσκευών και διαφόρων ηλεκτρονικών «πραγμάτων», δημιουργεί ένα παγκόσμιο νευρωτικό δίκτυο επικοινωνίας, το οποίο είναι βασισμένο στο Internet(IP) και το Cloud. Οι συσκευές αυτές και ο τρόπος επικοινωνίας αυτών μέσα από το cloud θα διεισδύσει σε κάθε πτυχή της ζωής μας , λόγο της έξυπνης διαχείρισης και επεξεργασίας των πληροφοριών, που θα μπορούν να συλλέξουν και ν' αναλύσουν οι συσκευές του IOT μεταξύ τους. Σαν αποτέλεσμα αυτού, μεγάλες ποσότητες πληροφοριών θα μεταφέρονται μέσα από το δίκτυο και θα καταλήγουν σε συστήματα ή συσκευές στις οποίες μπορούμε να προγραμματίσουμε και να ελέγξουμε. Σκοπός είναι συλλογή αυτών των πληροφοριών για να διευκολυνθεί ο τρόπος ζωής, να δημιουργηθούν νέες ευκαιρίες και υπηρεσίες προς όφελος του ανθρώπου και να μειωθεί η κατακρεούργηση του περιβάλλοντος.

Όπως προαναφέρθηκε, οι δυνατότητες που προσφέρει το IOT είναι τεράστιες, με νέες ιδέες υλοποίησης και με έναν δυναμικό τρόπο θα επηρεάσει τις ζωές όλων των ανθρώπων. Για αυτόν τον λόγο οργανισμοί όπως Alliance of IOT Innovations, Internet Society Releases Internet of Things, και διάφοροι άλλοι οργανισμοί, έχουν δημιουργηθεί για να βοηθήσουν στην μετάβαση αυτής, της νέας εποχής του IOT .



2. Ιστορική Αναδρομή

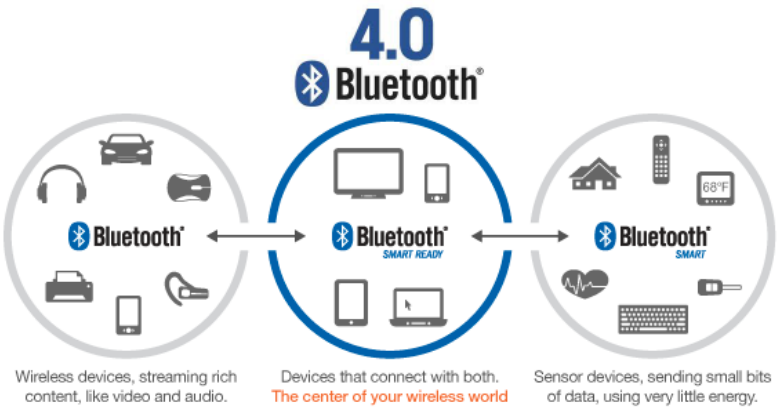
Το παραπάνω παράδειγμα, με τις συσκευές να αλληλοεπιδρούν με ευρεία γκάμα συσκευών και με το περιβάλλον, σε πολλούς χρήστες θα φαίνεται ουτοπικό και καινοτόμο, ότι η τεχνολογία αναπτύχθηκε βίαια στα πρόθυρα της νέας γενιάς του IOT , για να επιτρέψει την ασύγχρονη επικοινωνία αυτών των συσκευών, **όμως το IOT άρχιζε να υφίσταται σαν μια αόριστη σκέψη ήδη από το 1950.**

- Οι μηχανικοί της IBM είχαν την ανάγκη να ορίσουν ταυτότητες σε κάθε αντικείμενο και μηχάνημα που χρησιμοποιούσαν στην επιχείρηση . Η διαρκής ενασχόληση και οι πειραματισμοί με γραμμικά σχήματα, οδήγησαν στην ανακάλυψη των **Barcodes**. Νέοι πειραματισμοί από μηχανικούς και επιστήμονες ακολούθησαν σε επίπεδο hardware και κινητών φορητών συσκευών τις οποίες μπορείς να φοράς στον καρπό σου (**wearables**). Η πρώτη και αξιοσημείωτη συσκευή του Edward O. Throrp το **1955** ο οποίος κατασκεύασε ένα **ρολόι** το οποίο πρόβλεπε τους κύκλους που έκαναν οι ρουλέτες στα καζίνα του Las Vegas μέσα από περίπλοκους αλγορίθμους.

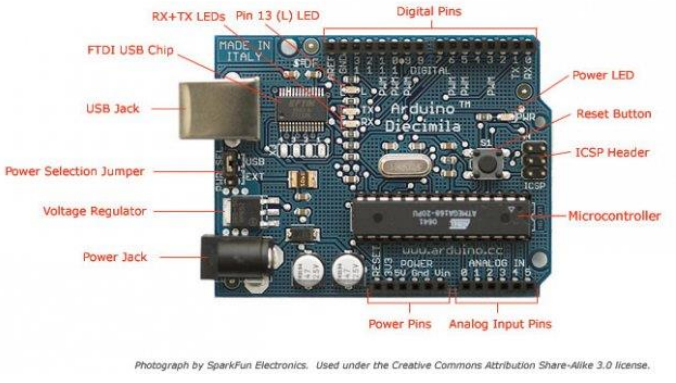
- Το **1967** από τον **Hubet Upton** δημιουργήθηκε η πρώτη συσκευή σε σχήμα μυωπικών γυαλιών η οποία βοηθούσε τα άτομα με ειδικές ανάγκες να διαβάζουν τα χείλια των ανθρώπων. Το 2011 η εταιρία Google εμπνεύστηκε από την ιδέα του Hubert και δημιούργησε το project Google Glass με στοιχεία από αυξημένη πραγματικότητα.

- **Τρία χρόνια μετά**, με την δημιουργία του δικτύου **ARPANET** για την επικοινωνία και ανταλλαγή δεδομένων ανάμεσα στις στρατιωτικές βάσεις των ΗΠΑ**, στάλθηκε το πρώτο μήνυμα απομακρυσμένων υπολογιστών.** Ήταν το πρώτο δίκτυο που σήμανε μια νέα εποχή δικτύωσης, και το ξεκίνημα για την εποχή του Internet που διανύουμε.
- Το 1982 ήταν η γενιά του Internet και του πρωτόκολλου TCP/IP, το οποίο πέρασε από την διαδικασία για να γίνει πρότυπο (standard). Με το πρωτόκολλο TCP/IP ξετυλίγεται μια νέα εποχή, ενός παγκόσμιου ιστού, και δίκτυα που ενώνονται μεταξύ τους, για να δημιουργηθεί το διαδίκτυο όπως το ξέρουμε σήμερα.
- Η τεχνολογία του RFID που θα χρησιμοποιηθεί κατά κόρων στην εποχή του Internet of Things, είναι η τεχνολογία που μας επιτρέψει την ασύρματη αλλά παθητική ανάγνωση και εγγραφή δεδομένων σε συσκευές. Η τεχνολογία αυτήν δημιουργήθηκε τον Ιανουάριο του **1973** από τον Mario Cardullo και όμως η ευρεία χρήση του RFID, κυρίως στον επιχειρησιακό κλάδο ξεκίνησε το 2013 με την πολυεθνική Inditex, να χρησιμοποιεί την τεχνολογία μαζικά σε όλα τα καταστήματα της, και εν συνεχεία με άλλες επιχειρήσεις να ασπάζονται το όραμα του Internet of Things.
- **Μια δεκαετία μετά**, αναπτύχθηκε η σκέψη επικοινωνίας «**machine to machine**» από φοιτητές του Πανεπιστημίου Carnegie Mellon της Pennsylvania. Εγκατέστησαν μηχανισμούς για την παρακολούθηση θερμοκρασίας από τερματικούς υπολογιστές, στα μηχανήματα αυτόματων πολιτών που υπήρχαν στο Πανεπιστήμιο.
- Το **1990** ο υπάλληλος Mark Weiser της Xerox Parc δημοσίευσε στον αμερικάνικο τύπο άρθρο για την εξέλιξη των υπολογιστών του 21^{ου} αιώνα και χρησιμοποίησε όρους ”καθολικών συστημάτων” και “ενσωματωμένα συστήματα επαυξημένης πραγματικότητας”.
- Ενώ το **1995** η **Siemens** ανακοίνωσε το πρώτο **chip** το οποίο μέσω δικτύου GSM επιτρέπει βιομηχανικά συστήματα να επικοινωνούν μεταξύ τους ασύρματα και να εκτελούν εντολές, ενώ η IEEE ξεκίνησε το πρώτο διεθνές φόρουμ για τα wearable computers.

- Το **1999** το MIT δημιουργεί το πρώτο κέντρο ερευνών με σύγχρονα συστήματα για έρευνες και μέσα σε 2 χρόνια ο David Brock ανακοίνωσε την εξέλιξη των Barcodes σε ένα νέο σύστημα ποιο έξυπνων τρόπων ανάγνωσης πληροφοριών. Αυτός ο τρόπος θα επέτρεπε τις τεχνολογίες RFID, Bluetooth και άλλες ασύρματες τεχνολογίες να τροποποιήσουν, διαβάσουν και να γράψουν δεδομένα σε αντικείμενα, μέσω ενός RFID tag. Αυτό το νέο σύστημα ονομάστηκε EPC (Electronic Product Code). Ο Ashton ο οποίος δούλευε στην βελτιστοποίηση της εφοδιαστικής αλυσίδας, ήθελε να προσελκύσει την προσοχή της διοίκησης σε μια νέα συναρπαστική τεχνολογία που ονομάζεται RFID. Ένα χρόνο μετά το Auto ID Center μετονομάστηκε σε Auto ID Labs και έγινε το πρώτο υπερσύγχρονο δίκτυο ανάπτυξης και standardizing του Internet of Things, το οποίο όνομα (Internet of Things) ανακοινώθηκε από τον Kevin Ashton μέσα στο Auto ID Center.



Στα τέλη του έτους ο Kevin έγραψε τα εξής στο περιοδικό RFID: *«Αν είχαμε υπολογιστές που ήξεραν τα πάντα και δούλευαν απροβλημάτιστα για να συλλέγουν ακόμα περισσότερα δεδομένα, χωρίς καμία βοήθεια από εμάς, θα είμαστε σε θέση να παρακολουθούμε και να «μετράμε τα πάντα», και σε μεγάλο βαθμό να μετράμε τα ποσοστά των αποβλήτων, των ζημιών και του κόστος. Θα γνωρίζουμε πότε τα πράγματα χρειάζονται αντικατάσταση, επισκευή ή ανάκληση. Πρέπει να ενισχύσουμε τους υπολογιστές με δικά τους μέσα συγκέντρωσης πληροφοριών, ώστε να μπορούν να δουν, να ακούσουν και να μυρίσουν τον κόσμο για τον εαυτό τους. Το RFID και η τεχνολογία αισθητήρων επιτρέπει στους υπολογιστές να παρατηρούν, να εντοπίζουν και να κατανοούν τον κόσμο, χωρίς να περιορίζονται από τα δεδομένα που έχουν εισαχθεί από τον άνθρωπο."*



- Το **2000** ο υπάλληλος της IBM Andy Stanforf & ο υπάλληλος Arlen Nipper της εταιρίας Eurotech δημιούργησαν το πρώτο πρωτόκολλο επικοινωνίας Machine to Machine, για συσκευές οι οποίες είναι διασυνδεδεμένες με τον ιστό. Το πρωτόκολλο ονομάστηκε από τους ίδιους MQ Telemetry Transport (MQTT), και ήταν ένα σημαντικό βήμα προς την ενίσχυση της ιδέας για το IOT
.
- Το **2005** μέλη από το πρόγραμμα **Interaction Design Institute Ivrea** κατασκευάσανε την πλατφόρμα του Arduino, για μια φτηνή λύση μικροελεγκτή που προορίζονταν για τους φοιτητές.
- Η ομάδα IPSO συντάχθηκε το **2008** με σκοπό να διαδώσουν το πρωτόκολλο IP σε όλα τα μελλοντικά σχέδια και προτάσεις του Internet of Things. Πλέον η IPSO έχει πάνω από 50 εταιρικά μέλη για την διάδοση του πρωτοκόλλου προς το μέλλον.
- **Δύο χρόνια μετά**, η τεχνολογία του Bluetooth αναβαθμίζεται και έρχεται στην αγορά ένα νέο standard με ονομασία Smart Bluetooth ή αλλιώς Bluetooth Low Energy(BLE), επιτρέποντας νέες εφαρμογές και συνδεδεμένες συσκευές στους τομείς της υγείας, άθλησης, και home entertainment να ενταχθούν στον κόσμου του IOT .
- Το **2010** πληροφορίες που διέρρευσαν σχετικά με τ' ότι η υπηρεσία της Google, Street View φωτογραφούσε 360 μοιρών φωτογραφίες και αποτύπωνε γειτονιές και δρόμους σε ηλεκτρονική μορφή, αλλά επίσης είχε αποθηκευμένους τόνους δεδομένων των δικτύων WiFi των ανθρώπων σε αυτές τις περιοχές. Οι άνθρωποι συζητούσαν αυτή την πληροφορία σαν την αρχή μιας νέας στρατηγικής της Google η οποία διχοτόμησε τις απόψεις των χρηστών του διαδικτύου, αλλά και του φυσικού κόσμου. **Την ίδια χρονιά**, η κινεζική κυβέρνηση ανακοίνωσε ότι θα κάνει το IOT να αποτελεί στρατηγική προτεραιότητα στο πενταετές σχέδιο τους.
- Ενώ το **2011**, η Gartner, η εταιρεία έρευνας της αγοράς που εφηύρε την περίφημη «διαφημιστική εκστρατεία του κύκλου για τις αναδυόμενες τεχνολογίες» περιλαμβάνεται ένα νέο στη λίστα της: «Το Internet of Things».
- Το **επόμενο έτος**, το θέμα της μεγαλύτερης ευρωπαϊκής διαδικτυακής διάσκεψης LeWeb ήταν το «Internet of Things». Ταυτόχρονα δημοφιλή περιοδικά που εστιάζουν στην τεχνολογία όπως το Forbes, το Fast Company, και το Wired άρχισαν να χρησιμοποιούν το IOT στο λεξιλόγιό τους για να περιγράψουν το νέο αυτό φαινόμενο. Την ίδια χρονιά το πρωτόκολλο του IP άλλαξε versioning και με την νέα έκτη έκδοση του υποστηρίζει περισσότερες συσκευές γρηγορότερες , αποδοτικότερες σε θέματα διασύνδεσης και με την υπόσχεση ότι μπορεί να υποστηρίξει των καλπάζοντας ρυθμό ζήτησης για διευθύνσεις έως το 2128.
- Τον Οκτώβριο του **2013**, η IDC δημοσίευσε μια έκθεση που αναφέρει ότι το IOT θα στοίχιζε $8.900 δισεκατομμύρια στην αγορά το 2020 και ο όρος Internet of Things έφτασε στη μαζική συνειδητοποίηση της αγοράς, όταν η Google ανακοίνωσε την αγορά της Nest για $3,2 δις μια εταιρία που κατασκεύαζε συσκευές για το IOT καθώς την ίδια στιγμή το Consumer Electronics Show (CES) στο Λας Βέγκας πραγματοποιήθηκε υπό το θέμα του IOT .

- Το **2014** η Apple ανακοίνωσε το HealthKit & HomeKit, δυο πλατφόρμες ανάπτυξης υλοποιήσεων και την υποστήριξη της πλατφόρμας από τις νέες συσκευές, με σκοπό η ιδέα του έξυπνου σπιτιού & τρόπο ζωής να έρθει πιο κοντά στο σήμερα. Επίσης η τεχνολογία iBeacon έφερε νέα πρότυπα στην αγορά των καταστημάτων και της πώλησης.

Όπως είδαμε στις από πάνω ιστορικές αναδρομές, τα σημεία κλειδιά για την ανάπτυξη του Internet of Things είναι η τεχνολογία του RFID και συναφείς τεχνολογίες διευθυνσιοδότησης -που αναπτύχθηκαν πρώτα στο κέντρο Auto ID Lab - καθώς και οι δυνατότητες του IPv6 θα επιτρέψουν κάθε αντικείμενο να έχει την δικιά του ξεχωριστή IP διεύθυνση, και αυτά τα αντικείμενα να «εισέλθουν» στο κόσμο του IOT .

3. Η έννοια του έξυπνου

Η κύρια δυνατότητα μιας έξυπνης συσκευής είναι η επεξεργασία δεδομένων - η οποία επιτυγχάνεται από έναν μικροεπεξεργαστή και ποικίλες θύρες επικοινωνίας - **για τον προγραμματισμό της.** Η έννοια του «έξυπνου» έγκειται στην ενσύρματη ή ασύρματη επικοινωνία της συσκευής με τον χρήστη, που λαμβάνει δράση μέσω αυτών των θυρών. Οι διάφοροι τρόποι ασύρματης επικοινωνίας και διαχείρισης της συσκευής αλλά και ο προγραμματισμός της για την αυτοματοποιημένη λειτουργία, είναι και ο κύριος λόγος χρήσης μιας έξυπνης συσκευής.

Η αντίδραση πριν από την δράση.

Η δυνατότητα των έξυπνων μηχανήματων είναι αντιστρόφως ανάλογη με την έννοιά επεξεργαστικά δυνατών. Θα ήταν λάθος να θεωρούμε ένα μηχάνημα έξυπνο γιατί προσφέρει κατασκευαστικά μεγάλες δυνατότητες στην ταχύτητα επεξεργασίας πληροφοριών. Η εφαρμογή μιας έξυπνης συσκευής μπορεί να επιτευχθεί με την επεξεργασία των δεδομένων, όχι απευθείας στην συσκευή αλλά στο Cloud.

Για παράδειγμα μια λευκή συσκευή δεν είναι αναγκασμένη να κάνει η ίδια υπολογισμούς, αλλά να είναι *έξυπνη αρκετά* ώστε να στείλει τα δεδομένα, μαζί με τις εργοστασιακές ρυθμίσεις και εξατομικευμένες επιλογές του χρήστη στο cloud προκειμένου να γίνει η επεξεργασία και να εφαρμόσει αποτέλεσμα, χωρίς την παρέμβαση του χρήστη.

Μια σημαντική σήμανση που θα αναλυθεί στα επόμενα κεφάλαια, θα είναι η εξέλιξη των δικτύων, και του cloud networking, καθώς τα δίκτυα θα πρέπει να εξελιχθούν σε πιο ασφαλή και γρήγορα, ενώ θα πρέπει να μειωθεί συγχρόνως τα κόστη και η κατανάλωση ενέργειας.

Η Ιδέα του Internet of things, περιλαμβάνει ολοκληρωμένες περιοχές συνδεσιμότητας και περιλαμβάνει σπίτια, πόλεις, αμάξια, ακόμα και δρόμους, με συσκευές να παρακολουθούν και να συλλέγουν δεδομένα και συμπεριφορές με σκοπό αυτές οι πληροφορίες να ενεργοποιούν ενέργειες και υπηρεσίες. Για παράδειγμα, το Cisco Internet of Things Group(IOT G) προβλέπει ότι θα υπάρχουν πάνω από 50 δισεκατομμύρια συνδεδεμένες

συσκευές μέχρι το 2020, ενώ οι μικροσυσκευές που θα συνδέονται στο διαδίκτυο και θα είναι μέρος του IOT θα φτάσουν σε αριθμό το ένα (1) τετράκις έως το 2025 και θα έχουν την δυνατότατά να συνδέονται με τα έξυπνα κινητά τηλέφωνα για να αφομοιώσουν ακόμα περισσότερες πληροφορίες και συνήθειες μας.

Ένα παράδειγμα τις διείσδυσης της τεχνολογίας του IOT , είναι η ποσότητα των έξυπνων συσκευών που θα διαθέτει ο κάθε άνθρωπος. Στην μέση αγορά, ο κάθε άνθρωπος έχει μια συσκευή smartphone στην κατοχή του, ενώ με το Internet of Things, ο αριθμός των έξυπνων συσκευών θα συμπεριλαμβάνει κάθε πόρτα, παράθυρο, λευκές συσκευές, ηλεκτρικές πρίζες, κλιματιστικά και διάφορες συσκευές που θα έχει στο ακίνητο του, και θα έχουν την δυνατότητα επικοινωνίας.

Έτσι η αγορά στον δυτικό κόσμο θα διχοτομηθεί και θα ξεπεράσει την αγορά των έξυπνων κινητών τηλεφώνων.

Έως εκ τούτου, από την τεχνολογική σκοπιά το Internet of Things, καθορίζεται από την δυνατότητα οι συσκευές να αλληλοεπιδρούν μεταξύ τους, με άλλα αντικείμενα, με το περιβάλλον, με ολοκληρωμένα συστήματα και υποδομές και με αυτοματοποιημένο τρόπο να εκτελούν διάφορες ενέργειες, και αυτές οι συσκευές αποτελούν την ιδέα του έξυπνου.

4. Συνδεσιμότητα

Το "Ίντερνετ των πραγμάτων" όπως αναφέρθηκε, έχει ως βάση την σύνδεση διάφορων μικρών συσκευών ή οχημάτων με ενσωματωμένους αισθητήρες και εξοπλισμό διασύνδεσης τόσο μεταξύ τους όσο και με τον κατασκευαστή, για να λαμβάνουν και να μεταδίδουν σχετικά δεδομένα με στόχο να προσφέρουν περισσότερες υπηρεσίες.

Με λίγα λόγια το IoT απεικονίζεται ως μια σειρά από νέα ανεξάρτητα ενσωματωμένα συστήματα διαστάσεων μικροτσίπ, smart συσκευές, real time systems, συστήματα συγκέντρωσης όλων των πληροφοριών σε μεγάλες βάσεις δεδομένων, που λειτουργούν με δικές τους υποδομές και χρησιμοποιούν το διαδίκτυο για τη διασύνδεση τους.

Τα τρία κύρια μέρη ενός IoT είναι:

1. τα «πράγματα», όπου συλλέγουν πληροφορίες οπουδήποτε και οποιαδήποτε στιγμή χρησιμοποιώντας RFID τεχνολογία, αισθητήρες και κώδικα
2. τα δίκτυα επικοινωνιών που συνδέουν τα «πράγματα»
3. τα υπολογιστικά συστήματα και οι εφαρμογές που επεξεργάζονται όσα δεδομένα ρέουν από και προς τα «πράγματα» όπως το cloud computing.

Η συνδεσιμότητα των τριών αυτών μερών του IoT πραγματοποιείται με τέσσερις τρόπους δικτύωσης (σύνδεσης και επικοινωνίας) όπως περιγράφονται σε έγγραφο του Internet Architecture Board - IAB (RFC 7452, Μάρτιος 2015 - https://tools.ietf.org/html/rfc7452) και παρουσιάζονται παρακάτω.

4.1 ΣΎΝΔΕΣΗ ΣΥΣΚΕΥΉ–ΠΡΟΣ–ΣΥΣΚΕΥΉ (DEVICE–TO–DEVICE COMMUNICATION)

Το μοντέλο αυτό επικοινωνίας της συσκευής προς συσκευή αντιπροσωπεύεται από δύο ή περισσότερες συσκευές που συνδέονται άμεσα και επικοινωνούν μεταξύ τους χωρίς ενδιάμεσο server. Αυτές οι συσκευές συνδέονται με πολλούς τύπους δικτύων, συμπεριλαμβανομένων των δικτύων IP ή το Internet, χρησιμοποιώντας πρωτόκολλα όπως το Bluetooth, Z-Wave, ή ZigBee.

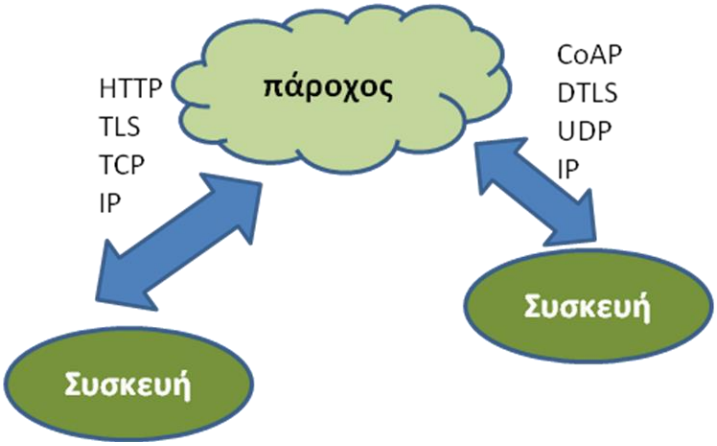
4.1 Σχεδιάγραμμα Απεικόνισης Σύνδεσης Συσκευή προς Συσκευή

Το **Bluetooth** πρόκειται για μια ασύρματη τηλεπικοινωνιακή τεχνολογία μικρών αποστάσεων, ένα πρότυπο για ασύρματα προσωπικά δίκτυα υπολογιστών (Wireless Personal Area Networks, WPAN). Το **Z-Wave** είναι ένα πρωτόκολλο ασύρματων επικοινωνιών για εφαρμογές οικιακού αυτοματισμού. Χρησιμοποιεί χαμηλής ισχύος ραδιοκύματα. Ένα πιο εξελιγμένο μέσο δικτύωσης από το Bluetooth αποτελεί το **ZigBee**. Πρόκειται για ένα τυποποιημένο πρωτόκολλο χαμηλής κατανάλωσης ισχύος σε Wireless Personal Area Networks (WPANs).Η device–to–device communication χρησιμοποιείται σε εφαρμογές όπως συστήματα οικιακού αυτοματισμού, που συνήθως χρησιμοποιούν μικρά πακέτα δεδομένων για επικοινωνία μεταξύ των συσκευών και με απαίτηση σχετικά χαμηλού ρυθμού μετάδοσης δεδομένων.

4.2 ΣΎΝΔΕΣΗ ΣΥΣΚΕΥΉΣ–ΠΡΟΣ–CLOUD (DEVICE–TO–CLOUD COMMUNICATION)

Η διασύνδεση στο IoT γίνεται εφαρμόζοντας τεχνολογίες, όπως το RFID και ασύρματους αισθητήρες, οι οποίες συλλέγουν τα δεδομένα που στη συνέχεια αξιοποιούνται από τα υπολογιστικά συστήματα. Αυτό έχει ως αποτέλεσμα την δημιουργία τεράστιων ποσοτήτων δεδομένων που θα πρέπει να αποθηκευτούν, να επεξεργαστούν και να παρουσιαστούν. Το cloud computing προσφέρει την υποδομή για τη συλλογή, ανάλυση, αποθήκευση και αποστολής πληροφοριών στον πελάτη. Έτσι επιτυγχάνεται η παροχή υπηρεσιών προς τους χρήστες που επιθυμούν την πρόσβαση σε εφαρμογές σε οποιοδήποτε χρόνο και μέρος.

Όπως φαίνεται στο σχεδιάγραμμα σε αυτό το μοντέλο, η συσκευή IoT συνδέεται άμεσα με μια υπηρεσία cloud διαδικτύου, όπως ένας πάροχος υπηρεσίας εφαρμογής για την ανταλλαγή δεδομένων και τον έλεγχο ροής των πληροφοριών.



***4.2** Σχεδιάγραμμα Απεικόνισης Σύνδεσης Συσκευής προς Cloud*

Η επικοινωνία συσκευής – παρόχου γίνεται με δυο τρόπους:

1ος τρόπος

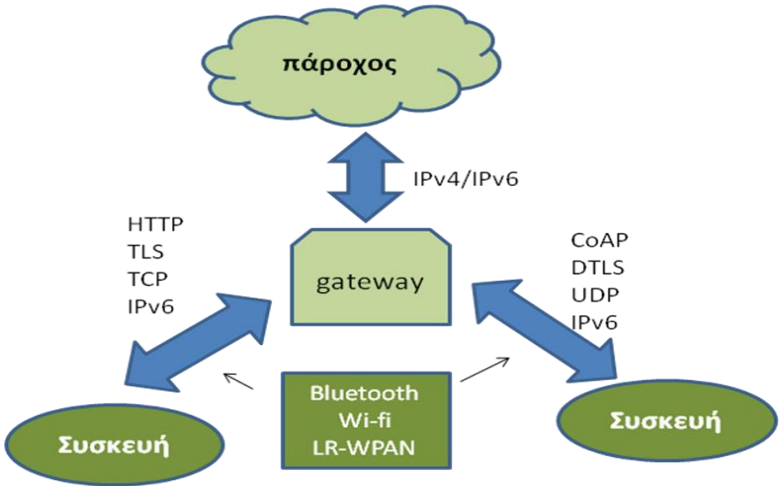
- Πρωτόκολλο Μεταφοράς Υπερκειμένου (HyperText Transfer Protocol, **HTTP**) : παρέχεται η δυνατότητα στο πρόγραμμα - πελάτης να στέλνει δεδομένα στον εξυπηρετητή.
- Το **TLS** (*Transport Layer Security*) είναι ένα πρωτόκολλο που εγγυάται ότι κατά την επικοινωνία εξυπηρετητή - πελάτη (server - client) μέσω του διαδικτύου δεν πρόκειται να μεσολαβήσει κάποιος τρίτος που θα "υποκλέψει" το περιεχόμενο της επικοινωνίας.
- Με το **TCP** (Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς) επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων.
- Το πρωτόκολλο διαδικτύου - **IP** είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων.

<u>2ος τρόπος</u>

- Οι συσκευές στις οποίες έχει εισαχθεί το Πρωτόκολλο Συσκευών Περιορισμένων Δυνατοτήτων **(CoAP)** μπορούν να λειτουργήσουν ταυτόχρονα ως εξυπηρετητές αλλά και ως πελάτες μέσα στο δίκτυο αισθητήρων. Η επικοινωνία ανάμεσα σε 2 οποιαδήποτε endpoints βασίζεται στην χρήση ενός απλού μοντέλου αιτήσεων/απαντήσεων βασισμένο στην λειτουργία του UDP. Σε αντίθεση με το HTTP το οποίο χρησιμοποιεί το TCP για τις συσκευές αυτού του τύπου είναι προτιμότερη χρήση του UDP καθώς οι απαιτήσεις για την διατήρηση των συνδέσεων υπερβαίνουν συχνά τις δυνατότητες των συσκευών.
- Το **DTLS** (datagram Transport Layer Security) παρέχει ισοδύναμη προστασία με το TLS στα πρωτόκολλα του στρώματος εφαρμογής που χρησιμοποιούν το UDP ως πρωτόκολλο μεταφοράς.
- Το πρωτόκολλο User Datagram Protocol – **UDP** είναι υπεύθυνο για τη μεταφορά δεδομένων.
- Το πρωτόκολλο διαδικτύου - **IP** είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων.

4.3 ΣΥΝΔΕΣΗ ΣΥΣΚΕΥΗΣ ΜΕ ΔΙΑΥΛΟ ΕΠΙΚΟΙΝΩΝΙΑΣ (DEVICE–TO–GATEWAY MODEL)

Σε αυτή την σύνδεση η συσκευή και ο πάροχος έρχονται σε επικοινωνία μέσω ενός διαύλου (gateway). Μια gateway συσκευή μπορεί να απορρίπτει, να αθροίζει και να ελέγχει τη μορφή των δεδομένων από μια ομάδα απλών αισθητήρων πριν τα στείλει κάπου αλλού.

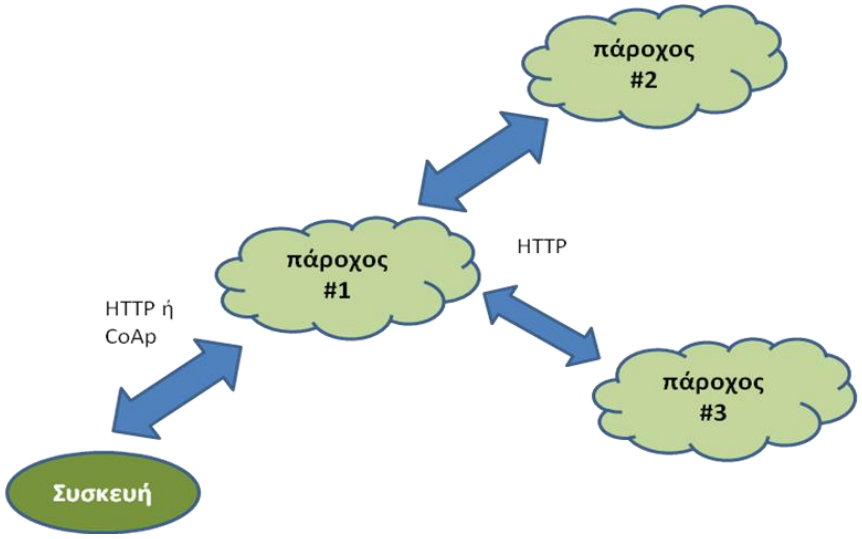


***4.3** Σχεδιάγραμμα Απεικόνισης σύνδεσης συσκευής με Δίαυλο επικοινωνίας*

Για τη σύνδεση «πράγματος» / συσκευής με το gateway ακολουθούνται οι τρόποι που περιγράφηκαν παραπάνω. Η συνδεσιμότητα gateway-cloud πραγματοποιείται με τα πρωτόκολλα IPv4/IPv6. Προτιμάται το IPv6 γιατί έχει καλύτερη δυνατότητα αυτορρύθμισης συσκευών, καλύτερη ποιότητα υπηρεσιών (QoS) και μεγαλύτερη ασφάλεια από το IPv4.

4.4 BACK – END ΜΟΝΤΈΛΟ ΑΝΤΑΛΛΑΓΉΣ ΔΕΔΟΜΈΝΩΝ (BACK – END DATA - SHARING MODEL)

Το back - end μοντέλο ανταλλαγής δεδομένων αναφέρεται σε μια αρχιτεκτονική επικοινωνίας που επιτρέπει στους χρήστες να εξάγουν και να αναλύουν τα δεδομένα των «πραγμάτων» από μια υπηρεσία cloud, σε συνδυασμό με δεδομένα από άλλες πηγές.



***4.4** Σχεδιάγραμμα Απεικόνισης Back-End Μοντέλου Ανταλλαγής Δεδομένων*

Για παράδειγμα, ένας εταιρικός χρήστης υπεύθυνος για ένα συγκρότημα γραφείων θα πρέπει να συλλέγει και να αναλύει τα δεδομένα κατανάλωσης ενέργειας και κοινής ωφέλειας που παράγονται από όλους τους αισθητήρες IoT και Internet-enabled συστήματα κοινής ωφελείας στις εγκαταστάσεις. Η back - end ανταλλαγή δεδομένων επιτρέπει στην εταιρεία να έχει εύκολη πρόσβαση και ανάλυση όλων των δεδομένων στο cloud που παράγεται από όλες τις συσκευές στο κτίριο.

5. Αρχιτεκτονική Αναφορά

Η αρχιτεκτονική των δεδομένων, δηλαδή ο τύπος των δεδομένων, η συχνότητα «ροής» αυτών στα συστήματα και στο cloud **διαφέρει** από τον τύπο δεδομένων ενός Personal Computing ή σε επικοινωνία Machine to Machine, ,με αποτέλεσμα η αρχιτεκτονική αναφορά να διαφέρει κατά κόρων από την συνηθισμένη του personal computing. Τα δεδομένα που θα παράγονται από τα έξυπνα κινητά συστήματα όπως τα wearables, και συστήματα των έξυπνων σπιτιών, θα είναι μικρά σε μέγεθος, αλλά με αυξημένη μετάδοση. Μια πολύ σημαντική δυνατότητα που μας επιτρέπει η επικοινωνία machine to machine – δηλαδή των συστημάτων που αναφερθήκαν πιο πάνω- είναι η δυνατότητα στις επιχειρήσεις να αυτοματοποιήσουν ορισμένα βασικά καθήκοντα, χωρίς να εξαρτώνται από τις κεντρικές ή cloud-based εφαρμογές και υπηρεσίες. Αυτά τα χαρακτηριστικά παρέχουν ευκαιρίες για να συλλεχθεί ένα ευρύ φάσμα δεδομένων αλλά και να υπάρχουν προκλήσεις όσον αφορά τον σχεδιασμό της δικτύωσης για αυτήν την νέα αρχιτεκτονική πληροφορίας. Ενώ το IoT είναι μακράν ο πιο δημοφιλής όρος για να περιγράψει το φαινόμενο του συνδεδεμένου κόσμου, υπάρχουν παρόμοιες έννοιες που αξίζουν κάποια προσοχή. Οι περισσότερες από αυτές τις έννοιες είναι παρόμοιες σε έννοια αλλά όλες έχουν ελαφρώς διαφορετικούς ορισμούς και διαφορετική αρχιτεκτονική. Η αρχιτεκτονική και τα πρωτόκολλά επικοινωνίας Machine to Machine (M2M) είναι σε χρήση για περισσότερα από μια δεκαετία, και είναι γνωστό στον τομέα των τηλεπικοινωνιών. Η M2M επικοινωνία ήταν αρχικά μια σύνδεση one-to-one, συνδέοντας ένα μηχάνημα στο άλλο, αλλά η σημερινή «*έκρηξη*» της συνδεσιμότητας της κινητής τηλεφωνίας σημαίνει ότι τα δεδομένα μπορούν πλέον να μεταδοθούν πιο εύκολα, μέσω ενός συστήματος δικτύων IP, σε ένα πολύ ευρύτερο φάσμα συσκευών.

Το Industry 4.0 περιγράφει ένα σύνολο από έννοιες που θα οδηγήσουν στην επόμενη βιομηχανική επανάσταση. Περιλαμβάνει όλα τα είδη των εννοιών συνδεσιμότητας αλλά προχωρεί περαιτέρω περιλαμβάνοντας πραγματικές αλλαγές στο φυσικό κόσμο γύρω μας, όπως η τεχνολογία 3D εκτύπωσης, τα υλικά νέας επαυξημένης πραγματικότητας, η ρομποτική, και τα προηγμένα υλικά. Το 2009 μια ομάδα ερευνητών από 20 μεγάλες επιχειρήσεις, καθώς κέντρα ερευνών ένωσαν την ιδεολογική τους τροχιά για να δημιουργήσουν μια βάση του αρχιτεκτονικού σχεδιασμού του IOT ,με την Ευρωπαϊκή κομισιόν να αγκαλιάζει και να στηρίζει θερμά, αυτήν την νέα προσπάθεια, και με αυτόν τον τρόπο, το project **IOT -A** γεννιέται. Η ομάδα του IOT Architecture Project (**IOT -A**), δημιουργήθηκε με σκοπό να αναπτύξει την λογική της αρχιτεκτονικής του Internet of Things, απαρνιόντας επιχειρησιακές εκτιμήσεις για την εξέλιξη του IOT , και εστιάζοντας πραγματικά στην τεχνολογική εξέλιξη. Δημιούργησε ξανά από την βάση νέες λύσεις για την κλιμακωτή εξέλιξη του IOT , τόσο σε θέματα επικοινωνίας των έξυπνων συσκευών αλλά και την διαχείριση πολύπλοκων υπηρεσιών.

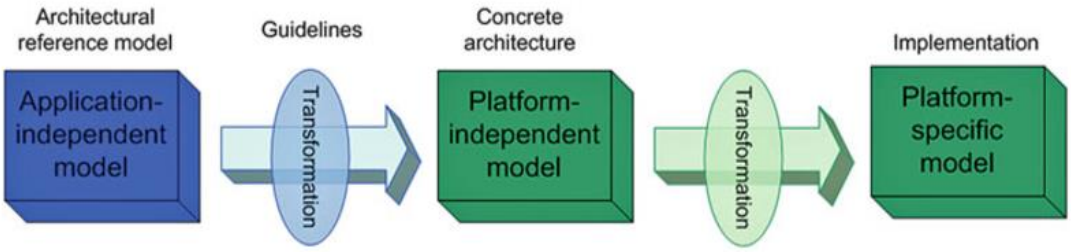
Ο ερευνητικός τομέας του IOT , αποτελείται από αρκετά διαφορετικά διακυβερνητικά μοντέλα, τα οποία συχνά δεν είναι συμβατά μεταξύ τους. Αυτό οδηγεί σε μια κατάσταση όπου η ασφάλεια και το απόρρητο των δεδομένων, αντιμετωπίζονται διαφορετικά και ανά περίπτωση λόγο νομοθετικών διαταγμάτων, την συνεχόμενη τροποποίηση των διαταγμάτων, των διαφορετικών εκδοχών αυτών - ανά τις Πολιτείες - με αποτέλεσμα να παρεμποδίζει σοβαρά την διαλειτουργικότητα και την ανάπτυξη μιας κοινής βάσης του IOT.
Βέβαια, η εξάπλωση του IOT είναι τόσο τεράστια, που θα ήταν αφελές να εξετάσουν την δημιουργία νέων πρωτοκόλλων τύπου, «Πρωτόκολλο που συνδυάζει όλα σε ένα» ή την δημιουργία μιας κοινής βάσης που να συνδυάζει την κάθε ξεχωριστή διαλειτουργικότητα των έξυπνων συσκευών ή των ίδιων νομοθετικών πλαισίων. Αυτό που έθεσε το IOT -A, είναι οι ταξινομήσεις ανάμεσα στα πρωτόκολλα και στα συστήματα επικοινωνίας, σύμφωνα με διαφορετικές αρχές όπως η κρισιμότητα στην μετάδοση, η λειτουργία του κατανεμημένου, η συγκέντρωση λειτουργίας σε ένα σημείο, και η αρχιτεκτονικής τους αναφορά.
Αυτές οι διαφοροποιήσεις ή οι λεγόμενες κλάσεις, μπορούν να προωθήσουν διαφορετικά τεχνολογικά προφίλ – λύσεων, ανάλογα τις ανάγκες και τις απαιτήσεις του προβλήματος. Η ομάδα του **IOT -A** αναφέρει επανειλημμένα ότι η ταυτοποίηση σε κατηγορίες, ενός **μοντέλου αναφοράς**, για ολοκληρωμένη λύση, θα παρέχει το κοινό έδαφος, και μιας αρχιτεκτονικής βάσης του IOT.

Δηλαδή, όταν αναφερόμαστε σε ένα μοντέλο αναφοράς εννοούμε ένα αφηρημένο πλαίσιο που αποτελείται από ένα σύνολο από ενωτικές έννοιες, αξιώματα και σχέσεις, για την κατανόηση των σημαντικών σχέσεων μεταξύ των οντοτήτων ενός περιβάλλον. Αυτό το μοντέλο αναφοράς θα επιτρέψει την ανάπτυξη συγκεκριμένων αρχιτεκτονικών που μπορεί να έχουν διαφορετικά επίπεδα από αόριστες έννοιές μεν, αλλά σημαντικές για να μπορέσουν να είναι ανεξάρτητες κάποιες προδιαγραφές από τις τεχνολογίες, specifications ή άλλες συγκεκριμένες λεπτομέρειες. Στο επίπεδο αυτό, των γκρίζων περιέχων του μοντέλου αναφοράς, επιτρέπει την υλοποίηση ενός πραγματικού συστήματος – framework- για τον εντοπισμό συγκεκριμένων **αρχιτεκτονικών αναφοράς**, που στην συνέχεια περιγράφουν κομμάτια αρχιτεκτονικής, καθώς και σχεδιαστικές επιλογές για την αντιμετώπιση των σύνθετων απαιτήσεων, όσο αφορά την λειτουργικότητα, την απόδοση, την ανάπτυξη και την ασφάλεια της αρχιτεκτονικής. Είναι πολύ σημαντικό οι διασυνδέσεις (interface) του πρωτοκόλλου με τον τρόπο υλοποίησης αρχιτεκτονικής να πρέπει να περάσουν από διαδικασία προτύπου (standard), για αν δοθούν βέλτιστες πρακτικές από την άποψη λειτουργικότητας και χρηστικότητας. Για αυτόν τον λόγο η ομάδα του IOT -A, κάθε κοινή τεχνική που χρησιμοποιεί για να καθιερώσει τα πρωτόκολλα επικοινωνίας, αρχιτεκτονικές, και άλλες τεχνολογικές λύσεις, αυτές οι τεχνικές προέρχονται από ένα **μοντέλο αναφοράς αρχιτεκτονικής (IOT Architectural Reference Model – ARM)**.

Αυτό έχει μεγάλο πλεονέκτημα στο να διασφαλίσει την λειτουργικότητα και σε προηγούμενε «εκδόσεις» των τεχνικών λύσεων, αλλά και να υιοθετήσει καθορισμένες λύσεις εργασίας για κάθε θέμα που αφορά το IOT.Καθώς η τακτική το να δημιουργείς ένα νέο standard στο εργαστήριο χωρίς να αντικρίζεις την ρεαλιστική εκδοχή του προβλήματος, είναι γνωστό την ομάδα του IOT A καθώς με την βοήθεια των τελικών χρηστών, νέων οργανωμένων ομάδων ενδιαφερόμενων, συγκεντρώνουν και εισάγουν νέες πληροφορίες και απαιτήσεις στον τρόπο που διεξάγονται οι αρχιτεκτονικές. Αυτές οι ομάδες είναι πολύ σημαντικές καθώς είναι σημαντικές πυγές για να λαμβάνει η ομάδα IOT A σχολιασμούς και προτάσεις για διαφορετική υλοποίηση των projects.Αυτοί οι σχολιασμοί είναι δομικά στοιχεία στον τρόπο επίλυσης και ανάπτυξης των projects με σκοπό να ικανοποιήσει μια συνολική και ολιστική προσέγγιση μιας ρεαλιστικής λύσης.

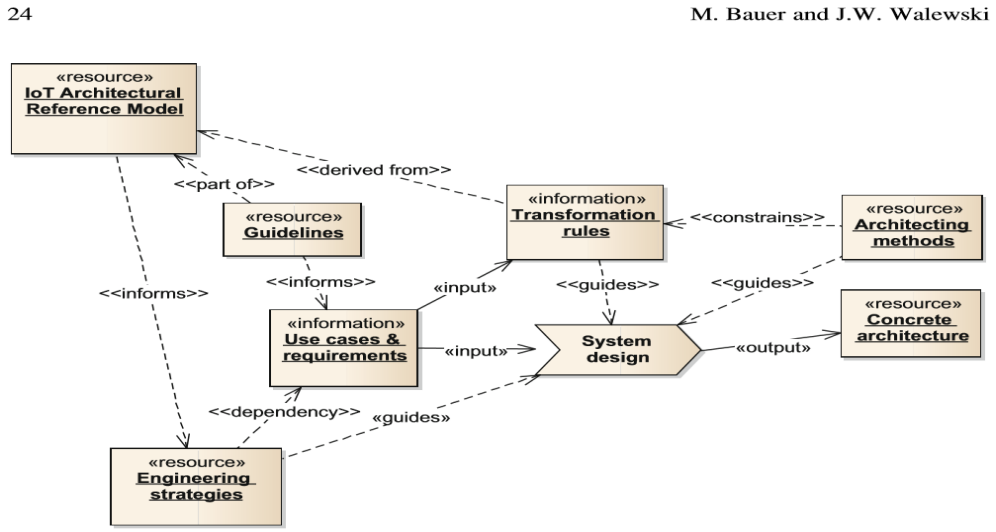
Με αυτόν τον τόπο η ομάδα IOT A κρατεί μια ανοιχτή προσέγγιση λύσεων καθώς αφουγκράζεται και την ιδεολογία του ανοιχτού Internet of Things, αφού οι πτυχές του απλώνονται σε πολλά φάσματα διαφορετικών κατηγοριών επιστημών όπως τον αυτοματισμό, την υγεία, τα οικονομικά, τις επιχειρήσεις. Σε πραγματικές περιπτώσεις οι ίδιες αρχές και το ίδιο γκρίζο επίπεδο που αναφερθήκαμε πιο πάνω απαιτείται καθώς στον κόσμο του IOT όλοι μπορούν να συμμετάσχουν και να εξελίξουν το ιδεολογικό κομμάτι. Ο στόχος όμως παραμένει ίδιος, στην real time παρακολούθηση των δεδομένων, των αντικειμένων και την ιχνηλασιμότητα του κάθε αντικειμένου, πρέπει να έχει μια ισορροπημένη έννοια αξίας στον κόσμο του IOT , για να απεχθή ένα ισορροπημένο κόστος. Η βασική ιδέα χρήσης του ARM από την ομάδα IOTA είναι ότι παρέχει μια κοινή δομή και τις κατευθυντήριες γραμμές για την αντιμετώπιση των βασικών πτυχών ανάπτυξης, χρησιμοποιώντας και αναλύοντας Internet of things enabled συστήματα.
Η ιδέα της δημιουργίας μια κοινής αρχιτεκτονικής για κάθε επιστημονικό πεδίο, είναι ιδιαίτερη και αρκετά δύσκολή καθώς πρέπει να καταγραφούν τα σχετικά πλεονεκτήματα για να μπορέσει να αποδώσει η τεχνική, και το σύστημα ARM βοηθάει στην παραγωγή αυτών των κοινών βάσεων, η οποίες έως ένα βαθμό δημιουργούνται με αυτόματο τρόπο.Η χρήση των μοντέλων όπως αυτού του ARM και μιας αρχιτεκτονικής, παρέχει μια περιγραφή που είναι πιο αφηρημένη από ότι είναι εγγενής στο πραγματικό σύστημα και στην εφαρμογή του η οποία παράγεται αυτόματα από το μοντέλο. Βέβαια αυτό είναι το κύριο πρόβλημα καθώς συγκεκριμένες αρχιτεκτονικές που έχουν σχεδιαστεί για μια συγκεκριμένη εφαρμογή με ιδιαίτερους περιορισμούς και επιλογές, ο ανασχεδιασμός αυτής, πρέπει να γίνει με χειροκίνητο τρόπο. Ακόμα και με χειροκίνητο τρόπο η χρηστικότητα της δημιουργίας μιας αρχιτεκτονικής ενός συστήματος βοηθούν τους μηχανικούς και τους σχεδιαστές συστημάτων για να δοκιμάσουν πραγματικά συστήματα, να ερευνήσουν τα μειονεκτήματα του και να τα λύσουν στην πορεία. Η δομή της αρχιτεκτονικής μπορεί να γίνει ρητή μέσα από μια αρχιτεκτονική περιγραφή και η εξαγωγή βασικών συστατικών των υφιστάμενων αρχιτεκτονικών, όπως μηχανισμοί ή η χρήση διάφορων προτύπων, καθιστά την αρχιτεκτονική σε αναφορική (reference architecture) η οποία είναι μια πιο γενικευμένη εικόνα του συστήματος. Αυτό μπορεί να διορθωθεί προσθέτοντας Guidelines προκειμένου

να προσδιορίσει τις συγκεκριμένες ιδιαιτερότητες επάνω σε αρχιτεκτονικές αναφοράς. Καθώς αυτός ο τρόπος είναι λειτουργικός, εφαρμόζεται και σε τεχνικές συστημάτων IOT και τα Guidelines έχουν την δυνατότητα να αναπτύξουν μια ανεξάρτητή εφαρμογή(ενός συστήματος) σε ένα ανεξάρτητο μοντέλο. Αυτό το είδος μεταμόρφωσης μπορείτε να το δείτε γραφικά στο παρακάτω σχήμα:



***5.1** Σχεδιάγραμμα Μεταμόρφωσης Ανεξάρτητης Εφαρμογής σε Ανεξάρτητο Μοντέλο*

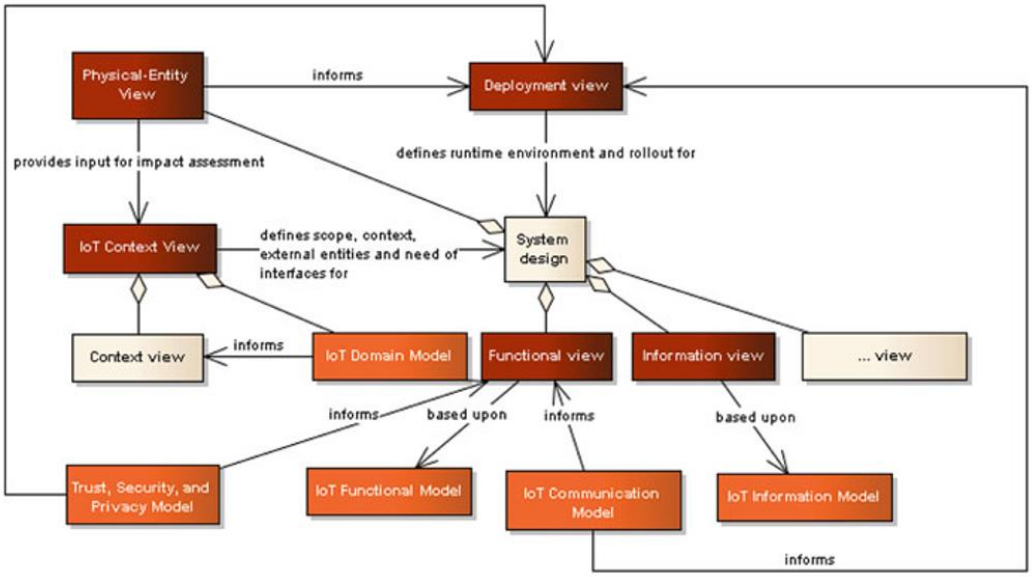
Είναι αρκετά σημαντικό να τονίσουμε ότι η χρηστικότητα του συστήματος ARM, παράγει διαφορετικού τύπου αρχιτεκτονικές για το IOT , για αυτό οι απαιτήσεις του κάθε προβλήματος, τα guidelines και τα use cases παίζουν σημαντικό ρόλο στην «μετάλλαξη» των αφηρημένων περιοχών (πιο πάνω αναφέρθηκαν και σαν γκρίζες περιοχές) του προβλήματος, σε μια σωστή και "στιβαρή " αρχιτεκτονική. Στην παρακάτω εικόνα βλέπετε την διαδικασία παραγωγής μια συγκεκριμένης αρχιτεκτονικής:



***5.2** Σχεδιάγραμμα Απεικόνισης Διαδικασίας για την Παραγωγή Συγκεκριμένων Αρχιτεκτονικών*

Η Συμβατότητα με άλλων ειδών αρχιτεκτονικές, είναι ένα μια χρονοβόρα διαδικασία, η οποία προέρχεται από την διαδικασία της δημιουργίας αρχιτεκτονικής που ακολουθεί μια διαδοχική προσέγγιση. Η προσέγγιση απαιτεί τον καθορισμό του πεδίου εφαρμογής, η

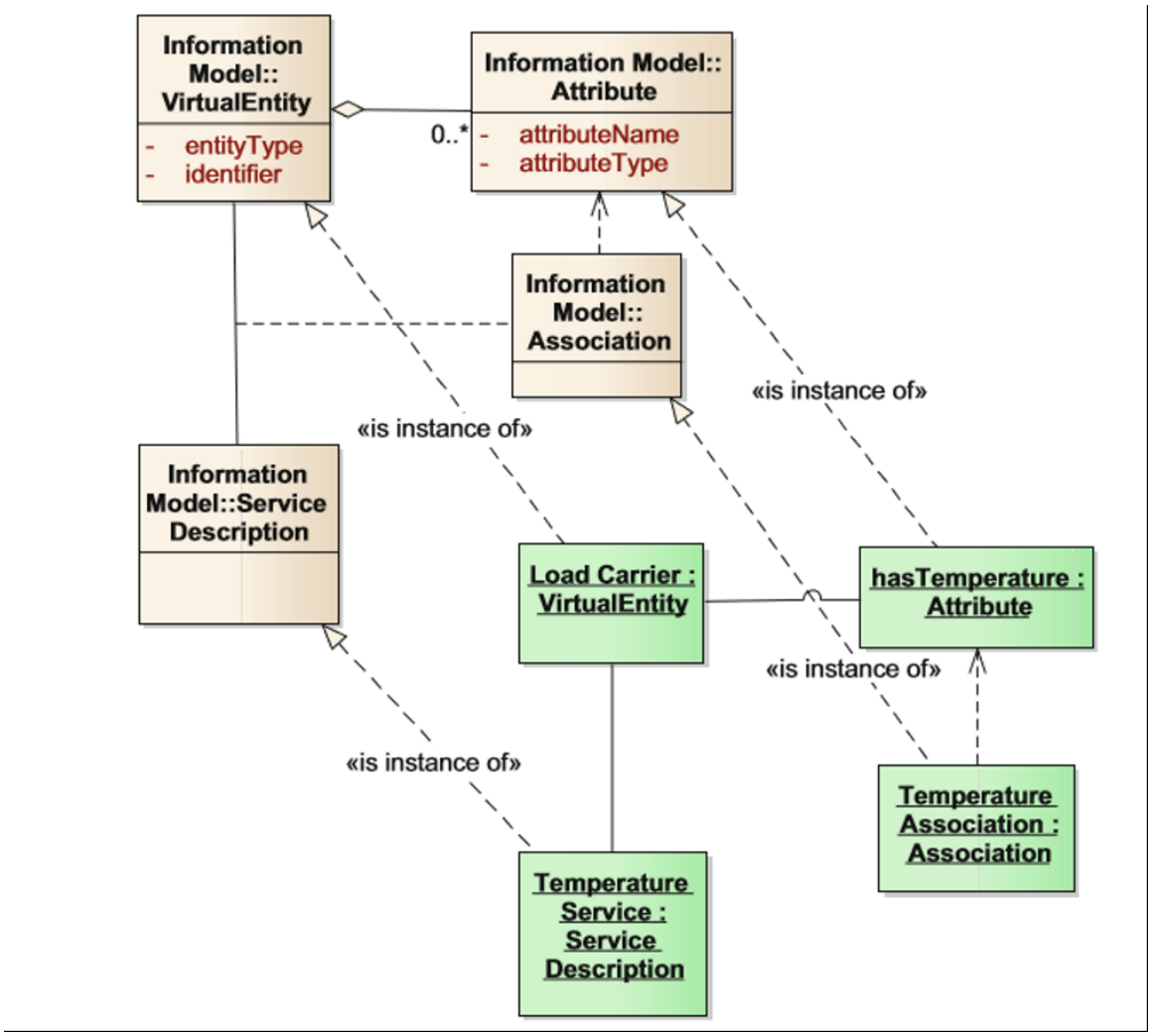
δημιουργία της Physical Entity όψης και Context όψης. Στην συνέχεια είναι ο καθορισμός των απαιτήσεων και η δημιουργία των επιπλέων όψεων (εκτός του Physical & Entity). Η αναφερόμενη διαδικασία δημιουργίας αρχιτεκτονική ονομάζεται και διαδικασία «Προσέγγισης του Καταρράκτη» (Royce 1970).



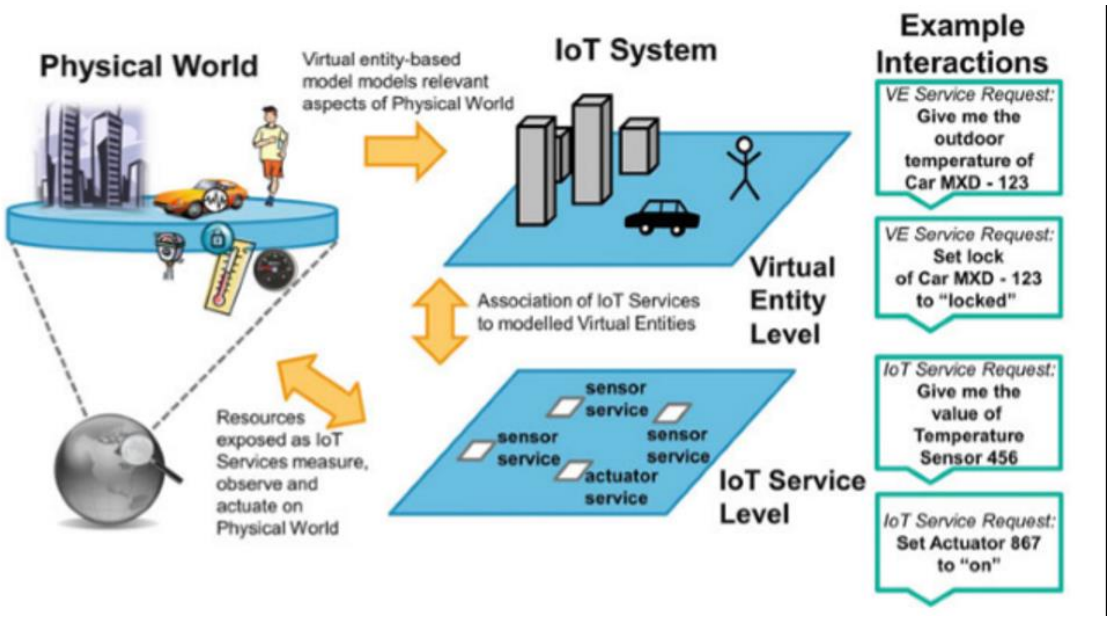
***5.3** Σχεδιάγραμμα σχέσεων αρχιτεκτονικών όψεων*

Η ομάδα του IOT-A εκτός από την δημιουργία περίπλοκων αρχιτεκτονικών των υποδομών του IOT, μελετά και τις **υπηρεσίες** του Internet of Things, προσπαθώντας να τις αναλύσει και να τις απλοποιήσει, οριοθετώντας αυτές σε σχεδιαγράμματα αρχιτεκτονικής. Η λογική των **υπηρεσιών** του IOT είναι όλες οι τεχνικές υπηρεσίες είναι οι μηχανισμοί, όπου οι ανάγκες και οι δυνατότητες ενώνονται σε ένα σύνολο μηχανισμών, οι οποίοι μηχανισμοί στον κόσμο των τεχνικών επιστημών είναι υλοποιημένοι σε μορφή κώδικα. Για αυτόν τον λόγο, οι **υπηρεσίες** παρέχουν έναν νοητό σύνδεσμο ανάμεσα στις πτυχές του IOT και μηχανισμών διάφορων συστημάτων που η αρχιτεκτονική τους δεν αποστάζετε την αρχιτεκτονική του Internet of Things. Καθώς η ομάδα του IOT-A έχει σκιαγραφήσει την αρχιτεκτονική του IOT, οι **υπηρεσίες** αποτελούν μέγιστης σημασίας, καθώς αποτελούν την διεπαφή ανάμεσα στο IOT και στην αλληλοεπίδραση του, με υλικά και φυσικά κομμάτια διασυνδέσεις όπως οι δίαυλοι επικοινωνίας ενός non- IOT σύστημα. Η χρηστικότητα των **υπηρεσιών** δίνει την λειτουργικότητα *αναζήτησης και εύρεσης πληροφοριών* ανάμεσα σε ποικίλα αρχιτεκτονικής συστημάτων. Πολλοί επιστήμονες θεωρούν ότι η λογική του Internet of Things, συγκαταλέγεται στην ιδέα των υπηρεσιών, που επιτρέπει την επικοινωνία του Φυσικού κόσμου, με αυτήν του ψηφιακού, όπως αναγράφηκε στο επιστημονικό τεύχος του Martin, έτους 2012. Η κατηγοριοποίηση των **υπηρεσιών** βάση των δεδομένων των επιστημών του IOT-A ανέρχεται σε 3 κατηγορίες, με κριτήριο το

επίπεδο της ενθυλάκωσης και της αφαιρετικότητας. Η πρώτη κατηγορία, είναι η *επιπέδου πόρων* που οι υπηρεσίες περιέχουν πληροφορίες σχετικά με την λειτουργικότητα των συσκευών του δικτύου είτε του τοπικού δικτύου είτε συσκευών σε κάποιο απομακρυσμένο δίκτυο, ανάλογα την ενθυλάκωση της υπηρεσίας. Η δεύτερη κατηγορία είναι το *εικονικό επίπεδο* καθώς οι υπηρεσίες αυτές, δίνουν την δυνατότητα προσπέλασης τρίτων υπηρεσιών, ακόμα και την αλλαγή των δεδομένων αυτών για να ενεργοποιήσουν αυτοματοποιημένες ενέργειες. Ένα παράδειγμα για να γίνει πιο κατανοητό το εικονικό επίπεδο είναι η διεπαφή NGSI version 2010.
Τέλος, το επίπεδο *ενσωματωμένης υπηρεσίας* είναι οι συνδυαστική μέθοδος των από πάνω κατηγοριών.



***5.4** Παράδειγμα Παραλλαγής Τρόπου Επικοινωνίας NGSI μέσω ενός Information Μοντέλου που Προσπελάζει Virtual Υπηρεσίες*



***5.5** Σχεδιάγραμμά Απεικόνισης της Συμπεριφοράς του Virtual Μοντέλου, μέσα στο Σύστημα IOT, που Αλληλοεπιδρά με Ιεραρχική Συμπεριφορά.*

Εν κατακλείδι το κεφάλαιο της Αρχιτεκτονικής Αναφοράς, σκιαγράφησε τις σημαντικές πτυχές της αρχιτεκτονικής του Internet Of Things, καθώς η επιστημονική κοινοπραξία του IOT-A θεωρείτε η πρώτη γραμμή του κύματος που ονομάζεται Internet Of Things. Οι πρώτες κινήσεις της ομάδας ήταν το 2009, που είχαν σαφώς αναγνωρίσει τις τεχνολογίες «κλειδιά» για την ανάπτυξη ενός παγκόσμιου IOT οράματος, καθώς οι υπηρεσίες, οι εφαρμογές και τα προϊόντα είναι οι «ρίζες» αυτού του οράματος. Σαν αποτέλεσμα η αρχιτεκτονική επιτρέπει αυτές τις «ρίζες» να μιλούν μεταξύ τους. Η επιστημονική κοινότητα, η κοινότητα των ερευνητών, και (στο κοντινό μέλλον) οι επιχειρήσεις, έχουν την δυνατότητα να εντάξουν την αρχιτεκτονική του IOT στα Projects και με τα σωστά εργαλεία να επωφεληθούν με την καινοτομία που προσφέρει το Internet of Things. Σε ό, τι αφορά την παραγωγή από πρωτοποριακών ιδεών σε πραγματικά προϊόντα και υπηρεσίες, σε πολλά επιστημονικά συνέδρια υπάρχει σαφής ανάγκη για την εκπαίδευση και την πληροφορία που λείπει αυτή τη στιγμή για να δημιουργηθούν αυτές οι υπηρεσίες και τα προϊόντα. Οι Επιχειρηματίες έχουν μια πολύ σαφή εικόνα για το τι θέλουν να επιτύχουν, αλλά δεν υπάρχει κανένας τρόπος για να κατανοήσουν την πολυπλοκότητα των προκλήσεων τους, για να επιλέξουν τα καλύτερα αρχιτεκτονικά πρότυπα σχεδιασμού που μπορεί να λύσει τα προβλήματα τους και να αποφασίσουν ποιες τεχνολογίες να χρησιμοποιήσουν στην πράξη. Από ένα όραμα για ένα προϊόν, ο σωστός σχεδιασμός σε όλο το σύνολο των μοντέλων, αρχιτεκτονικών και εργαλείων είναι μια αρκετά περίπλοκη διαδικασία. Η διαδικασία αυτή αντιμετωπίστηκε με την ανάπτυξη του αρχιτεκτονικού μοντέλου αναφοράς (ARM), το οποίο περιλαμβάνει όλα τα απαραίτητα πρότυπα και τα πρότυπα σχεδιασμού για την ανάπτυξη ενός πραγματικού προϊόντος. Είναι σημαντικό να κατανοηθεί από την ερευνητική κοινότητα, αλλά και το σύνολο της κοινότητας των φορέων καινοτομίας οι τεχνολογίες IOT μπορεί πραγματικά να χρησιμοποιηθούν για την υλοποίηση των έργων τους, δίνοντας, το πλεονέκτημα της καινοτομίας και την πιθανότητα

να διαπρέψουν στην αγορά. Είναι βέβαια γνωστό ότι κάποιες πτυχές της αρχιτεκτονικής χρειάζονται περαιτέρω εργασίες λόγο συνεχής αλλαγής της τεχνολογίας και το σύνολο των μοντέλων και αρχιτεκτονικών είναι αρκετά μεγάλο σε αριθμό, καθώς και κάποιες από αυτές είναι εξαιρετικά αόριστες. Αυτό που είναι σημαντικό είναι ότι η ARM και όλες οι σχετικές εξελίξεις δεν μπορούν να μονοπωλήσουν στην αποκλειστική κυριότητα μιας ενιαίας οργάνωσης, αλλά δίνει μεγάλη βοήθεια στο να χρησιμοποιηθεί το ARM, και μελλοντικά να τεθεί στο IOTA ως βάση. Μελλοντικά θα υπάρξει ανάγκη να αναπτυχθούν διαφορετικές διεπαφές, σε οποιοδήποτε επίπεδο, από το επίπεδο της συσκευής έως το επίπεδο υπηρεσιών, στην αρχιτεκτονική του ARM καθώς περισσότερες έρευνες και επαναστατικές εξελίξεις, όπως κβαντικές τεχνολογίες θα αναπτύσσονται σταδιακά. Η ομάδα IOT-A με το project αρχιτεκτονικής ARM δίνουν κατευθυντήριες γραμμές για τις εξελίξεις σε ορισμένα παιδία, όπως αυτά των πρωτοκόλλων.

Τέλος, πρέπει να αναπτυχθεί η θεματολογία της ασφάλειας εκτός επιστημονικής σφαίρας καθώς είναι απαραίτητη ενέργεια για την ανάπτυξη κοινωνικοπολιτικών μεθόδων ασφάλειας και ιδιωτικότητας. Ακόμη και πριν από το Internet of Things, καθώς και κάθε τεχνολογία για διασυνδεδεμένα αντικείμενα μπορεί να απορριφθεί με την αιτιολογία ότι παραβιάζει τις βασικές αρχές προστασίας της ιδιωτικής ζωής και ως εκ τούτου, θα πρέπει να γίνει εκτενέστατή εκπαίδευση για τα πλεονεκτήματα του Internet of Things για να διαπρέψει από αυτούς τους περιορισμούς.

6. Τεχνολογίες & Frameworks

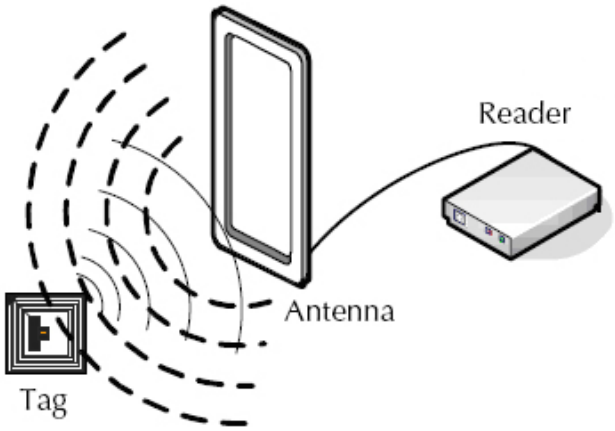
Η ανάπτυξη υπολογιστικών συστημάτων όπου τα ψηφιακά «πράγματα» μπορούν να αλληλοεπιδρούν με άλλα «πράγματα» για τη συλλογή δεδομένων οδήγησε στην ανάγκη για εύρεση και συνδυασμό νέων και αποτελεσματικών τεχνολογιών, οι οποίες έχουν την δυνατότητα να κάνουν τα πράγματα να εντοπίζονται και να επικοινωνούν μεταξύ τους.

Ως εκ τούτου, όλα καθοδηγούνται από τις νέες δυνατότητες ψηφιακής ανίχνευσης, τα ενσωματωμένα συστήματα πληροφορικής και επικοινωνιών που συνδέονται μέσω RFID (αναγνώρισης ραδιοσυχνοτήτων), ασύρματων δικτύων αισθητήρων (WSN), micro-chips, barcodes, QR (Quick Response) κωδικούς, Bluetooth, Wi-Fi, Beacons, Big Data, Analytics και Business Intelligence.

6.1 ΤΑΥΤΟΠΟΙΗΣΗ ΜΕΣΩ ΡΑΔΙΟΣΥΧΝΟΤΗΤΩΝ (RFID)

Το θεμέλιο του IoT είναι η τεχνολογία ανίχνευσης της συσκευής. Προς το παρόν η συλλογή πληροφοριών σε αυτό το σύστημα πραγματοποιείται από ηλεκτρονικές ετικέτες και αισθητήρες. Το Διαδίκτυο πραγμάτων χρησιμοποιεί ευρέος φάσματος τεχνολογίες που στέλνουν σήμα σε ένα ευρύ φάσμα συχνοτήτων όπως η RFID.

Η RFID είναι η πιο βασική τεχνολογία του IoT για την αναγνώριση, τον προσδιορισμό και τη σύνδεση των «πραγμάτων». Είναι ένα μικροτσίπ πομποδέκτης μαζί με ραδιοκύματα παρόμοιο με μία ετικέτα το οποίο θα μπορούσε να είναι τόσο ενεργητικό όσο και παθητικό, ανάλογα με τον τύπο της εφαρμογής. Οι ενεργητικές ετικέτες έχουν μια μπαταρία (παροχή ισχύος) και συνεχώς εκπέμπουν σήματα δεδομένων, ενώ οι παθητικές ετικέτες δεν έχουν τροφοδοσία και απορροφούν ενέργεια από το ηλεκτρομαγνητικό πεδίο που δημιουργεί η κεραία της συσκευής ανάγνωσης. Το RFID σύστημα, αποτελείται από ετικέτες/ αναμεταδότες, ένα πρόγραμμα ανάγνωσης και ένα υπολογιστικό σύστημα υποστήριξης (λογισμικό).



Ανάλογα με τον τύπο της εφαρμογής, οι συχνότητες RFID διαιρούνται σε τέσσερις διαφορετικές περιοχές συχνοτήτων :

I. χαμηλής συχνότητας (135 kHz ή λιγότερο)
II. υψηλής συχνότητας (13.56MHz)
III. Ultra-High Frequency (862MHz 928MHz)
IV. μικροκυμάτων συχνότητας (2.4G, 5,80)

6.2 ΑΣΎΡΜΑΤΕΣ ΤΕΧΝΟΛΟΓΊΕΣ

Σε αυτήν την ενότητα θα παρουσιαστούν οι τεχνολογίες δικτύου που μπορούν να βοηθήσουν στην μεγάλης κλίμακας ανάπτυξη του IoT. Εφόσον η κάθε συσκευή ενδέχεται να χρειάζεται να επικοινωνήσει με άλλες σε οποιαδήποτε απόσταση και με διαφορετικό μέσο επικοινωνίας, υπάρχουν συγκεκριμένες κατάλληλες τεχνολογίες αναλόγως των αποστάσεων:

- BAN (Body Area Network), μερικά μέτρα PAN (Personal Area Network), από 10 έως 100 m
- LAN (Local Area Network), μερικά km MAN (Metropolitan Area Network), 10 έως 100 km
- WAN (Wide Area Network), 1000 km GAN (Global Area Network).

***6.2.1** Τεχνολογίες επικοινωνίας ανάλογες τις απόστασης*

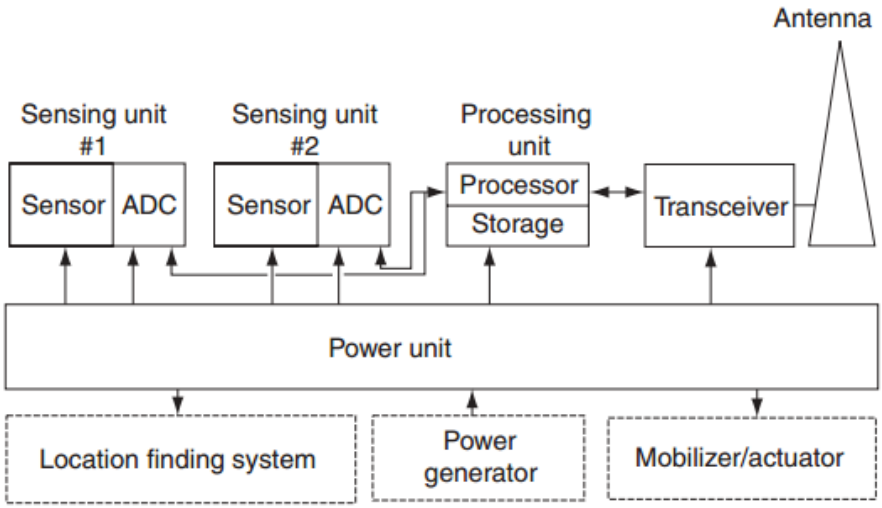
Οι ασύρματες τεχνολογίες (με τα πρωτόκολλα) για το IoT που θα αναπτυχθούν στην παρούσα εργασία είναι οι ακόλουθες: ZigBee (IEE 802.15.4), WiMax (IEE 802.16), WiFi (IEEE 802.11), Bluetooth (IEEE 820.15.1), UWB (IEE 802.15.3a), Flash OFDM κυψελωτά συστήματα (IEE 802.20).

- Το **ZigBee** είναι μια ασύρματη τεχνολογία που αναπτύχθηκε για να καλύψει τις ανάγκες για χαμηλό κόστος, χαμηλή ισχύς των ασύρματων δικτύων αισθητήρων. Συγκεκριμένα το ZigBee που χρησιμοποιούν οι μικροί, χαμηλής ισχύος ψηφιακοί δεκτές για την επικοινωνία τους βασίζεται στο 802.15.4 πρότυπο της IEEE για τα ασύρματα προσωπικά τοπικά δίκτυα (WPAN), όπως για παράδειγμα τα ασύρματα ακουστικά που συνδέονται με τα κινητά τηλέφωνα. Το ZigBee στοχεύει στις εφαρμογές ραδιοσυχνότητας (RF) που απαιτούν ένα χαμηλό ρυθμό μεταφοράς δεδομένων, μεγάλη ζωή μπαταριών, και εξασφαλισμένη δικτύωση.
- **WiMAX** αποκαλείται η τεχνολογία ασύρματης δικτύωσης η οποία λειτουργεί με παρεμφερή τρόπο με το Wi-Fi, ωστόσο με πολύ μεγαλύτερη εμβέλεια. Συγκεκριμένα, ενώ το Wi-Fi εξασφαλίζει εμβέλεια επικοινωνίας μέχρι 100 μέτρα, το WiMax φθάνει τα 35 χιλιόμετρα ή και παραπάνω.
- Η **UWB** τεχνολογία μπορεί γενικά να οριστεί σαν μια οποιαδήποτε ασύρματη μεταβίβαση που καταλαμβάνει ένα μήκος κύματος με συχνότητα 1,5 GHz. Είναι μια νέα μορφή της ασύρματης τεχνολογίας που βασίζεται σε μεταβίβαση χαμηλής ισχύος και κωδικοποιημένες ωθήσεις σε περιβάλλον μικρής απόστασης. Η UWB τεχνολογία χρησιμοποιείται σε εμπορικές και βιομηχανικές εφαρμογές για τον καθορισμό αποστάσεων ανάμεσα σε αντικείμενα, στην ανίχνευση αντικειμένων και καταστάσεων δια μέσου οικοδομών, σε συστήματα ασφαλείας και σε ιατρικά συστήματα.
- Η ανακάλυψη των **Flash OFDM** κυψελωτών ραδιοσυστημάτων βελτίωσε τις ασύρματες επικοινωνίες, αφού προσέφερε χρήση περισσότερων καναλιών, επικάλυψη ραδιοσυχνοτήτων, ενώ πομποί και δέκτες χρειαζόταν πλέον λιγότερη ισχύ για την λειτουργία τους, κάτι που σήμαινε μικρότερο κόστος, βάρος και μέγεθος, καθώς και λιγότερες παρεμβολές. Η κύρια ιδέα είναι ότι η γεωγραφική περιοχή που καλύπτει το σύστημα επικοινωνίας, χωρίζεται σε κυψέλες. Κάθε κυψέλη χρησιμοποιεί ένα σύνολο συχνοτήτων που μπορεί να χρησιμοποιούν και άλλες κοντινές κυψέλες αλλά όχι οι γειτονικές της.

Επιπλέον, με την ενσωμάτωση της τεχνολογίας **IPv6** στο IoT, μπορούμε να αντιληφθούμε την από άκρο σε άκρο επικοινωνία με τον τρέχοντα εξοπλισμό του δικτύου και τη βελτίωση της αναμετάδοσης και της αποτελεσματικότητας του, χαρακτηριστικά που αυξάνουν περαιτέρω την ασφάλεια της μετάδοσης πληροφοριών.

Δίκτυο ασύρματων αισθητήρων - Wireless Sensor Network (WSN)

Ιδιαίτερα σημαντική τεχνολογία του IoT αποτελεί το Δίκτυο ασύρματων αισθητήρων (Wireless Sensor Network (WSN)). Το WSN αποτελείται από ένα μεγάλο αριθμό μικροσκοπικών κόμβων αισθητήρων, με δυνατότητα ανίχνευσης των «πραγμάτων». Ο ρόλος των αισθητήρων είναι η παροχή ακατέργαστων πληροφοριών για επεξεργασία, μετάδοση, ανάλυση και ανατροφοδότηση πληροφοριών. Οι κόμβοι συλλέγουν και προωθούν τα δεδομένα στο σταθμό βάσης για την από κοινού παρακολούθηση των «πραγμάτων». Στα ασύρματα δίκτυα αισθητήρων υπάρχουν ένας ή περισσότεροι σταθμοί βάσης και αρκετοί κόμβοι αισθητήρων. Η βασική σύνθεση του κόμβου δικτύου αισθητήρων περιλαμβάνει τη μονάδα επεξεργασίας, τη μονάδα επικοινωνίας και τη μονάδα ενέργειας. Ο σταθμός βάσης χρησιμεύει ως επεξεργαστής δεδομένων που συνδέει το δίκτυο αισθητήρων με τον εξωτερικό κόσμο.



***6.2.2** Δίκτυο ασύρματων αισθητήρων (WSN)*
Πηγή: International Journal of Computer Applications (2015)
"A Review on Internet of Things (IoT)"

6.3 CLOUD COMPUTING

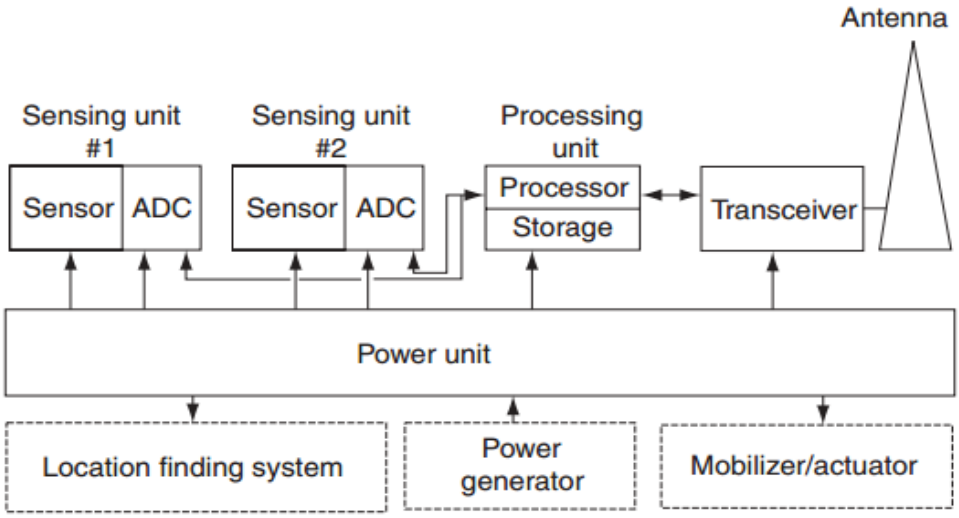
Πρόκειται για μια έξυπνη τεχνολογία υπολογιστών με την οποία μεγάλος αριθμός servers συγκλίνουν σε μία πλατφόρμα cloud, η οποία επιτρέπει την κατανομή των πόρων μεταξύ τους και την πρόσβαση στα πράγματα οποιαδήποτε στιγμή και από οποιοδήποτε μέρος. Το cloud computing είναι το πιο σημαντικό μέρος του IoT, το οποίο δεν συνδέει μόνο τους διακομιστές, αλλά αναλύει και τις χρήσιμες πληροφορίες που λαμβάνονται από τους αισθητήρες παρέχοντας υψηλή ικανότητα αποθήκευσης.

***6.3** Cloud Computing*
Πηγή: International Journal of Computer Applications (2015)
"A Review on Internet of Things (IoT)"

6.4 ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΚΤΥΟΥ

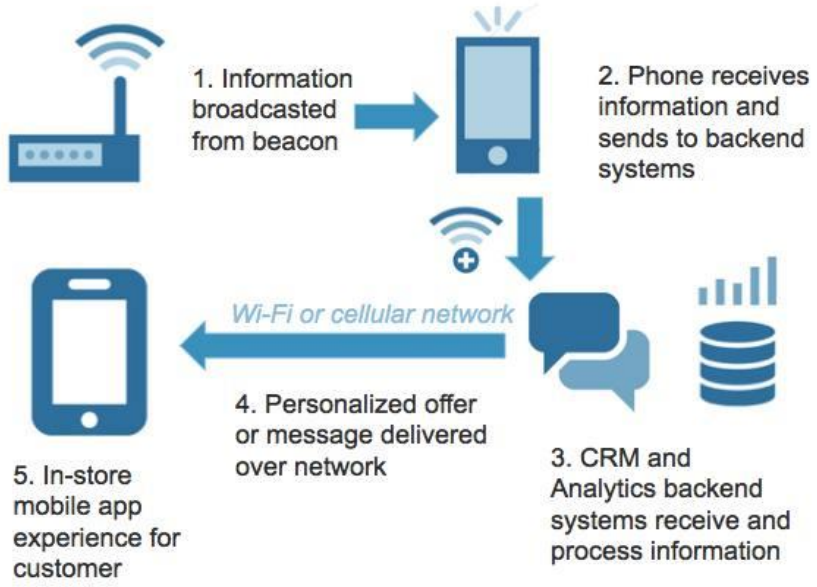
Οι τεχνολογίες αυτές έχουν διαδραματίσει σημαντικό ρόλο στην επιτυχία του IoT δεδομένου ότι είναι υπεύθυνες για την σύνδεση μεγάλου αριθμού πραγμάτων, προσφέροντας ένα γρήγορο και αποτελεσματικό δίκτυο. Για ευρύ φάσμα δίκτυο συνήθως χρησιμοποιούνται τα 3G, 4G κ.λπ. ενώ για ένα δίκτυο επικοινωνίας μικρής εμβέλειας χρησιμοποιούνται τεχνολογίες όπως Bluetooth, WiFi κ.α.

- ***Δίκτυο ασύρματων αισθητήρων - Wireless Sensor Network (WSN).*** Ιδιαίτερα σημαντική τεχνολογία του IoT αποτελεί το Δίκτυο ασύρματων αισθητήρων (Wireless Sensor Network (WSN)). Το WSN αποτελείται από ένα μεγάλο αριθμό μικροσκοπικών κόμβων αισθητήρων, με δυνατότητα ανίχνευσης των «πραγμάτων». Ο ρόλος των αισθητήρων είναι η παροχή ακατέργαστων πληροφοριών για επεξεργασία, μετάδοση, ανάλυση και ανατροφοδότηση πληροφοριών. Οι κόμβοι συλλέγουν και προωθούν τα δεδομένα στο σταθμό βάσης για την από κοινού παρακολούθηση των «πραγμάτων». Στα ασύρματα δίκτυα αισθητήρων υπάρχουν ένας ή περισσότεροι σταθμοί βάσης και αρκετοί κόμβοι αισθητήρων. Η βασική σύνθεση του κόμβου δικτύου αισθητήρων περιλαμβάνει τη μονάδα επεξεργασίας, τη μονάδα επικοινωνίας και τη μονάδα ενέργειας. Ο σταθμός βάσης χρησιμεύει ως επεξεργαστής δεδομένων που συνδέει το δίκτυο αισθητήρων με τον εξωτερικό κόσμο.



***6.4.1** Δίκτυο Ασύρματων Αισθητήρων (WSN)*
Πηγή: International Journal of Computer Applications (2015)
"A Review on Internet of Things (IoT)"

- ***Beacon.*** Εξίσου σημαντική είναι η **beacon technology**, η οποία αποτελείται από μικρές ασύρματες συσκευές/μικροπομποί που μεταδίδουν συνεχώς ένα απλό ραδιοφωνικό σήμα. Στις περισσότερες περιπτώσεις, το σήμα μπορεί να διαβαστεί από τα smartphones που χρησιμοποιούν τεχνολογία Bluetooth Low Energy (BLE). Όταν η κινητή συσκευή ανιχνεύει το σήμα Beacon, διαβάζει τον αριθμό αναγνώρισης του πομπού (ID), υπολογίζει την απόσταση από το πομπό και, με βάση αυτά τα δεδομένα, ενεργοποιεί την εφαρμογή του κινητού. Πρόκειται για μια Real-time επικοινωνία με τους χρήστες. Προσφέρει άμεση και σε πραγματικό χρόνο πρόσβαση στις παρεχόμενες υπηρεσίες οποιαδήποτε στιγμή.



***6.4.2** Beacon Tecnhology*
*Πηγή**: https://iot-analytics.com/rise-of-beacon-technology/***

- ***Επικοινωνία κοντινού πεδίου (NFC).*** Μία άλλη τεχνολογία το NFC (Near field communication) ή αλλιώς «επικοινωνία κοντινού πεδίου» που δημιουργήθηκε από τις εταιρείες Nokia, Philips και Sony και αποτελεί μια ασύρματη τεχνολογία διασυνδεσιμότητας η οποία επιτρέπει την ανταλλαγή πληροφοριών ανάμεσα σε συσκευές όπως smartphones και tablets. Η λειτουργία του NFC είναι αρκετά απλή: αρκεί να πλησιάσουν μεταξύ τους δύο συσκευές που υποστηρίζουν NFC για να αλληλεπιδράσουν και να ανταλλάξουν πληροφορίες σε αντίθεση με τις τεχνολογίες Bluetooth και WiFi στις οποίες προϋπόθεση για την επικοινωνία των συσκευών αποτελεί η εδραίωση της σύνδεσης (ενεργοποίηση-ανακάλυψη-σύζευξη).Η συχνότητα λειτουργίας της τεχνολογίας NFC είναι τα 13.56 MHz ενώ υποστηρίζει ταχύτητες μεταφοράς δεδομένων έως και 424 Kbps. Η απόσταση που μπορούν να αλληλεπιδράσουν δύο NFC συσκευές θεωρητικά είναι τα 20 εκατοστά. Το πλαίσιο λειτουργίας της NFC τεχνολογίας ορίζει δύο τρόπους λειτουργίας τον ενεργό, κατά τον οποίο και οι δύο συσκευές παράγουν ένα RF σήμα μέσω του οποίου πραγματοποιείται η μεταφορά των δεδομένων, και τον παθητικό, κατά τον οποίο μόνο η μία συσκευή παράγει RF σήμα ενώ η άλλη συσκευή λειτουργεί ως «στόχος» μεταφέροντας τα δεδομένα στην πρώτη χωρίς να τροφοδοτείται από εξωτερική πηγή ενέργειας. Ορισμένες εφαρμογές οι οποίες αξιοποιούν την τεχνολογία NFC είναι στη λιανική, όπου μια συσκευή NFC μπορεί να λειτουργεί ως scanner διαβάζοντας πληροφορίες από RFID ετικέτες, σε οποιουδήποτε είδους πληρωμές και ως επαγγελματική κάρτα, για την ανταλλαγή των στοιχείων των επαφών

(όνομα, διεύθυνση, τηλέφωνο, email, κτλ.). που είναι καταχωρημένα στις συσκευές μας.

- ***Narrow–Band IoT (NB–IoT)*** Αρχικά, για τη διασύνδεση συσκευών στο IoT χρησιμοποιήθηκαν τα δίκτυα κινητής τηλεφωνίας. Με τη περαιτέρω ανάπτυξη του "Internet of things", το πρόβλημα που εμφανίστηκε είναι ότι τα υπάρχοντα δίκτυα κινητής τηλεφωνίας δεν μπορούσαν να υποστηρίξουν την ταυτόχρονη σύνδεση στο διαδίκτυο χιλιάδων συσκευών που είναι στον ίδιο χώρο, ενώ η κατανάλωση ενέργειας είναι αρκετά μεγάλη. Γι' αυτό το λόγο επινοήθηκε η Narrow-Band IoT (NB-IoT). Πρόκειται για μία τεχνολογία σύνδεσης συσκευών μέσω δικτύων κινητής επικοινωνίας όπου η κατανάλωση ενέργειας κινείται σε πολύ χαμηλά επίπεδα, επιτρέποντας την ταυτόχρονη σύνδεση στο διαδίκτυο μεγάλου αριθμού συσκευών.

6.5 ΝΑΝΟΤΕΧΝΟΛΟΓΙΑ

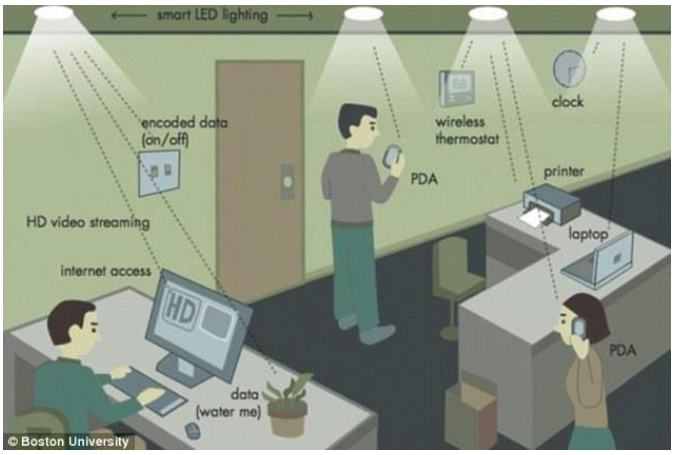
Αυτή η τεχνολογία πραγματεύεται μικρότερη και βελτιωμένη εκδοχή των πραγμάτων που βρίσκονται διασυνδεδεμένα. Μπορεί να μειώσει την κατανάλωση ενός συστήματος επιτρέποντας την ανάπτυξη των συσκευών στην κλίμακα του νανο – μέτρου. Οι συσκευές μπορούν να χρησιμοποιηθούν ως αισθητήρες ή ενεργοποιητές ακριβώς όπως και μία κανονική συσκευή.

6.6 ΤΕΧΝΟΛΟΓΙΕΣ ΜΙΚΡΟ-ΗΛΕΚΤΡΟ-ΜΗΧΑΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ (MEMS)

Οι MEMS είναι ένας συνδυασμός των ηλεκτρικών και μηχανικών εξαρτημάτων που χρησιμοποιούνται σε διάφορες εφαρμογές, συμπεριλαμβανομένων των αισθητήρων και ενεργοποιητών. Τα εξαρτήματα αυτά χρησιμοποιούνται ήδη στο εμπόριο σε πολλούς τομείς με τη μορφή των μετατροπέων και επιταχυνσιόμετρων. Ο συνδυασμός MEMS και νανοτεχνολογίας οδηγεί σε μια οικονομική και αποδοτική λύση για το σχεδιασμό του συστήματος επικοινωνίας του IoT. Η μείωση του μεγέθους των αισθητήρων και των ενεργοποιητών έχει ως αποτέλεσμα να υπάρχουν υπολογιστικές συσκευές παντού, υψηλότερο εύρος συχνοτήτων κ.α.

6.7 ΟΠΤΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

Οι ραγδαίες εξελίξεις στον τομέα των οπτικών τεχνολογιών, με τη μορφή τεχνολογιών όπως η Li-Fi και η BiDi της Cisco, θα μπορούσαν να είναι μια σημαντική ανακάλυψη στην ανάπτυξη του Ίντερνετ των Πραγμάτων.



Η Li-Fi (Light-Fidelity) τεχνολογία χρησιμοποιεί το ηλεκτρομαγνητικό φάσμα για τη μεταφορά δεδομένων. Αντί όμως για ραδιοσήματα, το Li-Fi μεταδίδει δεδομένα σε δυαδικό κώδικα χρησιμοποιώντας την τεχνολογία VLC (Visible Light Communication) που αξιοποιεί το φως από LED. Ομοίως, η Bi-Directional (BiDi) τεχνολογία δίνει ένα ethernet 40G για ένα μεγάλο εύρος συσκευών συνδεδεμένων στο δίκτυο IoT.

6.8 ΣΥΜΠΕΡΑΣΜΑ

Σύμφωνα με τα παραπάνω, μπορούμε να ορίσουμε το Διαδίκτυο των Πραγμάτων ως το δίκτυο που χρησιμοποιεί συσκευές ραδιοσυχνοτικής αναγνώρισης (RFID - radio frequency identification), υπέρυθρους αισθητήρες, συστήματα παγκόσμιου εντοπισμού θέσης, σαρωτές λέιζερ και άλλες αισθητήριες διατάξεις πληροφοριών, σύμφωνα με το συμφωνημένο πρωτόκολλο σε κάθε στοιχείο συνδεδεμένο στο Διαδίκτυο, για ανταλλαγή πληροφοριών και επικοινωνία, προκειμένου να επιτευχθούν έξυπνες λειτουργίες αναγνώρισης, εντοπισμού θέσης, παρακολούθησης και διαχείρισης.

7. Η Εξέλιξη του Internet Protocol

Το μέλλον του Internet of Things, δεν θα μπορέσει να πάρει μορφή και να αναπτυχθεί οικουμενικά, εάν δεν προηγηθεί ένα κύμα εξέλιξης του πρωτόκολλου του διαδικτύου, το Internet Protocol και η λοιπή σουίτα Πρωτοκόλλων διαδικτύου. Το Πρωτόκολλο Διαδικτύου ή Internet Protocol αποτελεί το κύριο πρωτόκολλο επικοινωνίας για την μετάδοση πακέτων δεδομένων, μέσα σε ένα διαδίκτυο οποιαδήποτε υποδομής αυτού, καθώς αναλαμβάνει την δρομολόγηση των πακέτων και καθορίζει τη μορφή των πακέτων που στέλνονται μέσω ενός διαδικτύου, καθώς και τους μηχανισμούς που χρησιμοποιούνται για την προώθηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό μέσω ενός ή περισσότερων δρομολογητών. Γι' αυτούς τους σκοπούς, το IP, χρησιμοποιεί συγκεκριμένες μεθόδους διευθυνσιοδότησης και δομές για την ενθυλάκωση των πακέτων δεδομένων. Το Πρωτόκολλο IP εισήχθη από τους Vint Cerf και Bob Kahn το 1974 και συνδέεται στενά με το Πρωτόκολλο Ελέγχου Μετάδοσης (TCP), με αποτέλεσμα ολόκληρη η σουίτα των πρωτοκόλλων του Διαδικτύου να αναφέρεται απλά ως σουίτα TCP/IP. Η πρώτη μεγάλης κλίμακας έκδοση του Πρωτοκόλλου IP, ήταν η έκδοση 4 (IPv4) η οποία επικρατεί μέχρι και σήμερα σε όλο το Διαδίκτυο. Ωστόσο, λόγω του ότι δεν επαρκούν πλέον οι διευθύνσεις, τα τελευταία χρόνια και για την μεγαλύτερη ανάγκη σε θέματα ταχύτητας και εύρος ζώνης(bandwidth) , έχει αναπτυχθεί η διάδοχη έκδοση του πρωτοκόλλου, η έκδοση 6 (IPv6), η οποία είναι εν ενεργεία και χρησιμοποιείται εξαπλωνόμενη σε όλο τον κόσμο. Το Πρωτόκολλο IP, είναι υπεύθυνο για τη διευθυνσιοδότηση των κόμβων και την δρομολόγηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό, κατά μήκος ενός ή περισσότερων δικτύων. Για το σκοπό αυτό, το πρωτόκολλο IP, καθορίζει ένα σύστημα διευθυνσιοδότησης, το οποίο έχει δύο λειτουργίες. Έτσι κάθε πακέτο IP, αποτελείται από μια κεφαλίδα και στη συνέχεια ακολουθούν τα δεδομένα. Στη κεφαλίδα αυτή εμπεριέχονται πληροφορίες: πρώτον, για τα δεδομένα που εμπεριέχονται στο πακέτο και δεύτερον, οι διευθύνσεις αφετηρίας και προορισμού. Η διαδικασία προσθήκης της κεφαλίδας σε ένα πακέτο δεδομένων ονομάζεται ενθυλάκωση. Το Πρωτόκολλο IP είναι μια υπηρεσία χωρίς σύνδεση, είναι ανεξάρτητο από την τεχνολογία του υλικού, που χρησιμοποιείται σε κάθε δίκτυο, και δεν χρειάζεται να την γνωρίζει πριν την μετάδοση.

7.1 ΑΞΙΟΠΙΣΤΙΑ

Εκτός από τον ορισμό της μορφής των αυτοδύναμων πακέτων, το Πρωτόκολλο IP ορίζει τη σημασιολογία της επικοινωνίας, και χρησιμοποιεί τον όρο βέλτιστη προσπάθεια, για να περιγράψει την υπηρεσία που παρέχει. Ουσιαστικά το πρότυπο αυτό ορίζει, ότι παρ' όλο που το πρωτόκολλο IP κάνει τη βέλτιστη δυνατή προσπάθεια για να αποδώσει ένα πακέτο στο προορισμό του, το υποκείμενο υλικό από το οποίο είναι φτιαγμένα τα εκάστοτε δίκτυα που διασχίζει, μπορεί να συμπεριφερθεί λανθασμένα. Έτσι, το πρωτόκολλο, δεν εγγυάται ότι θα μπορέσει να αντιμετωπίσει τα παρακάτω προβλήματα:

- Αλλοίωση δεδομένων
- Απώλεια αυτοδύναμου πακέτου
- Επανάληψη αυτοδύναμου πακέτου
- Επίδοση με καθυστέρηση ή εκτός σειράς.

Για την αντιμετώπιση του κάθε ενός από αυτά τα σφάλματα, χρειάζονται πρόσθετα, υψηλότερα επίπεδα λογισμικού πρωτοκόλλων. Η μόνη διαβεβαίωση που μπορεί να δώσει το πρωτόκολλο IP στην έκδοση 4 (IPv4), είναι το αν τα μπιτ της κεφαλίδας έχουν υποστεί αλλοίωση ή όχι κατά τη διάρκεια της μεταφοράς. Αυτή η πληροφορία εμπεριέχεται σε ένα πεδίο της κεφαλίδας του IP πακέτου, που ονομάζεται Άθροισμα Ελέγχου Κεφαλίδας (Header Checksum). Κάνοντας χρήση του checksum, μπορεί να διαπιστωθεί εάν η κεφαλίδα έχει μεταφερθεί σωστά ή όχι, και αναλόγως το πακέτο απορρίπτεται ή όχι. Στην έκδοση 6 (IPv6) ωστόσο, έχει εγκαταλειφθεί η χρήση του αθροίσματος ελέγχου κεφαλίδας, προς όφελος της ταχείας προώθησης μέσω ορισμένων στοιχείων δρομολόγησης στο δίκτυο.

7.2 ΜΟΡΦΗ ΠΑΚΕΤΟΥ ΣΤΟ IPV4

- **Επικεφαλίδα.**
  Η επικεφαλίδα στο IPv4 αποτελείται από δεκατέσσερα πεδία, από τα οποία τα δεκατρία είναι απαραίτητα. Το δέκατο τέταρτο πεδίο είναι προαιρετικό και ονομάζεται «Επιλογές». Τα πεδία στην επικεφαλίδα ορίζονται με το περισσότερο σημαντικό πεδίο και για το διάγραμμα και το τμήμα «συζήτηση», τα περισσότερο σημαντικά bit βρίσκονται μπροστά. Έτσι το ο είναι το "περισσότερο σημαντικό bit" MSB).

- **Έκδοση & Μήκος Επικεφαλίδας.**
  Το πρώτο πεδίο της επικεφαλίδας σε ένα IP πακέτο είναι το πεδίο της έκδοσης του πρωτοκόλλου, μήκους 4-bit. Για το IPv4 αυτό έχει την τιμή 4 (απ' όπου και

προέρχεται το όνομα IPv4). Το δεύτερο πεδίο (4-bits) είναι το μήκος της επικεφαλίδας (IHL, Internet Header Length). Αυτό μας δίνει το μήκος της επικεφαλίδας σε λέξεις των 32 bit. Επειδή η επικεφαλίδα του IPv4 μπορεί να περιέχει μεταβλητό αριθμό επιλογών, αυτό το πεδίο παρέχει το μήκος της επικεφαλίδας. Η μικρότερη τιμή του πεδίου είναι 5.

- **Συνολικό Μήκος & Αναγνώριση.**
  Το πεδίο «Συνολικό μήκος» έχει μήκος 16-bits και καθορίζει το συνολικό μήκος του κομματιού (fragment) σε bytes, συμπεριλαμβανομένων επικεφαλίδας και των δεδομένων. Το ελάχιστο μήκος του πακέτου είναι 20 bytes και το μέγιστο μήκος είναι 2^{16}-1=65535 bytes, καθότι το μήκος του πεδίου Συνολικό Μήκος είναι 16 bits. Διάφορες συσκευές και μερικές φορές τα υποδίκτυα μπορεί να επιβάλλουν περιορισμούς στο μέγεθος των αυτοδύναμων πακέτων, τα οποία σ' αυτήν την περίπτωση πρέπει να σπάσουν σε μικρότερα κομμάτια. Στο IPv4 η διάσπαση μπορεί να γίνει στους σταθμούς εργασίας ή στους δρομολογητές.
  Το πεδίο αναγνώριση είναι το πεδίο ταυτότητας και χρησιμεύει για τον μοναδικό προσδιορισμό των κομματιών (fragments) που ανήκουν στο ίδιο αρχικό IP αυτοδύναμο πακέτο.

- **Σημαίες.**
  Αυτό είναι ένα πεδίο των τριών bit και χρησιμεύει να ελέγχει ή να προσδιορίζει τα κομμάτια. Αυτά είναι (κατά σειρά από το περισσότερο σημαντικό προς το λιγότερο):

  bit 0: Δεσμευμένο, πρέπει να είναι 0

  bit 1: Απαγόρευσης διάσπασης του αυτοδύναμου πακέτου (DF=Don't Fragment)

  bit 2:Ένδειξης ύπαρξης περισσότερων κομματιών (MF=More Fragments)

  Εάν η σημαία DF έχει τεθεί στο 1 και για την δρομολόγηση του πακέτου είναι απαραίτητη η διάσπασή του, τότε το πακέτο απορρίπτεται. Αυτό θα μπορούσε να χρησιμοποιηθεί κατά την αποστολή πακέτων σε σταθμούς εργασίας, οι οποίοι δεν έχουν επαρκείς πόρους για τον χειρισμό της διάσπασης. Επίσης μπορεί να χρησιμοποιηθεί για την αυτόματη ανίχνευση της Μέγιστης Μονάδας Μεταφοράς κατά Μήκος της Διαδρομής (Path MTU Discovery) είτε αυτόματα από το software των σταθμών εργασίας, είτε χειροκίνητα με την χρήση διαγνωστικών εργαλείων, όπως τα ping και traceroute. Σε πακέτα που δεν έχουν διασπαστεί η σημαία MF είναι 0. Για διασπασμένα πακέτα όλα τα κομμάτια έχουν το MF=1, εκτός από το τελευταίο πού έχει το MF=0. Το τελευταίο κομμάτι έχει μη μηδενικό πεδίο Δείκτη εντοπισμού τμήματος, το οποίο το διακρίνει από ακομμάτιαστα πακέτα.

- **Δείκτης εντοπισμού τμήματος.**
  Ο δείκτης εντοπισμού τμήματος είναι 13-bit και απαριθμεί σε οκτάδες Byte. Προσδιορίζει την θέση ενός συγκεκριμένου κομματιού, από την αρχή του αρχικού ακομμάτιαστου αυτοδύναμου πακέτου. Το πρώτο κομμάτι έχει δείκτη εντοπισμού τμήματος 0. Αυτό επιτρέπει έναν μέγιστο αριθμό θέσεων (213 − 1) × 8 = 65,528 bytes, το οποίο και ξεπερνά το μέγιστο μήκος του IP πακέτου, που είναι 65535 bytes, εάν συμπεριλάβουμε και το μήκος της επικεφαλίδας (65,528 + 20 = 65,548 bytes).

- **Χρόνος Ζωής.**
  Το πεδίο αυτό οριοθετεί το χρόνο ζωής του αυτοδύναμου πακέτου. Έχει μήκος 8 bit και χρησιμεύει στο να καταστρέφονται αυτοδύναμα πακέτα που για διάφορους λόγους περιφέρονται άσκοπα στο Internet. Δίνεται σε δευτερόλεπτα, αλλά χρόνοι μικρότεροι από 1s στρογγυλεύονται στο 1 s. Στην πράξη έχει οριστεί σαν μετρητής αναπηδήσεων: Όταν ένα αυτοδύναμο πακέτο φτάσει σε έναν δρομολογητή, ο δρομολογητής μειώνει το πεδίο "χρόνου ζωής" κατά 1. Όταν μηδενιστεί, ο δρομολογητής απορρίπτει το πακέτο και στέλνει ένα μήνυμα τέλους χρόνου του πρωτοκόλλου μηνυμάτων ελέγχου του Internet(ICMP Time Exceeded) μήνυμα στον αποστολέα. Το πρόγραμμα traceroute χρησιμοποιεί το μήνυμα τέλους χρόνου του ICMP. για να εκτυπώσει τους δρομολογητές που χρησιμοποιούνται από τα πακέτα στη διαδρομή τους από την πηγή στον προορισμό.

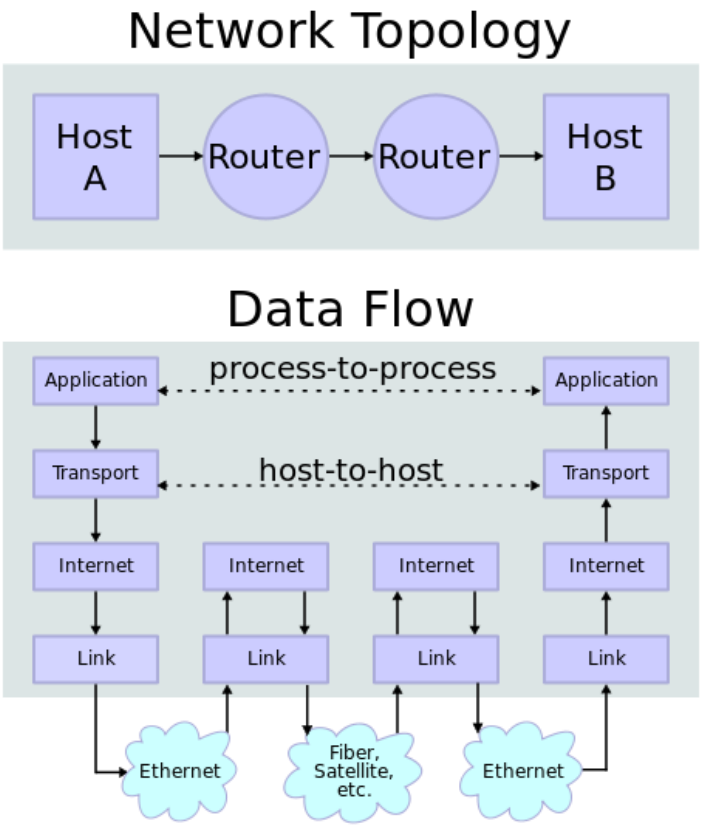
- **Άθροισμα Ελέγχου Επικεφαλίδας.**
  Το 16-bits άθροισμα ελέγχου της επικεφαλίδας, χρησιμοποιείται για έλεγχο σφαλμάτων της επικεφαλίδας. Μόλις ένα πακέτο φτάσει σε έναν δρομολογητή, ο δρομολογητής υπολογίζει το άθροισμα ελέγχου της επικεφαλίδας και το συγκρίνει με το πεδίο αθροίσματος ελέγχου της επικεφαλίδας. Εάν δεν ταιριάζουν, τότε ο δρομολογητής απορρίπτει το πακέτο. Σφάλματα στο πεδίο δεδομένων πρέπει να διαχειριστούν από το ενθυλακωμένο πρωτόκολλο. Και το UDP και το TCP έχουν πεδία αθροισμάτων ελέγχου. Όταν ένα πακέτο φτάσει σε έναν δρομολογητή, ο δρομολογητής μειώνει το πεδίο χρόνου ζωής (TTL). Συνεπώς ο δρομολογητής πρέπει να υπολογίσει το νέο άθροισμα ελέγχου.

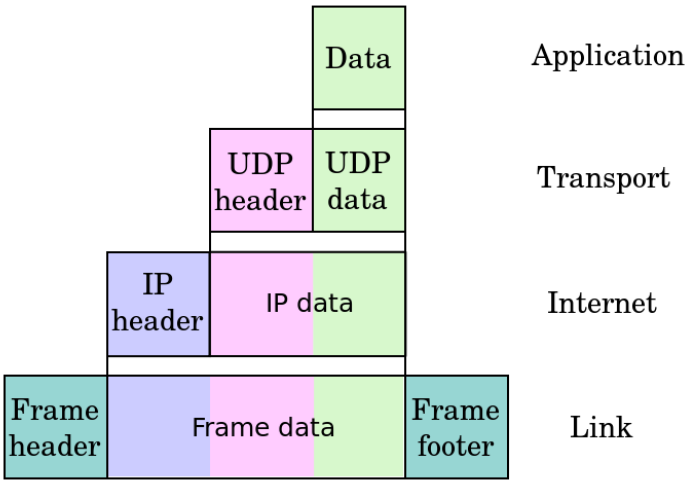
- **Διεύθυνση Πηγής & Προορισμού.**
  Το πεδίο διεύθυνση πηγής αναγράφει την διεύθυνση IP του αποστολέα του πακέτου και μπορεί να τροποποιηθεί μόνο από NAT servers, ισχύει το ίδιο και για το πεδίο διεύθυνσης προορισμού.

- **Διάσπαση και επανασύνδεση.**
  Το IP καθιστά δυνατό το να επικοινωνεί το ένα δίκτυο με το άλλο. Ο σχεδιασμός προβλέπει την συνύπαρξη δικτύων διαφόρων τύπων. Το πρωτόκολλο είναι ανεξάρτητο από την φύση της υποκείμενης τεχνολογίας μετάδοσης του επιπέδου σύνδεσης. Τα δίκτυα με διαφορετικό υλικό συνήθως διαφέρουν όχι μόνο στην μέγιστη ταχύτητα μετάδοσης, αλλά επίσης και στη μέγιστη μονάδα μετάδοσης (MTU). Όταν ένα δίκτυο θέλει να στείλει αυτοδύναμα πακέτα σε δίκτυα με μικρότερο MTU, μπορεί να διασπάσει το αυτοδύναμο πακέτο. Στο IPv4 αυτή η λειτουργία είναι τοποθετημένη στο επίπεδο internet και εκτελείται στο IPv4 από τους δρομολογητές. Αντίθετα το IPv6, η επόμενη γενιά του πρωτοκόλλου Internet, δεν επιτρέπει στους δρομολογητές να κάνουν διάσπαση. Οι σταθμοί εργασίας πρέπει να προσδιορίσουν το MTU της διαδρομής, προτού αποστείλουν τα αυτοδύναμα πακέτα.

- **Δεδομένα.**
  Το τμήμα δεδομένων του πακέτου, δεν συμπεριλαμβάνεται στο Άθροισμα Ελέγχου, το οποίο και γι' αυτό αποκαλείται Άθροισμα Ελέγχου Επικεφαλίδας. Ο τρόπος αναπαράστασης των περιεχομένων του βασίζεται στην τιμή που υπάρχει στο πεδίο «Αριθμός Πρωτοκόλλου» της επικεφαλίδας.

7.3 ΣΧΕΔΙΑΓΡΑΜΑ IPV4





7.4 INTEPNET PROTOCOL VERSION 6

Το IPv6 είναι η πιο πρόσφατη αναθεώρηση του πρωτοκόλλου Internet (IP), του βασικού πρωτοκόλλου επικοινωνίας πάνω στο οποίο έχει χτιστεί ολόκληρο το διαδίκτυο. Πρόκειται να αντικαταστήσει το παλιότερο IPv4, το οποίο χρησιμοποιείται μέχρι σήμερα. Το IPv6 αναπτύχθηκε από την Τακτική Δύναμη Μηχανικών του Internet (Internet Engineering Task Force, IETF), για να ασχοληθεί με το επί μακρόν αντιμετωπιζόμενο πρόβλημα της εξάντλησης των διευθύνσεων του IPv4 και της ταχύτητας και εύρος ζώνης(bandwidth). Με το IP protocol 6 ο αριθμός των διευθύνσεων φτάνει έως 340 εντεκάκις(undercillion) διαφορετικές διευθύνσεις IP (Ivy Wigmore, 2009).

Τον Σεπτέμβριο του 1993 η IETF δημιούργησε μία προσωρινή περιοχή IP επόμενης γενεάς, για να ασχοληθεί ειδικά με το θέμα αυτό. Η νέα περιοχή καθοδηγούταν από τους Allison Mankin και Scott Bradner και είχε ένα διευθυντήριο από 15 μηχανικούς με ποικίλα υπόβαθρα, για καθορισμό κατευθύνσεων και προκαταρκτική εξέταση των εγγράφων με τις προτάσεις. Τα μέλη της ομάδας εργασίας ήταν οι J. Allard (Microsoft), Steve Bellovin (AT&T), Jim Bound (Digital Equipment Corporation), Ross Callon (Wellfleet), Brian Carpenter (CERN), Dave Clark (MIT), John Curran (NEARNET), Steve Deering (Xerox), Dino Farinacci (Cisco), Paul Francis (NTT), Eric Fleischmann (Boeing), Mark Knopper (Ameritech), Greg Minshall (Novell), Rob Ullmann (Lotus), and Lixia Zhang (Xerox). Η IETF υιοθέτησε το μοντέλο των IP διευθύνσεων στις 25 Ιουλίου του 1994, με τον σχηματισμό διαφόρων ομάδων εργασίας. Το 1996 εκδόθηκε μία σειρά RFCs που καθόριζε την έκδοση 6 (IPv6) του πρωτοκόλλου Internet, ξεκινώντας με την RFC 1983.(Η έκδοση 5, χρησιμοποιήθηκε από το πειραματικό Internet Stream Protocol). Αναμένεται τα IPv4 και IPv6 θα χρησιμοποιηθούν παράλληλα στο προσεχές μέλλον. Οι κόμβοι IPv4 και IPv6 δεν μπορούν να επικοινωνήσουν απ' ευθείας, αλλά χρειάζονται την βοήθεια ενδιαμέσων πυλών ή πρέπει να χρησιμοποιήσουν άλλους μηχανισμούς μετάβασης.

Σε σύγκριση με το IPv4, το protocol 6 καθορίζει μία νέα μορφή πακέτου, σχεδιασμένη για να ελαχιστοποιεί την επεξεργασία των πακέτων από τους δρομολογητές. Επειδή οι επικεφαλίδες των πακέτων του IPv4 και IPv6 διαφέρουν σημαντικά, τα δύο πρωτόκολλα δεν μπορούν να συνεργαστούν. Όμως από τις περισσότερες πλευρές το IPv6 είναι μία συντηρητική επέκταση του IPv4. Τα περισσότερα πρωτόκολλα του επιπέδου μεταφοράς και εφαρμογής, χρειάζονται λίγη ή και καθόλου μετατροπή για να δουλέψουν πάνω στο IPv6. Εξαίρεση αποτελούν τα πρωτόκολλα εφαρμογών, τα οποία ενσωματώνουν διευθύνσεις του επιπέδου internet, όπως το FTP και το NTPv3, όπου η νέα μορφή των διευθύνσεων μπορεί να προκαλεί συγκρούσεις με την σύνταξη υπαρχόντων πρωτοκόλλων. Στο IPv6, έχει απλοποιηθεί η επικεφαλίδα και η προώθηση του πακέτου. Παρόλο που η επικεφαλίδα των πακέτων IPv6 είναι τουλάχιστον διπλάσια από την επικεφαλίδα των πακέτων IPv4, η επεξεργασία των πακέτων είναι αποδοτικότερη, επειδή χρειάζονται λιγότερη επεξεργασία από τους δρομολογητές. Αυτό προάγει την σχεδιαστική Αρχή απ΄ Άκρου σ΄ Άκρο (end-to-end principle) του Internet, η οποία προβλέπει ότι η περισσότερη

επεξεργασία πρέπει να πραγματοποιείται στους ακραίους κόμβους. Η επικεφαλίδα του πακέτου IPv6, είναι απλούστερη από την επικεφαλίδα του πακέτου IPv4. Πολλά πεδία τα οποία χρησιμοποιούνται σπάνια, έχουν μετακινηθεί στις προαιρετικές επεκτάσεις της επικεφαλίδας. Οι δρομολογητές IPv6, δεν κάνουν διάσπαση των πακέτων IP. Οι συσκευές IPv6, είναι υποχρεωμένες είτε να ανακαλύψουν την Μέγιστη Μονάδα Μεταφοράς της Διαδρομής (path MTU discovery), ή να μην στείλουν πακέτα μεγαλύτερα από την προεπιλεγμένη Μέγιστη Μονάδα Μεταφοράς (Maximum transmission unit, MTU), η οποία είναι 1280 οκτάδες. Επιπλέων ένα χαρακτηριστικό αρκετά σημαντικό είναι ότι το v6 αποφεύγει την τριγωνική δρομολόγηση (triangular routing) και για αυτό είναι το ίδιο αποτελεσματικό με το σταθερό IPv6. Οι δρομολογητές του IPv6, επιτρέπουν να μετακινηθούν ολόκληρα υποδίκτυα σε άλλους δρομολογητές, χωρίς επαναρίθμηση. Ένας κόμβος IPv6, μπορεί προαιρετικά να επεξεργαστεί πακέτα πάνω από όριο του ipv4 στα (216–1) οκτάδες. Τα πακέτα αυτά αναφέρονται σαν Jumbograms και μπορούν να έχουν μέγεθος μέχρι (232–1) οκτάδες. Η χρήση των Jumbograms μπορεί να βελτιώσει την απόδοση πάνω σε συνδέσεις υψηλού MTU.

Μέχρις ότου το IPv6 εκτοπίσει πλήρως το IPv4, είναι απαραίτητος ένας αριθμός μεταβατικών μηχανισμών, που θα επιτρέψει σε συσκευές που χρησιμοποιούν μόνο το IPv6, να έχουν πρόσβαση σε υπηρεσίες του IPv4, και να επιτρέψουν σε απ΄ άκρου σε άκρον συσκευές που χρησιμοποιούν το IPv6, να μπορούν να επικοινωνούν μέσα από ένα δίκτυο που υποστηρίζει μόνο IPv4. Πολλοί από αυτούς τους μεταβατικούς μηχανισμούς χρησιμοποιούν την τεχνική tunneling, με την οποία ενθυλακώνουν κυκλοφορία του IPv6 σε δίκτυα IPv4. Αυτή είναι μία ατελής λύση η οποία μπορεί να δημιουργήσει προβλήματα. Τα πρωτόκολλα tunneling είναι μία προσωρινή λύση για δίκτυα τα οποία δεν υποστηρίζουν διπλή στοίβα (dual-stack), όπου και τα δύο πρωτόκολλα τρέχουν ανεξάρτητα το ένα από το άλλο, δηλαδή και τα δύο πρωτόκολλα τρέχουν στο ίδιο δίκτυο και δεν είναι απαραίτητη η ενθυλάκωση του IPv6 στο IPv4 και αντιστρόφως. Η διπλή στοίβα καθορίζεται στο RFC 4213 και το πρωτόκολλο IP 41, δηλώνει πακέτα IPv4 τα οποία ενθυλακώνουν αυτοδύναμα πακέτα (datagrams) IPv6. Μερικοί δρομολογητές ή συσκευές μετατροπής διευθύνσεων δικτύου (NAT) μπορεί να μπλοκάρουν το πρωτόκολλο 41. Για να διέλθει διαμέσου τέτοιων συσκευών, μπορεί να χρησιμοποιηθούν πακέτα UDP για την ενθυλάκωση αυτοδύναμων πακέτων IPv6. Δημοφιλείς είναι επίσης και άλλες μορφές ενθυλάκωσης, όπως οι AYIYA και η Generic Routing Encapsulation.

Παρότι αυτή είναι η πλέον πρόσφορη πραγματοποίηση του IPv6, καθότι παρακάμπτει πολλά μειονεκτήματα της τεχνικής tunneling, δεν είναι πάντοτε εφικτή, επειδή πεπαλαιωμένος δικτυακός εξοπλισμός δεν μπορεί να υποστηρίξει το IPv6. Έτσι π.χ. δρομολογητές συνδρομητών μπορεί να χρειάζονται είτε ενημέρωση του software είτε ακόμη και αλλαγή του hardware. Αυτό σημαίνει ότι διαχειριστές δικτύων πρέπει να καταφεύγουν στην τεχνική του tunneling, μέχρις ότου η ραχοκοκαλιά των δικτύων υποστηρίξει τη διπλή στοίβα.

7.5 SLAAC

Οι συσκευές που συνδέονται σε ένα δίκτυο IPv6 μπορούν να αποδώσουν αυτόματα στον εαυτό τους μία IPv6 διεύθυνση, χρησιμοποιώντας το πρωτόκολλο Neighbor Discovery Protocol (Πρωτόκολλο Ανακάλυψης Γειτόνων). Αυτό το πετυχαίνουν χρησιμοποιώντας Μηνύματα Ανακάλυψης Δρομολογητών του Πρωτοκόλλου Μηνυμάτων Ελέγχου του Internet, έκδοση 6 (Internet Control Message Protocol version 6 (ICMPv6)). Με τα πακέτα αυτά οι συσκευές ζητούν από τους δρομολογητές να τους στείλουν τις παραμέτρους διαμόρφωσής τους. Οι δρομολογητές ανταποκρίνονται σε αυτήν την αίτηση με ένα πακέτο διαφήμισης του δρομολογητή, το οποίο περιέχει τις παραμέτρους διαμόρφωσης του Επιπέδου Internet (Internet Layer). Εάν η Ανεπίσημη αυτόματη απόδοση διευθύνσεων IPv6 είναι ακατάλληλη για μία εφαρμογή, τότε ένα δίκτυο μπορεί να χρησιμοποιεί επίσημη διαμόρφωση (stateful configuration) χρησιμοποιώντας το Πρωτόκολλο Δυναμικής Απόδοσης Διευθύνσεων, έκδοσης 6 (Dynamic Host Configuration Protocol version 6 (DHCPv6)), ή ακόμη μπορεί να αποδοθεί στη συσκευή χειροκίνητα μία διεύθυνση IPv6 (στατική διεύθυνση). Η ταχύτητα τις διαδικασίας είναι η βέλτιστη καθώς με το νέο πρωτόκολλο έχει απλοποιηθεί η επικεφαλίδα και η προώθηση του πακέτου. Παρόλο που η επικεφαλίδα των πακέτων IPv6 είναι τουλάχιστον διπλάσια από την επικεφαλίδα των πακέτων IPv4, η επεξεργασία των πακέτων είναι αποδοτικότερη, επειδή χρειάζονται λιγότερη επεξεργασία από τους δρομολογητές. Αυτό προάγει την σχεδιαστική Αρχή απ΄ Άκρου σ΄ Άκρο (end-to-end principle)του Internet, η οποία προβλέπει ότι η περισσότερη επεξεργασία πρέπει να πραγματοποιείται στους ακραίους κόμβους. Η επικεφαλίδα του πακέτου IPv6, είναι απλούστερη από την επικεφαλίδα του πακέτου IPv4. Πολλά πεδία τα οποία χρησιμοποιούνται σπάνια, έχουν μετακινηθεί στις προαιρετικές επεκτάσεις της επικεφαλίδας. Οι δρομολογητές IPv6, δεν κάνουν διάσπαση των πακέτων IP. Οι συσκευές IPv6, είναι υποχρεωμένες είτε να ανακαλύψουν την Μέγιστη Μονάδα Μεταφοράς της Διαδρομής (path MTU discovery), ή να μην στείλουν πακέτα μεγαλύτερα από την προεπιλεγμένη Μέγιστη Μονάδα Μεταφοράς (Maximum transmission unit, MTU),η οποία είναι 1280 οκτάδες.

Επιπλέων ένα νέο χαρακτηριστικό του IP Version 6 είναι αφαίρεση του περιορισμού του ορίου μεγέθους του πακέτου σε 2^{16}–1 οκτάδες δεδομένων που ίσχυε στην εμπορικά προηγούμενη έκδοση. Ένας κόμβος IPv6, μπορεί προαιρετικά να επεξεργαστεί πακέτα πάνω από αυτό το όριο. Αυτό διευκολύνει την διεκπεραίωση επιπλέων δυνατοτήτων του κόμβου, όπως αυτού του SLAC. Τα πακέτα αυτά αναφέρονται σαν Jumbograms και μπορούν να έχουν μέγεθος μέχρι 2^{32}–1 οκτάδες. Η χρήση των Jumbograms μπορεί να βελτιώσει την απόδοση πάνω σε συνδέσεις υψηλού MTU.

7.6 ΜΗΧΑΝΙΣΜΟΙ ΜΕΤΑΒΑΣΗΣ

Σε σύγκριση με το IPv4, το πιο προφανές πλεονέκτημα του IPv6,είναι ο μεγαλύτερος χώρος διευθύνσεων. Οι διευθύνσεις στο IPv4 έχουν μήκος 32 bits, το οποίο μας παρέχει $4{,}3x10^9$ (4,3 δισεκατομμύρια)διευθύνσεις. Οι διευθύνσεις στο IPv6 έχουν μήκος 128 bits, που καταλήγει σε έναν χώρο $3{,}4\times10^{38}$ διευθύνσεων. Ένας τέτοιος χώρος διευθύνσεων κρίνεται επαρκής για το ορατό μέλλον. Μέχρις ότου το IPv6 εκτοπίσει πλήρως το IPv4, είναι απαραίτητος ένας αριθμός μεταβατικών μηχανισμών, που θα επιτρέψει σε συσκευές που χρησιμοποιούν μόνο το IPv6, να έχουν πρόσβαση σε υπηρεσίες του IPv4, και να επιτρέψουν σε απ΄ άκρου σε άκρον συσκευές που χρησιμοποιούν το IPv6, να μπορούν να επικοινωνούν μέσα από ένα δίκτυο που υποστηρίζει μόνο IPv4. Πολλοί από αυτούς τους μεταβατικούς μηχανισμούς χρησιμοποιούν την τεχνική tunneling, με την οποία ενθυλακώνουν κυκλοφορία του IPv6 σε δίκτυα IPv4. Αυτή είναι μία ατελής λύση η οποία μπορεί να δημιουργήσει προβλήματα. Τα πρωτόκολλα **tunneling** είναι μία προσωρινή λύση για δίκτυα τα οποία δεν υποστηρίζουν διπλή στοίβα (dual-stack), όπου και τα δύο πρωτόκολλα τρέχουν ανεξάρτητα το ένα από το άλλο. Παρακάτω αναλύονται κάποιοι μηχανισμού μετάβασης, και τρόπους συμβατότητας μεταξύ του IPv4 & IPv6

- **SIIT.**
  Η μέθοδος Stateless IP/ICMPP Translation είναι υπεύθυνη για την μετάφραση των κεφαλίδων, μεταξύ IPv4 & IPv6 με παράδειγμα επικεφαλίδας του IPv6 σε μορφή: *::ffff:0:0:0/96* και μετατρέπει την την επικεφαλίδα σε μια μορφή της τάξης *::ffff:0:a.b.c.d*, μια μορφή που κατανοείται από την Ipv4. Όπως είναι κατανοητό η μέθοδος SIIT είναι μια τεχνική που στοχεύει στο πρόβλημα μετάφρασης, και επιλύνει μεμονωμένα το πρόβλημα, αλλά είναι υποχρεωτική η χρήση συμπληρωματικής τεχνικής για την επίλυση της συμβατότητας, όπως τεχνικές tunneling που αναλύονται στη συνέχεια.

- **Tunneling.**
  Πολλοί από τους τωρινούς χρήστες του Internet δεν έχουν υποστήριξη διπλής στοίβας για το IPv6. Επομένως δεν μπορούν να έχουν απ' ευθείας πρόσβαση σε τοποθεσίες IPv6. αντίθετα πρέπει να χρησιμοποιήσουν δίκτυα IPv4 για να μεταφέρουν πακέτα IPv6. Αυτό επιτυγχάνεται χρησιμοποιώντας μία τεχνική γνωστή ως tunneling, η οποία ενθυλακώνει πακέτα IPv6 μέσα σε IPv4, χρησιμοποιώντας στην πραγματικότητα το IPv4 σαν επίπεδο σύνδεσης αντί του IPv6.

Το πρωτόκολλο IP 4, δηλώνει πακέτα IPv4 τα οποία ενθυλακώνουν αυτοδύναμα πακέτα (datagrams) IPv6. Μερικοί δρομολογητές ή συσκευές μετατροπής διευθύνσεων δικτύου (NAT) μπορεί να μπλοκάρουν την τεχνική αυτή. Για να διέλθει διαμέσου τέτοιων συσκευών, μπορεί να χρησιμοποιηθούν πακέτα UDP για την ενθυλάκωση αυτοδύναμων πακέτων IPv6. Δημοφιλείς είναι επίσης και άλλες μορφές ενθυλάκωσης, όπως οι AYIYA και η Generic Routing Encapsulation. Αρκετοί προηγμένοι δρομολογητές, ενθυλακώνουν μια τεχνική η

οποία ονομάζεται αυτοματοποιημένη τεχνική tunneling(automatic tunneling) η οποία λειτουργεί με τις τεχνικές και προσφέρει το πλεονέκτημα μετάβασης από το IP4 σε IP6, όπως εξηγήθηκε παραπάνω. Οι προδιαγραφές αυτής της αυτοματοποιημένης λειτουργείας ορίζεται με τα παρακάτω πρωτόκολλα:

- Το πρωτόκολλο **6to4**, με βάση τις προδιαγραφές του RFC3056 βασίζεται στο πρωτόκολλο ενθυλάκωσης νούμερο 41. Η τεχνική αυτήν είναι η πιο διαδεδομένη τεχνική μέχρι σήμερα.

- Το πρωτόκολλο **Teredo**, χρησιμοποιεί ενθυλάκωση τύπου UDP και μπορεί να μεταδώσει σε πολλαπλούς NAT κόμβους, αυτή η τεχνική εισάχθηκε στην αγορά το 2007 με τα Windows Vista και επίσης υποστηρίζεται και σε UNIX συστήματα.

- Το πρωτόκολλο **ISATAP**, διαφέρει σχετικά με τα παραπάνω αναφερόμενα πρωτόκολλα καθώς χρησιμοποιεί το δίκτυο IPv4 σαν εικονικό δίκτυο, και χρησιμοποιεί πίνακες που αντιστοιχούν διευθύνσεις IPv4 σε διευθύνσεις IPv6. Επιπλέων αυτή η τεχνική χαρακτηρίζεται σαν intra-site τεχνική, δηλαδή υπάρχει η δυνατότητα δημιουργίας εικονικού δικτύου ανάμεσα σε δύο κόμβους αντί όλου του δικτύου, μέσα σε ένα εταιρικό δίκτυο.

- **Dual Stack.**

  Η διπλή στοίβα αναφέρεται σε απ΄ άκρον σε άκρο πραγματοποίηση και των δύο πρωτοκόλλων του IPv4 και IPv6. Δηλ. και τα δύο πρωτόκολλα τρέχουν στο ίδιο δίκτυο και δεν είναι απαραίτητη η ενθυλάκωση του IPv6 στο IPv4 και αντιστρόφως. Η διπλή στοίβα καθορίζεται στο RFC 4213 (RFC Forum 2005). Παρότι αυτή είναι η πλέον πρόσφορη πραγματοποίηση του IPv6, καθότι παρακάμπτει πολλά μειονεκτήματα της τεχνικής tunneling, δεν είναι πάντοτε εφικτή, επειδή πεπαλαιωμένος δικτυακός εξοπλισμός δεν μπορεί να υποστηρίξει το IPv6. Έτσι π.χ. δρομολογητές συνδρομητών μπορεί να χρειάζονται είτε ενημέρωση του software είτε ακόμη και αλλαγή του hardware. Αυτό σημαίνει ότι διαχειριστές δικτύων πρέπει να καταφεύγουν στην τεχνική του tunneling, μέχρις ότου η ραχοκοκαλιά των δικτύων υποστηρίξει τη διπλή στοίβα.

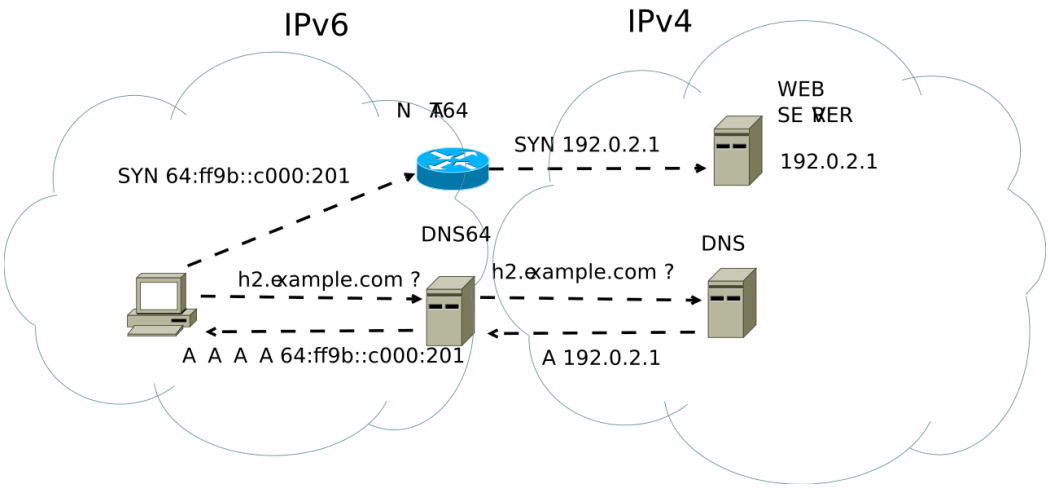
- **Embedded Systems.**

  Εξοπλισμός χαμηλού επιπέδου, όπως κάρτες δικτύου και μεταγωγείς δικτύου μπορεί να μην επηρεαστούν από την αλλαγή του πρωτοκόλλου, εφ' όσον μεταδίδουν πλαίσια επιπέδου σύνδεσης χωρίς να εξετάζουν το περιεχόμενο. Όμως δικτυακές συσκευές οι οποίες χρησιμοποιούν την διεύθυνση IP για να πραγματοποιήσουν την δρομολόγηση, χρειάζεται να κατανοούν το IPv6. Το μεγαλύτερο μέρος του εξοπλισμού θα μπορούσε με αναβάθμιση του software ή του firmware να μεταβεί στο πρωτόκολλο IPv6, με την προϋπόθεση ότι διαθέτει επαρκή

μνήμη EEPROM για τη νέα στοίβα του IPv6 και μνήμη RAM. Όμως οι κατασκευαστές μπορεί να είναι απρόθυμοι να ξοδέψουν για την ανάπτυξη software για hardware το οποίο έχουν ήδη πουλήσει, όταν αποβλέπουν σε νέες πωλήσεις συσκευών που υποστηρίζουν το πρωτόκολλο IPv6.
Σε άλλες περιπτώσεις ασύμβατος εξοπλισμός πρέπει να αντικατασταθεί, είτε διότι ο κατασκευαστής δεν υπάρχει πλέον, είτε διότι το firmware του δικτύου είναι γραμμένο σε μόνιμη μνήμη μόνο ανάγνωσης(ROM).

- **Proxy Server using NAT Technology.**

  Η επόμενη λύση που μπορούν να εκμεταλλευτούν οι υπεύθυνοι IT επιχειρησιακών και οργανισμών για την διατήρηση συμβατότητας με την IPv6 είναι η χρήση ενός web proxy server, και της χρήση της τεχνολογίας NAT64 για την επικοινωνία των διευθύνσεων IPv6 με διευθύνσεις IPv4 καθώς η τεχνολογία του NAT64 δημιουργεί έναν «χάρτη» των IPv4 & IPv6 διευθύνσεων που επιτρέπει την επικοινωνία.



7.6 Σχεδιάγραμμα Επικοινωνίας μέσω NAT64 & DNS64

7.7 ΣΤΑΤΙΣΤΙΚΑ

Η αλλαγή των πρωτοκόλλων του IPv4 σε IPv6 θα πραγματοποιηθεί σταδιακά, με αργούς ρυθμούς σε όλη την εμφύλιο, η πρώτη αξιοσημείωτη αλλαγή με στατιστικά νούμερα σημειώθηκαν τον Σεπτέμβριο του 2013, με ποσοστό 4% να έχει αλλάξει IPv4 domain name, και σε ποσοστό 16,2% των δικτύων παγκοσμίως που μπορούν να υποστηρίξουν πρωτόκολλο IPv6.

Από την πλευρά των Λειτουργικών Συστημάτων υπολογιστών, η υποστήριξη έχει ξεκινήσει από το 2008, σε όλα τα κύρια UNIX και Windows συστήματα, καθώς τόσο για καταναλωτές και σε επιχειρήσεις/οργανισμούς, με παράδειγμα οι κυβερνήσεις των ΗΠΑ & Κίνα να χρησιμοποιούν πρωτόκολλο IPv6.

Το 2009 οι πάροχοι κινητών υπηρεσιών των ΗΠΑ ολοκλήρωσαν τις διεργασίες για την υποστήριξη των IPv6, υποστήριξη τεχνολογίας LTE ενώ στον Ελλαδικό χώρο ο πάροχος ΟΤΕ έφερε την LTE συνδεσιμότητα τον Νοέμβριο του 2012. Σε πιο πρόσφατο κλίμα, οι συσκευές με IPv6 που χρησιμοποίησαν την μηχανή αναζήτησης της Google, ανήλθαν σε ποσοστό 11,1% με ποσοστό ανάπτυξης 4,8% σε σύγκριση με το 2005 ενώ οι Web Servers σε παγκόσμια κλίμακα 14% υποστηρίζουν το νέο πρωτόκολλο του IP με βάση τα στατιστικά στοιχεία (Wikipedia, 2016 < https://en.wikipedia.org/wiki/IPv6#Deployment >, τελευταία επίσκεψη 26 Μαΐου 2016).

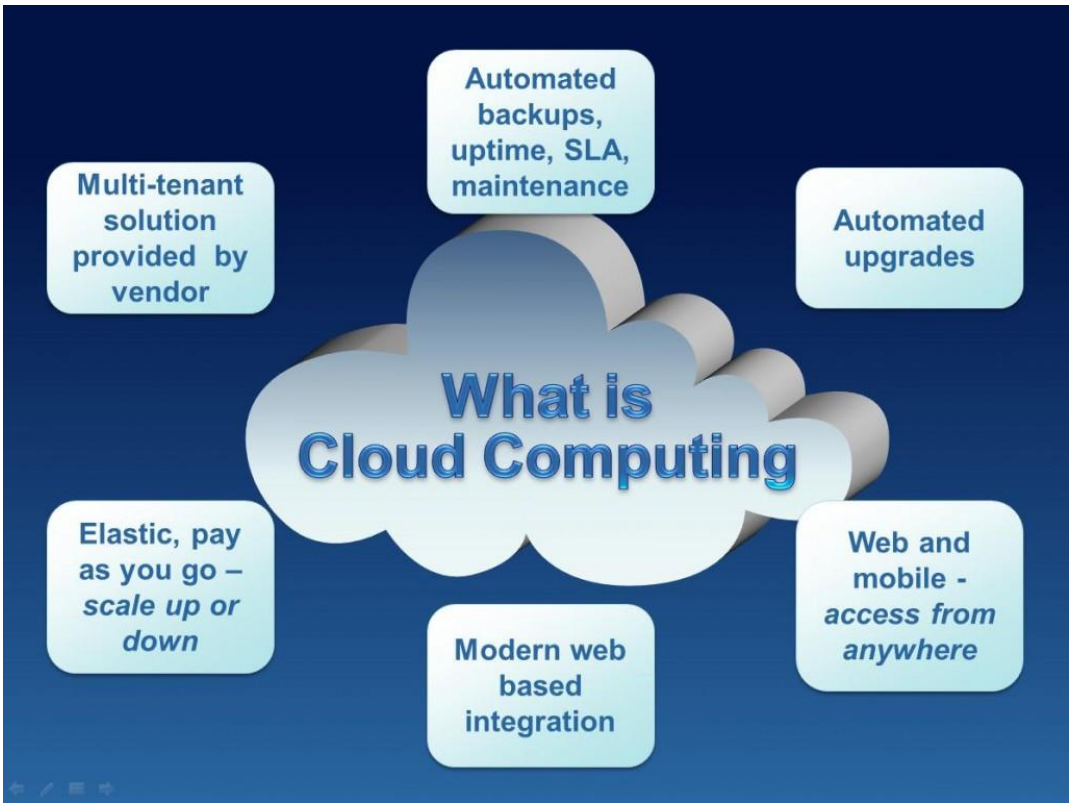
8. Cloud Computing

Η έννοια cloud computing συνδέεται με την ορολογία του Internet of Things, και την τεχνολογική εξέλιξη που ακολουθεί. Το Cloud Computing ή αλλιώς στα ελληνικά το Υπολογιστικό Νέφος, είναι η συνέχεια του αρκετά παλαιότερου **Application Service Provisioning** με την ενσωμάτωση νέων τεχνολογιών και δυνατοτήτων, και την γενική υλοποίηση της αφαιρετικότητας, δηλαδή ότι ο χώρος του cloud computing δεν ανήκει σε φυσικό χώρο αλλά και σε φυσικό ιδιοκτήτη. Αντιθέτως, στην υλοποίηση του cloud computing για την εξασφάλιση χωρητικότητας των προσωπικών μας δεδομένων, ο καταναλωτής ενοικιάζει/αγοράζει ένας μέρος από τους πόρους και τον χώρο της υπηρεσίας, και αυτομάτως ορίζεται ιδιοκτήτης των δεδομένων αυτών.

Οι υπολογιστικοί πόροι του παρόχου χρησιμοποιούνται για να εξυπηρετήσουν πολλαπλούς καταναλωτές με τη χρήση του μοντέλου πολλαπλών μισθωτών (multi-tenant), με τους διάφορους φυσικούς και εικονικούς πόρους να ανατίθενται δυναμικά και εκ νέου ανάλογα με τη ζήτηση των καταναλωτών. Υπάρχει μια αίσθηση ανεξαρτησίας από τον τόπο στο γεγονός ότι ο πελάτης δεν έχει γενικά κανέναν έλεγχο ή γνώση σχετικά με την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά μπορεί να είναι σε θέση να προσδιορίζει την τοποθεσία σε ένα υψηλότερο επίπεδο αφαίρεσης (πχ. χώρα, κράτος, ή datacenter). Παραδείγματα πόρων αποτελούν οι αποθηκευτικοί χώροι, η επεξεργασία, η μνήμη, το bandwidth του δικτύου, καθώς και οι εικονικές μηχανές. Ένας καταναλωτής μπορεί να δεσμεύσει από μόνος του τους υπολογιστικούς πόρους που χρειάζεται ανάλογα με τις ανάγκες του, όπως χρόνο στον server και αποθηκευτικό χώρο στο δίκτυο, ανάλογα και με το κόστος που δίνει η εταιρία που προσφέρει την υπηρεσία. Οι δυνατότητες είναι διαθέσιμες μέσω του δικτύου και προσβάσιμες μέσω τυποποιημένων μηχανισμών που προωθούν την χρήση από ετερογενείς thin ή thick client πλατφόρμες (π.χ. κινητά τηλέφωνα, φορητούς υπολογιστές και PDAs).Το άλλο και σημαντικό που κάνει την τεράστια διαφορά, είναι πως το cloud διαθέτει virtualization, τ' οποίο τα τελευταία χρόνια κάλπασε σε εξέλιξη. Με την χρήση επιτυγχάνεται μια ισότητα και εξοικονόμηση πόρων, καθώς ο καθένας χρησιμοποιεί το αναγκαίο ποσοστό των πόρων που μπορούν να δεσμευτούν προς χρήση γρήγορα και ελαστικά, σε ορισμένες περιπτώσεις αυτόματα, έτσι ώστε να εμφανιστούν άμεσα ως μη διαθέσιμοι (scale out) και επίσης να αποδεσμευτούν γρήγορα για να εμφανιστούν ξανά ως διαθέσιμοι (scale in). Για τον καταναλωτή, οι διαθέσιμες δυνατότητες για δέσμευση και χρήση συχνά φαίνεται να είναι απεριόριστες και μπορούν να αγοραστούν ανά πάσα στιγμή και σε οποιαδήποτε ποσότητα. Για να γίνει κατανοητή ο όρος **virtualization**, θα εμβαθύνουμε ελαφρά προς την κατανόηση του. Δηλαδή με το virtualization το hardware διαχωρίζεται από το software (λειτουργικά συστήματα και εφαρμογές). Ο hypervisor είναι ένα νέο επίπεδο «virtualization layer»

μεταξύ του hardware και του software, που ενοποιεί τους φυσικούς πόρους και τους διαμοιράζει στα ιδεατά συστήματα με τρόπο διάφανο. Τα ιδεατά συστήματα συνεχίζουν να νομίζουν ότι επικοινωνούν απευθείας με το hardware, αλλά στην πραγματικότητα επικοινωνούν με το **virtualization layer**. Αυτό επιτρέπει τη μετακίνηση επεξεργαστικής ισχύος, μνήμης ή και storage από ένα virtual machine σε άλλο εν ώρα λειτουργίας και σύμφωνα με τις ανάγκες. Το αποτέλεσμα είναι η καλύτερη εκμετάλλευση των πόρων συνολικά οποιαδήποτε χρονικής στιγμής , μεγάλη εξοικονόμηση ενέργειας και φυσικού χώρου και ευκολότερη διαχείριση της υποδομής. Σήμερα το virtualization έχει διεισδύσει σε πολλές επιχειρήσεις, αλλά αναμένεται ότι γρήγορα τα περισσότερα συστήματα θα γίνουν ιδεατά, καθώς οι απαιτήσεις για αποδοτική χρησιμοποίηση του hardware, μείωση της ηλεκτρικής κατανάλωσης και αναγκών ψύξης, γίνονται όλο και πιο επιτακτικές. Αυτά τα συστήματα έχουν την ικανότητα να καλύπτουν εκτενέστερες γεωγραφικές περιοχές, με την ποικιλομορφία χρήσης του συστήματος για τις ανάγκες του κάθε ξεχωριστού χρήστη. Αυτό το είδος λειτουργικότητα ονομάζεται **multi-tenacy** με το οποίο χρήστες διαφορετικών λειτουργικών συστημάτων, διαφορετικών χωρών, χρησιμοποιούν το ίδιο σύστημα και σε πολλές περιπτώσεις και την ίδια βάση δεδομένων. Τα συστήματα cloud ελέγχουν και βελτιστοποιούν αυτόματα τη χρήση των πόρων, αξιοποιώντας μια δυνατότητα μέτρησης σε κάποιο επίπεδο αφαίρεσης που είναι κατάλληλο για το είδος της υπηρεσίας (πχ. αποθήκευση, επεξεργασία, bandwidth, ενεργοί λογαριασμοί χρηστών).Η χρήση των πόρων μπορεί να παρακολουθείται, να ελέγχεται, και να παρουσιάζεται με τη μορφή reports, παρέχοντας διαφάνεια τόσο για τον πάροχο όσο και για τον καταναλωτή της χρησιμοποιούμενης υπηρεσίας. Η αρχή του **multitenancy** δεν είναι καθολικά αποδεκτή και στηρίζεται στη βιομηχανία λογισμικού, και αυτό μπορεί να είναι μια πηγή ανταγωνιστικής διαφοροποίησης.

Καθώς το Cloud Computing είναι αναπόσπαστο κομμάτι του Internet of Things, και της υπολογιστής οντότητας που ξέρουμε ως σήμερα, το National Institute of Standards and Technology(NIST) των Ηνωμένων Πολιτειών Αμερικής έχει εκδώσει την σημασία ορολογίας και εννοιών του Cloud Computing (Peter Mell & Tim Grace(2009) **Definition of Cloud Computing.** ΗΠΑ: NIST), με βάση την ορολογία θα εμβαθύνουμε στην κατανόηση του Cloud Computing.



***8.0.1** Έννοιες που αντιπροσωπεύει το Cloud Computing*

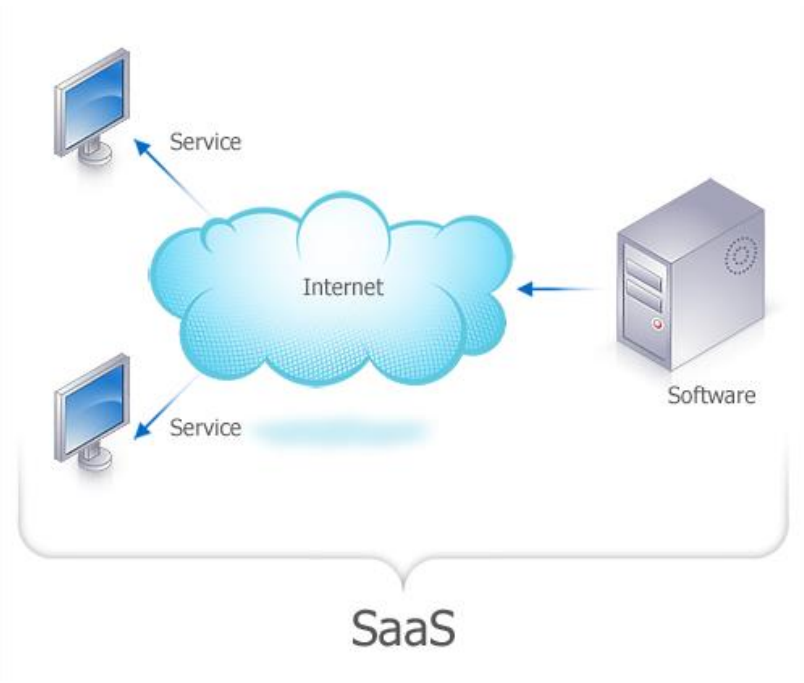
Το cloud computing είναι ένα μοντέλο που επιτρέπει ευέλικτη, on-demand δικτυακή πρόσβαση σε ένα κοινόχρηστο σύνολο παραμετροποιήσιμων υπολογιστικών πόρων (όπως δίκτυα, servers, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες), το οποίο μπορεί να τροφοδοτηθεί γρήγορα και να διατεθεί με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο της υπηρεσίας. Αυτό το cloud μοντέλο προωθεί την διαθεσιμότητα και αποτελείται από πέντε βασικά χαρακτηριστικά, τρία μοντέλα παροχής υπηρεσιών, και τέσσερα μοντέλα ανάπτυξης:

- **Private cloud:** Η cloud υποδομή λειτουργεί αποκλειστικά και μόνο για έναν. Η διαχείρισή της μπορεί να γίνεται από τον ίδιο τον οργανισμό και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού.
- **Community cloud:** Η cloud υποδομή μοιράζεται μεταξύ πολλών οργανισμών και υποστηρίζει μια συγκεκριμένη κοινότητα που έχει κοινές ανησυχίες (πχ. αποστολή, απαιτήσεις ασφαλείας, πολιτική και θέματα συμμόρφωσης). Η διαχείρισή της μπορεί να γίνεται από τον ίδιο τον οργανισμό ή από τρίτους και μπορεί να βρίσκεται εντός ή εκτός των εγκαταστάσεων του οργανισμού.
- **Public cloud:** Η cloud υποδομή διατίθεται στο ευρύ κοινό ή σε μια μεγάλη ομάδα εταιρειών και ανήκει σε έναν οργανισμό που πουλά υπηρεσίες cloud.

- **Hybrid cloud:** Η cloud υποδομή είναι μια σύνθεση από δύο ή περισσότερα clouds (private, community or public) τα οποία παραμένουν μοναδικές οντότητες, αλλά συνδέονται μεταξύ τους με τυποποιημένη ή αποκλειστική τεχνολογία που επιτρέπει τη φορητότητα δεδομένων και εφαρμογών (π.χ. εξισορρόπηση φόρτου εργασίας μεταξύ των clouds).

Αντίστοιχα και τα μοντέλα παροχής υπηρεσιών ποικίλουν, προσφέροντας διαφορετικές δυνατότητες. Συνοπτικά, αυτά που ισχύουν την δεδομένη στιγμή, είναι τα ακόλουθα:

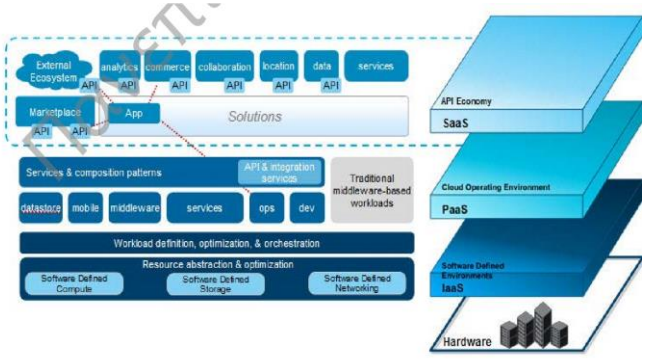
- **Cloud Software as a Service (SAAS):** Η δυνατότητα που παρέχεται στον καταναλωτή είναι να χρησιμοποιεί τις εφαρμογές του παρόχου που τρέχουν σε μια cloud υποδομή. Οι εφαρμογές είναι προσβάσιμες από διάφορες client συσκευές μέσω ενός thin client interface, όπως ένα πρόγραμμα περιήγησης στο Web (π.χ. web-based email). Ένα καλό παράδειγμα, ώστε να γίνει αντιληπτό αυτό είναι το Google Drive και οι εφαρμογές που μπορούν να τρέξουν απ' ευθείας σε αυτό.



  Ο καταναλωτής δεν έχει τη διαχείριση ή τον έλεγχο της χρησιμοποιούμενης cloud υποδομής συμπεριλαμβανομένων των δικτύων, των servers, των λειτουργικών συστημάτων, των αποθηκευτικών μονάδων, ή ακόμα και μεμονωμένων δυνατοτήτων της εφαρμογής, με την πιθανή εξαίρεση κάποιων περιορισμένων user-specific ρυθμίσεων παραμετροποίησης των εφαρμογών.
- **Cloud Platform as a Service (PAAS):** Η δυνατότητα που παρέχεται στον καταναλωτή είναι να αναπτύσσει πάνω στην cloud υποδομή εφαρμογές που έχει δημιουργήσει ή εφαρμογές που έχει αποκτήσει, οι οποίες έχουν δημιουργηθεί με χρήση γλωσσών προγραμματισμού και εργαλείων που υποστηρίζονται από τον πάροχο. Ο καταναλωτής δεν διαχειρίζεται ούτε ελέγχει τη σχετική cloud υποδομή που συμπεριλαμβάνει τα δίκτυα, τους servers, τα λειτουργικά συστήματα ή τα αποθηκευτικά μέσα, αλλά έχει τον έλεγχο των εφαρμογών που έχουν αναπτυχθεί,

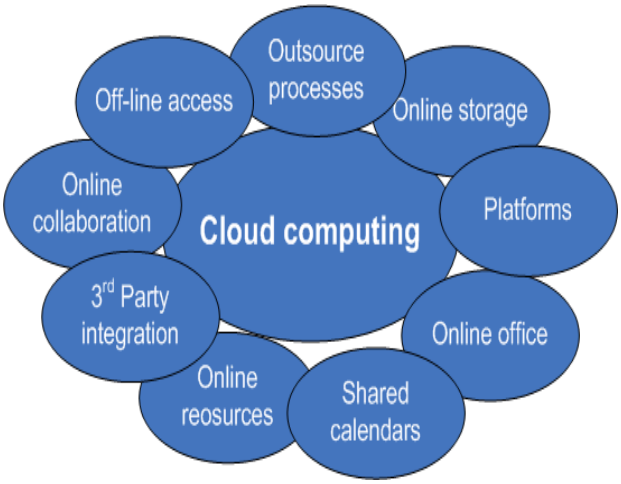
και ενδεχομένως, των παραμετροποιήσεων του περιβάλλοντος φιλοξενίας των εφαρμογών.

- **Storage as a Service (STAAS):** Στο μοντέλο αυτό υπάρχει κάποιος πάροχος αποθηκευτικού χώρου online ο οποίος στην ουσία τον νοικιάζει έναντι κάποιας αμοιβής. Ένα παράδειγμα απλό θα μπορούσε να θεωρηθεί το *Dropbox*.
- **Hardware as a Serice(HASS):** Ο προμηθευτής αυτής της cloud υπηρεσίας παρέχει στον χρήστη έναντι «ενοικίου»-αμοιβής το hardware που χρειάζεται όπως web servers, μνήμη CPU ,αποθηκευτικό χώρο και ότι άλλο χρειάζεται ο χρήστης σε επίπεδο hardware. Τα χρήματα που πληρώνει κάποιος στο HaaS είναι αντίστοιχα της χρήσεως των πόρων του συστήματος που κάνει.
- **Database as a Service (DAAS):** Σε αυτό το μοντέλο υπάρχει μία υπηρεσία online παρέχει την βάση δεδομένων την οποία μπορούμε να χρησιμοποιήσουμε με κάποιο web application. Σε αυτό το μοντέλο το βασικό πλεονέκτημα είναι ότι πληρώνουμε ανάλογα με την χρήση. Ουσιαστικά όσο πιο πολύ κόσμος χρησιμοποιεί την εφαρμογή μας τόσο περισσότερα χρήματα πληρώνουμε. Μία τέτοια υπηρεσία είναι η mongoDB.
- **Cloud Infrastructure as a Service (IAAS):** Η δυνατότητα που παρέχεται στον καταναλωτή είναι να μπορεί να δεσμεύσει προς χρήση επεξεργαστική ισχύ, αποθηκευτικά μέσα, δίκτυα, και άλλους θεμελιώδεις υπολογιστικούς πόρους, όπου ο καταναλωτής είναι σε θέση να αναπτύξει και να εκτελέσει αυθαίρετο λογισμικό, το οποίο μπορεί να περιλαμβάνει λειτουργικά συστήματα και εφαρμογές. Ο καταναλωτής δεν έχει τη διαχείριση ή τον έλεγχο της χρησιμοποιούμενης cloud υποδομής, αλλά έχει τον έλεγχο των λειτουργικών συστημάτων, των αποθηκευτικών μέσων, των εφαρμογών που έχουν αναπτυχθεί και πιθανόν κάποιον περιορισμένο έλεγχο επιλεγμένου εξοπλισμού δικτύωσης (π.χ. firewalls). Ένα καλό παράδειγμα, ώστε να γίνει αντιληπτό αυτό είναι το Oceanos IAAS το οποίο αναπτύχθηκε στο πλαίσιο ανάπτυξης από την ΕΕ με πρόγραμμα DigitalGreece, NSRF 2007-2013.



8.0.2 *Απεικόνιση ορισμού NIST για την Αρχιτεκτονική του Cloud Computing*

8.1 ΤΟ ΜΕΗΕΘΟΣ ΤΟΥ CLOUD



Η διάσταση του Cloud και η χωρητικότητα που δίνει η κάθε επιχείρηση στους καταναλωτές, είναι μεν κομμάτι της πολιτικής της εκάστοτε εταιρίας αλλά συνολικά ο χώρος που καταλαμβάνει μαζικά, από την οπτική της οντότητας σαν τεχνολογία και υπηρεσία που προσφέρεται, μετριέται σε μορφή petabytes στον κυβερνοχώρο.

Όπως είναι αντιληπτό, το μέγεθος είναι αρκετά μεγάλο, καθώς υπολογίστηκαν μικρές και κολοσσιαίες εταιρίες που προσφέρουν λύσεις cloud computing, όπως Google, Facebook, Amazon, Microsoft, Apple, με τα ανάλογα προϊόντα και υπηρεσίες που προσφέρουν.
Είναι σημαντικό να υπενθυμίσουμε ότι οι υπηρεσίες του Cloud, δεν σταματάνε στην Online αποθήκευση των δεδομένων και των Backup, αλλά επεκτείνονται σε ένα ευρύ φάσμα λειτουργικότητας. Ένα παράδειγμα είναι οι ευρέος γνωστές υπηρεσίας Mail όπως οι Gmail,Outlook,Yahoomail που βασίζονται στην αρχιτεκτονική του WebMail και υλοποιούνται με λύσεις Cloud Computing, καθώς και οι δικτυακές σουίτες γραφείου, όπως οι Zoho, GoogleDogs, OfficeOnline, και Live Documents. Επιπλέων η τεχνολογία του Cloud Computing και ο όγκος που προστίθεται αντανακλάτε και στην ψηφιακή ψυχαγωγία, με υπηρεσίες όπως το Spotify, iTunes και SoundCloud να λειτουργούν εξολοκλήρου με servers στο cloud, για να εξυπηρετήσουν τους πελάτες τους, για την αγορά ή την διαμοίραση μουσικής (streaming). Συνοψίζοντας οι παραπάνω υπηρεσίες χρειάζονται έναν σημαντικό μεγάλο χώρο αποθήκευση των δεδομένων για την σωστή λειτουργεία της υπηρεσίας αλλά και σαν μια ολοκληρωμένη εικόνα οικοσυστήματος. Παρακάτω θα παραθέσουμε κάποια νούμερα χωρητικότητας για τις εκάστοτε υπηρεσίες, για την κατανόηση ότι η τεχνολογία **cloud είναι ισόμετρη με τον συντελεστή χωρητικότητας**.

- Με ανακοίνωση της Facebook Inc. στο επίσημο site, δημοσίευσε ότι ο διαδικτυακός χώρος που αποδίδει ένα τυπικό warehouse της επιχείρησης ανέρχεται στην τάξη του 300 petabyte, με καθημερινή κίνηση των 600 tearybtes (Facebook, 2014, **Scaling the Facebook data warehouse to 300 PB** <https://code.facebook.com/posts/229861827208629/scaling-the-facebook-data-warehouse-to-300-pb/> Τελευταία επίσκεψη: 6/6/16).

- Η Microsoft με τα τελευταία στοιχεία που έδωσε στην δημοσιότητα, ο χώρος για τις υπηρεσίες Outlook & Onedrive της αντιστοιχούν σε 150petabytes και για την Azure Service σε 300 petabytes (Microsoft Datacenter Team,2015, **Datacenter Fact Sheet 2015**, https://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx>, Τελευταία επίσκεψη: 6/6/16)
- Η Dropbox από το 2012 και έπειτα έχει αναπτύξει την χωρητικότητα των datacenters αναλογικά με την εγγραφή νέων χρηστών, τις τάξεις 12X με αποτέλεσμα των Μάρτιο του 2016 τα data farms της εταιρίας να αντιστοιχούν σε 500 petabytes σε διάστημα 4 χρόνων. (Dropbox, 2016, **Scaling to exabytes and beyond** < https://blogs.dropbox.com/tech/2016/03/magic-pocket-infrastructure/>, Τελευταία επίσκεψη: 6/6/16).

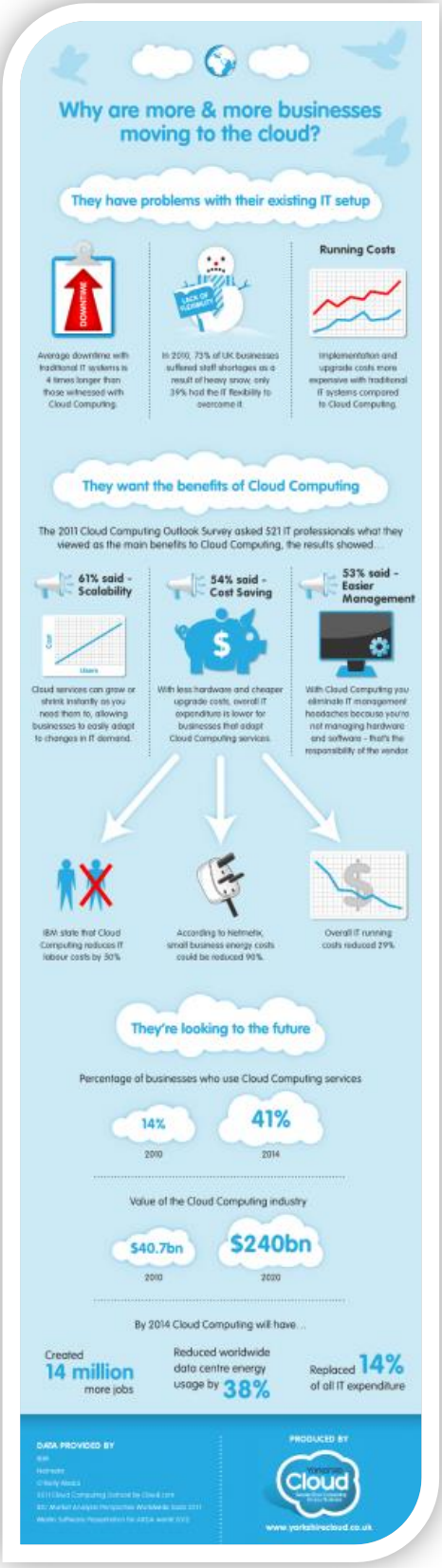
Για να γίνει κατανοητή η τάξη μεγέθους, η διαφορά με έναν προσωπικό υπολογιστή, η μέση χωρητικότητα είναι στα 500GB για συνολική αποθήκευση των δεδομένων, ρυθμίσεων και κομμάτια του λειτουργικού συστήματος. Ένα petabyte είναι 1024 terabytes, και για να αποτελέσει έναν data center, κατά μέσο όρο υπάρχουν πάνω από 100 χιλιάδες σκληροί δίσκοι, με συνολική γεωγραφική κάλυψη κτηρίου πάνω από 30,000 κυβικά εκατοστά, με την χρήση συστημάτων 4U enclosure για την σύμπτυξη 48 σκληρών δίσκων σε ένα συμπιεσμένο χώρο, για την εξοικονόμηση χώρου στο data center.

Εκτός από τον παράγοντα χώρου, τόσο ψηφιακού όσο και φυσικού η κάθε εταιρία, πρέπει να υπολογίσει και το **bandwidth**, που θα χρειαστεί, για να λειτουργήσει ομαλά η υπηρεσία που προσφέρει. Κάθε χρήστης υπολογίζεται ότι θα κάνει κάποιες κλήσεις προς τους servers της επιχείρησης. Για παράδειγμα, η Dropbox έχει ανακοινώσει ότι ο μέσος όρος ανταλλαγής δεδομένων είναι στα 6,7GB το δευτερόλεπτο, που αντιστοιχεί στα 57Gbps.

8.2 CLOUD & ΑΣΦΑΛΕΙΑ

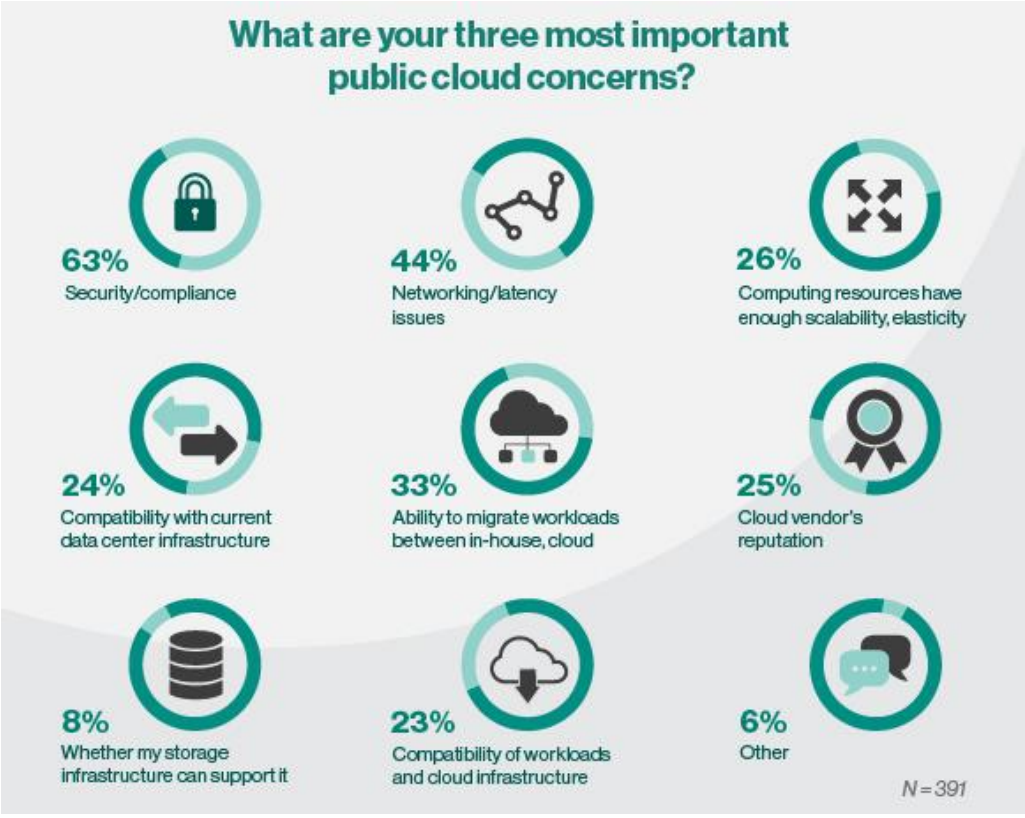
Σχετικά με τα ζητήματα ασφάλειας, όλες οι υπηρεσίες cloud έχουν προβλεφθεί οι δικλείδες ασφαλείας, όπως πολύ καλή χρήση δικαιωμάτων χρηστών, ασφαλή πρόσβαση (ακόμα και μέσω ανοικτού internet), όπως SSL και άλλα. Εκτός αυτού, υπάρχουν πιστοποιήσεις για προμηθευτές cloud υπηρεσιών που κινούνται σε συγκεκριμένα επίπεδα και τις οποίες ένα εσωτερικό τμήμα μηχανογράφησης δεν θα μπορούσε σχεδόν ποτέ να αποκτήσει.
Από κατασκευής λοιπόν, το επίπεδο ασφαλείας είναι πολύ ανώτερο συγκριτικά. Αυτό όμως είναι η Ασφάλεια, η οποία δεν εμπεριέχει και την απαραίτητη Ιδιωτικότητα. Τους λόγους τους αναφέραμε πιο πάνω και αφορούν πως τρέχουν σε τρίτους servers. Αυτές οι υπηρεσίες, χρησιμοποιούν συν τ' άλλα αλγορίθμους κρυπτογράφησης. Αυτό όμως έχει να κάνει και με τον καθένα που παρέχει αυτές. Σε αντίθεση με κάποιες άλλες υπηρεσίες cloud ανοιχτού κώδικα, οι οποίες παρέχουν ένα υψηλό επίπεδο κρυπτογράφησης, όπου τα δεδομένα του χρήστη, είναι εξ' φύσεως αδύνατο να ειδωθούν από όποιον έχει άμεση πρόσβαση στον server που αυτά βρίσκονται (για παράδειγμα το Tonido, η το Memopal. Φυσικά, η κάθε μια από αυτές τις υπηρεσιες έχει δώσει την δική της έμφαση στο θέμα κρυπτογράφησης, μα η κάθε μια σε διαφορετικά επίπεδα.

Επιπλέον, μιλώντας για επαγγελματικές και αυξημένες ανάγκες, όπου απαιτείται η αγορά μια τέτοιας υπηρεσίας (η ενοικίαση, σωστότερα), πρέπει να ληφθεί υπόψη πως το cloud δεν είναι μόνο λογισμικό. Είναι και υπηρεσίες που παρέχονται από τον προμηθευτή. Κάποιες τέτοιες συνοδευτικές εργασίες ενός λογισμικού οι οποίες πρέπει να παρέχονται από τον προμηθευτή σας,



είναι: updates σε νέες εκδόσεις, οι νέες release για το system software (για οποιοδήποτε λειτουργικό σύστημα υποστηρίζουν), το καθημερινό backup, ο έλεγχος υγείας (health-checks) όλων των επιμέρους συστημάτων, η συντήρηση των servers, για να διατηρηθεί η ακεραιότητα των επιπέδων ασφαλείας.

Φυσικά αυτά τα επίπεδα ασφάλειας μπορεί να μην είναι αρκετά για τα επαγγελματικά/εταιρικά δεδομένα τα οποία έχουν έχουν μια υψηλή διαβάθμιση. Σίγουρα το όσο ασφαλές και είναι cloud, δεν είναι η βέλτιστη λύση για όλα τα προβλήματα αποθήκευσης και κινητικότητας της επιχείρησης. Σε μια εποχή που η βιομηχανική/εταιρική κατασκοπία και ανταγωνισμός βρίσκεται σε έξαρση, με την χρήση ευαίσθητων δεδομένων- ακόμα και άνευ επαρκών ενδείξεων- είναι αρκετό για να στοχοποιηθεί και κατηγορηθεί η επιχείρηση. Σε μια εποχή που είμαστε σε διαρκή κίνηση και συγχρόνως η πρόσβαση στο διαδίκτυο μπορεί να είναι και φορητή, από οποιοδήποτε σημείο. Μπορούμε να έχουν διάφορα αναγκαία έγγραφα μας, αρχεία, την μουσική τις φωτογραφίες μας, να διαμοιραζόμαστε υλικό με άλλους ανθρώπους, και με επιπλέον ακόμα παρελκόμενες υπηρεσίες και ευκολίες που προσφέρει ο κάθε πάροχος και η χρήση της τεχνολογίας του Cloud Computing.



8.3 ΛΙΣΤΑ HOSTING SERVICES

Παρακάτω παρατίθεται μια λίστα, καθώς έχει γίνει διαδικτυακή έρευνα για τους παρόχους που προσφέρουν μια ευρεία γκάμα Cloud υπηρεσιών.

1. **Acronis**
2. **Backblaze**
3. **Barracuda Backup Services**
4. **Bitcasa**
5. **BOX**
6. **BullGuard**
7. **CloudMe**
8. **Comodo**
9. **CrashPlan**
10. **Cubby**
11. **CloudPT**
12. **Diino**
13. **Dropbox**
14. **Dropmysite**
15. **Dump Truck**
16. **Druva Insync**
17. **Engyte**
18. **ElephantDrive**
19. **Evault**
20. **FilesAnywhere**
21. **Google Drive**
22. **GoAruna**
23. **HandyBackup**
24. **iCloud**
25. **Infint**
26. **Inrascale**
27. **Iperius Online Storage**
28. **Inntonis**
29. **Jumpshare**
30. **JustCloud**
31. **Jungle Disk**
32. **KeepVault**
33. **KinericD**
34. **MediaFire**
35. **Mega**

36. **Memopal**
37. **MiMedia**
38. **Minus**
39. **MyPogolup**
40. **Mozy**
41. **MyVault**
42. **OneDrive**
43. **ownCloud**
44. **PowerFolder**
45. **Pithos**
46. **SpiderOAK**
47. **SugarSync**
48. **SyncBox**
49. **Sparkleshare**
50. **Seafile**
51. **Syncplicity**
52. **Tarsnap**
53. **TeaDrive**
54. **Tresorit**
55. **Tonido**
56. **Wuala**
57. **Zetta**
58. **Zmada**

8.4 ΟΦΕΛΗ ΓΙΑ ΤΟΥΣ ΧΡΗΣΤΕΣ

Τα οφέλη για τους τελικούς χρήστες από την χρήση της διαδικτυακής δομής Cloud Computing περιλαμβάνουν την σημαντικότατη μείωση του κόστους χρήσης λογισμικού, καθώς η χρέωση πραγματοποιείται τμηματικά ανάλογα με την χρήση και όχι κατά την χρήση/εγκατάσταση όπως με το συμβατικό λογισμικό. Επίσης, την αύξηση ταχύτητας χρήσης, ευελιξίας και συμβατότητας των δεδομένων, καθώς και την χρήση και εφαρμογή της τεχνολογίας χωρίς να απαιτείται η αγορά οποιουδήποτε επιπλέον software ή hardware για την ταχύτατη εκμάθηση εφαρμογών από τους τελικούς χρήστες.Την απεριόριστη χωρητικότητα (on-line) αποθήκευσης δεδομένων χωρίς την ανάγκη προμήθειας συμβατικών μέσων αποθήκευσης όπως οι εξωτερικοί σκληροί δίσκοι καθώς και την ταχύτατη πρόσβαση σε πληροφορίες (on-line) από οποιοδήποτε μέρος του κόσμου με υψηλή ασφάλεια δεδομένων και το ταχύτατο real-time back-up δεδομένων που πραγματοποιείται αυτόματα εξοικονομώντας χρόνο για τους τελικούς χρήστες. Είναι ευνόητο λοιπόν ότι ένας μεγάλος πάροχος υπηρεσιών cloud computing μπορεί να προσφέρει καλύτερες, πιο εξελιγμένες και πιο φθηνές υπηρεσίες ασφάλειας στους χρήστες σε σύγκριση με την αυτόνομη δημιουργία cloud λύσεων από τον ίδιο. Μπορεί επίσης να προσφέρει μηχανισμούς κωδικοποίησης με σκοπό να αυξήσει την αποδοτικότητα των μέτρων που λαμβάνει, ώστε να αποφεύγει απειλές, ενώ αντίθετα με το αυτόνομο cloud δίκτυο του χρήστη, αυτό είναι δύσκολο να επιτευχθεί. Σχετικά με τα πλεονεκτήματα προς την πράσινη οικονομία εκτιμάται ότι αν σήμερα η εν λόγω τεχνολογία χρησιμοποιούνταν πλήρως από όλους τους χρήστες πληροφορικής οι ατμοσφαιρικοί ρύποι στον πλανήτη θα μπορούσαν να μειωθούν έως και 5% συνολικά ή αλλιώς 2,5 δισεκατομμύρια τόνους διοξείδιο του άνθρακα (CO_2). Σημειώνεται ότι η επιβάρυνση του περιβάλλοντος από την χρήση συστημάτων πληροφορικής ενδέχεται να διπλασιαστεί την επόμενη 10ετία, άρα η μείωση των ατμοσφαιρικών ρύπων παγκόσμια θα μπορούσε να μειωθεί σε βάθος χρόνου έως και 5 δισεκατομμύρια τόνους διοξείδιο του άνθρακα (CO_2) ετησίως χάρη στην χρήση της τεχνολογίας Cloud Computing.

8.5 ΟΦΕΛΗ ΓΙΑ ΤΙΣ ΜΙΚΡΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Τα οφέλη για τις εταιρίες και ιδιαίτερα για τις μικρές επιχειρήσεις όπως τονίζει η Microsoft χωρίζονται σε 10 βασικά επίπεδα, τα οποία καλύπτουν τις ανάγκες τις επιχείρησης στον τομέα IT και προτρέπουν την σταδιακή μετατροπή τους, με την χρήση τεχνολογίας Cloud Computing. Η εργασιακή ασφάλεια είναι ένας κρίσιμος παράγοντας καθώς η διατήρηση των δεδομένων ανάλογα με τις ανάγκες της αγοράς, καθώς και η υλοποίηση προσαρμοσμένων ροών εργασίας, εξακολουθούν να είναι ευθύνη της επιχείρησης. Αν και ορισμένες εργασίες δεν πραγματοποιούνται πλέον στις εγκαταστάσεις του οργανισμού σας, οι διαχειριζόμενες υπηρεσίες cloud εξασφαλίζουν περισσότερο χρόνο για πιο στρατηγικούς ρόλους, παρέχοντας νέες ευκαιρίες και εξασφαλίζοντας τον σωστό κατακερματισμό του συστήματος με συνέπεια την εξασθενημένη εργασιακή ασφάλεια.

Στον ελληνικό χώρο, υπάρχει ο φόβος της πτώσης σε προοπτικές εξέλιξης του εργαζομένου, αλλά αυτός είναι ένας μύθος που επισημάνει η Microsoft (Microsoft, 2016), καθώς οι επαγγελματίες πληροφορικής που εργάζονται σε επιχειρήσεις και οργανισμούς που χρησιμοποιούν υπηρεσίες και τεχνολογίες Cloud Computing γίνονται ακόμα πιο απαραίτητοι. Η Cloud τεχνολογία επιτρέπει τη μετάβαση ορισμένων εφαρμογών στο cloud, εκτός των εγκαταστάσεων του οργανισμού, αλλά με την εξαίρεση της ενημέρωσης και της συντήρησης των διακομιστών, όλες οι υπόλοιπες εργασίες διαχείρισης των εφαρμογών παραμένουν στα χέρια του επαγγελματία πληροφορικής (IT). Η παρακολούθηση, η ενημέρωση, η ενσωμάτωση με υπηρεσίες όπως οι υπηρεσίες καταλόγου Active Directory, η ασφάλεια και η εποπτεία δικτύου είναι εργασίες που εξακολουθούν να είναι απαραίτητες για τους οργανισμούς που χρησιμοποιούν υπηρεσίες cloud. Ωστόσο, αν εκλείψει ο ρόλος του επαγγελματία πληροφορικής, αυτή η μείωση του κόστους τίθεται σε κίνδυνο. Πολλές δεξιότητες των επαγγελματιών πληροφορικής εξακολουθούν να είναι απαραίτητες όσον αφορά την ασφάλεια, τη διαχείριση του δικτύου, τις δυνατότητες ενσωμάτωσης, τις υπηρεσίες καταλόγου Active Directory και τη διαχείριση της υποδομής. Ο ρόλος του επαγγελματία πληροφορικής (IT) εξελίσσεται όσο αυξάνεται η διαθεσιμότητα υπολογιστικής ισχύος και δικτυακών χώρων αποθήκευσης – αυτό είναι αδιαμφισβήτητο, όπως μας έχει διδάξει η εξέλιξη του ρόλου του επαγγελματία πληροφορικής (IT) στο παρελθόν.

Η δυνατότητα του εκτεταμένου ελέγχου των δεδομένων του οργανισμού με την χρήση Cloud Computing, δίνει την δυνατότητα στην επικοινωνία των δεδομένων ακόμα και εάν βρίσκονται σε διαφορετικές υπηρεσίες cloud, από διαφορετικούς παρόχους ή ακόμα και στο τοπικό εταιρικό δίκτυο, ενώ παράλληλα παραμένουν προσβάσιμα (τα δεδομένα) στις εφαρμογές Cloud. Οι καλύτερες λύσεις cloud αποτελούνται από συνδυασμούς υπηρεσιών εντός και εκτός των εγκαταστάσεων του οργανισμού.

9. Ασφάλεια

Με όλες αυτές τις συσκευές να συνδέονται στο διαδίκτυο, το οποίο φιλοξενεί μεγάλους κινδύνους και τρωτά σημεία που θα μπορούσαν να καταστήσουν οποιαδήποτε συσκευή προσβάσιμη σε έναν κακόβουλο χρήστη καταγράφεται έντονη η ανάγκη για άμεση, αποτελεσματική και ευκρινή καταγραφή και αναπαράσταση των δεδομένων που παράγονται, μεταφέρονται και μεταδίδονται από κόμβο σε κόμβο.

Η ασφάλεια είναι απαραίτητη συνιστώσα στη διάδοση των τεχνολογιών και εφαρμογών IoT. Γι' αυτό το λόγο, τα «πράγματα» θα πρέπει να είναι σε θέση να επιβάλουν την δική τους ασφάλεια όσον αφορά για τις εφαρμογές που υποστηρίζουν, την πρόσβαση στο δίκτυο, τις συσκευές και την χρήση από τους ιδιώτες.

Σύμφωνα με τη θεωρία ένα ασφαλές δίκτυο παρέχει τα εξής χαρακτηριστικά :

1) Πιστοποίηση (Authentication)
2) Ακεραιότητα (Integrity)
3) Εμπιστευτικότητα (Confidentiality)
4) Κρυπτογράφηση (Encryption)

Η ακεραιότητα, η εμπιστευτικότητα, η κρυπτογράφηση και σε ορισμένες περιπτώσεις η πιστοποίηση, μπορούν να διασφαλιστούν με τη διαδικασία της κρυπτογράφησης στα πακέτα και τα σήματα που ανταλλάσσονται στο δίκτυο.

9.1 ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Σε μια μελέτη της HR Enterprise Security φαίνεται ότι το 80% των συσκευών παρουσιάζουν ανησυχία της ιδιωτικότητας (privacy) όταν συνδέονται σε cloud services ή μεταφέρουν προσωπικές πληροφορίες, οι οποίες δεν έχουν κρυπτογραφηθεί. Οι πληροφορίες που παρέχονται από τις συσκευές συγκεντρώνονται και χρησιμοποιούνται μαζί με τις υπόλοιπες πληροφορίες σε ένα κοινό web server. Το γεγονός αυτό σημαίνει ότι οι συσκευές μπορούν να συνδέονται με μια μοναδική ταυτότητα μέσω της διευθυνσιοδότησης, η οποία δημιουργεί την ανάγκη για προστασία των προσωπικών δεδομένων και ασφαλή ανταλλαγή πληροφοριών.

Επίσης, το 90% των συσκευών συλλέγουν προσωπικές πληροφορίες, το 80% δεν έχουν κωδικούς πρόσβασης οπότε θίγεται η αυθεντικότητα τους και το 60% με 70% των

συσκευών δεν έχουν την δυνατότητα κρυπτογράφησης και προστασίας κατεβάζοντας τις σχετικές ενημερώσεις.

***9.1.1** Πεδία Ασφάλειας στο IoT*
Πηγή: HP Enterprise Security, Internet of Things Research Study 2014 ISSA: October 2014 • The Internet of Things (IoT)

Συνοψίζοντας, τα θέματα που θεωρούνται ότι χρήζουν περαιτέρω λήψη μέτρων για την ασφάλεια των διασυνδεδεμένων «πραγμάτων» είναι:

- ✓ οι κόμβοι που δεν τους παρέχεται επίβλεψη
- ✓ μέτρα για την αποφυγή φυσικής επίθεσης
- ✓ μέτρα στην ασύρματη δικτύωση που επιτρέπει την εύκολη παρακολούθηση/ καταγραφή/ αλλοίωση δεδομένων
- ✓ λεπτομερής παρακολούθηση των πόρων των κόμβων με περιορισμένες δυνατότητες, που δεν επιτρέπουν δηλαδή τη λειτουργία πολύπλοκων δομών άμυνας και προστασίας
- ✓ τα σημεία όπου υπάρχει μη αξιόπιστος τρόπος επικοινωνίας (ασύρματη εκπομπή)

- **Προκλήσεις ασφάλειας στο IoT.**
  Οι βασικές προκλήσεις ασφάλειας που αντιμετωπίζει το IoT θα λέγαμε ότι πρέπει:

A. Να παρέχει αντοχή σε επιθέσεις, καθώς θα πρέπει να αποφεύγονται τα μοναδικά σημεία αστοχίας, ενώ το δίκτυο θα πρέπει να μπορεί να ανακάμψει μετά από μια επίθεση.

B. Να παρέχει αυθεντικοποίηση των συμμετεχόντων πραγμάτων
C. Να παρέχει κατάλληλη εξουσιοδότηση, ώστε ο έλεγχος πρόσβασης να επιτρέπει ή όχι την πρόσβαση στη βάση των δικαιωμάτων κάθε συμμετέχουσας συσκευής
D. Να διασφαλίζει την ιδιωτικότητα, καθώς το IoT υπάρχει παντού.

Ορισμένοι τομείς της ασφάλειας που θα πρέπει να επικεντρώσουν την προσοχή τους οι χρήστες του IoT είναι ευπάθεια στην επίθεση, κλωνοποίηση ετικετών και κλοπή ταυτότητας, δικαιώματα πρόσβασης σε δεδομένα, ποιότητα και ακεραιότητα, δέσμευση και διατήρηση των προσωπικών στοιχείων.

- **Τρόποι επίθεσης και τεχνικές αντιμετώπισης στο IoT.**
  Υπάρχουν διάφοροι τρόποι επίθεσης στη λειτουργία του δικτύου πραγμάτων:

A. με καταστροφή κόμβων.
B. με εξασθένιση ή καταστροφή της μετάδοσης π.χ χρησιμοποιώντας σήματα παρεμβολής.
C. με επιθέσεις άρνησης παροχής υπηρεσιών

Πιο αναλυτικά, με καταστροφή των κόμβων μπορούν να υποκλαπούν, να αντιγραφούν ή να τροποποιηθούν τα δεδομένα. Τα κρίσιμα σημεία για την υποκλοπή είναι τα σημεία διαχείρισης και συγκέντρωσης του δικτύου. Η εφαρμογή μεθόδων κρυπτογράφησης των δεδομένων μπορεί να προσφέρει την άμυνα έναντι της υποκλοπής. Επίσης, η μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο πραγμάτων πραγματοποιείται συνήθως κακόβουλα, με την πρόθεση αντιγραφής, τροποποίησης ή καταστροφής δεδομένων. Η πλέον απλή μέθοδος προστασίας στην περίπτωση αυτή είναι οι έλεγχοι συνθηματικού.

Τέλος, οι αδυναμίες ενός δικτύου πραγμάτων δρουν ως πύλες για την εκδήλωση κακόβουλων επιθέσεων. Οι επιθέσεις αυτές μπορούν να πάρουν τις εξής μορφές: α) *επιθέσεις δρομολόγησης* όπου λόγω του σχεδιασμού του διαδικτύου δεν υπάρχει τρόπος επαλήθευσης, επομένως κάθε δρομολογητής μπορεί να αυτοπαρουσιάζεται ως η βέλτιστη επιλογή για δρομολόγηση της κίνησης και β) *επιθέσεις άρνησης παροχής υπηρεσίας* με την οποία προκαλείται διατάραξη του δικτύου μέσα από τον κατακλυσμό του από τεχνητά μηνύματα, που το υπερφορτώνουν και παρεμποδίζουν ή περιορίζουν τη θεμιτή πρόσβαση σε αυτό.

- **Οι τεχνικές που απαιτούνται:**
  A. σύστημα επιβολής πολιτικής ασφάλειας
  B. συστήματα διαχείρισης ταυτότητας και των δικαιωμάτων
  C. κρυπτογράφηση των δεδομένων

Για να αντιμετωπιστούν τα παραπάνω θα πρέπει να αναπτυχθεί η ανθεκτικότητα του δικτύου. Μια από τις μεγαλύτερες προκλήσεις στη σύνδεση συστημάτων και αισθητήρων είναι η ασφάλεια και η προστασία της ιδιωτικότητας. Κάθε φορά που κάποιο «πράγμα» συνδέεται με το παγκόσμιο διαδίκτυο και με άλλα «πράγματα», νέα προβλήματα ασφάλειας προκύπτουν ως προς την εμπιστευτικότητα, την αυθεντικότητα και την ακεραιότητα των δεδομένων που ανιχνεύονται και ανταλλάσσονται από αυτά. Όσον αφορά την επικοινωνία μεταξύ των «πραγμάτων», έρευνες σε πρωτόκολλα δίνουν λύσεις στην ακεραιότητα, την αυθεντικότητα και το απόρρητο των συσκευών. Τέτοια πρωτόκολλα είναι το TLS ή το DTLS καθώς και το IPv6 με το IPsec.

- **Τρόπος λειτουργίας του TLS.**

  Το TLS είναι ένα κρυπτογραφικό πρωτόκολλο που έχει σαν στόχους την ιδιωτικότητα και την ακεραιότητα των δεδομένων κατά την επικοινωνία ανάμεσα σε μια εφαρμογή πελάτη - εξυπηρετητή. Το TLS χρησιμοποιείται ως ενδιάμεσο πρωτόκολλο μεταξύ του επιπέδου εφαρμογών και του επιπέδου μεταφοράς. Χρησιμοποιεί ασύμμετρη κρυπτογραφία για ανταλλαγή κλειδιών, συμμετρική κρυπτογραφία για ιδιωτικότητα και κώδικες επαλήθευσης αυθεντικοποίησης μηνυμάτων για επαλήθευση της ακεραιότητας των δεδομένων.

  Όταν ο πελάτης και ο εξυπηρετητής αποφασίσουν να ξεκινήσουν μια σύνδεση TLS η χειραψία ξεκινά με τον πελάτη να ζητάει μια ασφαλή σύνδεση, στέλνοντας τη λίστα κρυπταλγορίθμων που υποστηρίζει. Ο εξυπηρετητής επιλέγει από τη λίστα αυτή το ισχυρότερο που υποστηρίζει ο ίδιος και ενημερώνει τον πελάτη για την απόφαση. Ο εξυπηρετητής στέλνει την ταυτότητά του στη μορφή ενός ψηφιακού πιστοποιητικού. Το πιστοποιητικό περιέχει το όνομα του εξυπηρετητή, την αρχή πιστοποίησης και το δημόσιο κλειδί του εξυπηρετητή. Ο πελάτης επαληθεύει την εγκυρότητα του πιστοποιητικού. Προκειμένου να παραχθούν τα κλειδιά ο πελάτης κρυπτογραφεί έναν τυχαίο αριθμό με το δημόσιο κλειδί του εξυπηρετητή και στέλνει το αποτέλεσμα. Ο εξυπηρετητής είναι ο μόνος που μπορεί να αποκρυπτογραφήσει το μήνυμα, με τη βοήθεια του ιδιωτικού κλειδιού του.

***9.1.2** Πρωτόκολλο TLS*
Πηγή: https://el.wikipedia.org/wiki/TLS

- **Πρωτόκολλο IPv6.**

Το πρωτόκολλο IPv6 διευκολύνει την ασφαλή ανταλλαγή πληροφοριών μεταξύ των δικτυακών συσκευών. Ο κάθε κόμβος IPv6 υποστηρίζει δυνατότητες κρυπτογράφησης κατά τη μεταφορά δεδομένων. Ειδικότερα, η υποστήριξη του πρωτοκόλλου IPsec (IP security) είναι υποχρεωτική για κάθε κόμβο IPv6. Το IPsec είναι ένα πρωτόκολλο ανοιχτών προδιαγραφών που διασφαλίζει το απόρρητο των επικοινωνιών για την ασφάλεια ενός δικτύου. Μερικές από τις υπηρεσίες που προσφέρει είναι:

A. προστασία από την αλλοίωση των δεδομένων
B. προστασία εναντίον των επιθέσεων
C. κωδικοποίηση δεδομένων

9.2 ΑΠΕΙΛΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ IOT

Στο κόσμο του IoT παρουσιάζεται η ανάγκη βελτιστοποίησης των υπολογιστικών πόρων/ενέργειας από αισθητήρες και πράγματα με την υλοποίηση μέτρων για εξασφάλιση εμπιστευτικότητας / ακεραιότητας / διαθεσιμότητας. Διαφορετικά επίπεδα επεξεργασίας παρουσιάζουν δυσκολία στο συντονισμό εμπλεκομένων μέτρων με αποτέλεσμα την ύπαρξη τρωτών σημείων**.** Παράδειγμα: οι περισσότεροι από τους αισθητήρες δεν έχουν τη δυνατότητα να δημιουργήσουν κρυπτογραφημένη σύνδεση επειδή η χρήση των πόρων είναι υπερβολική και έχει συνέπεια στην φυσική αυτονομία της συσκευής. Μερικά από τα πιθανά προβλήματα που σχετίζονται με το IoT έχουν ως ακολούθως:

- **Γενικά (εικονικές και φυσικές απειλές)**

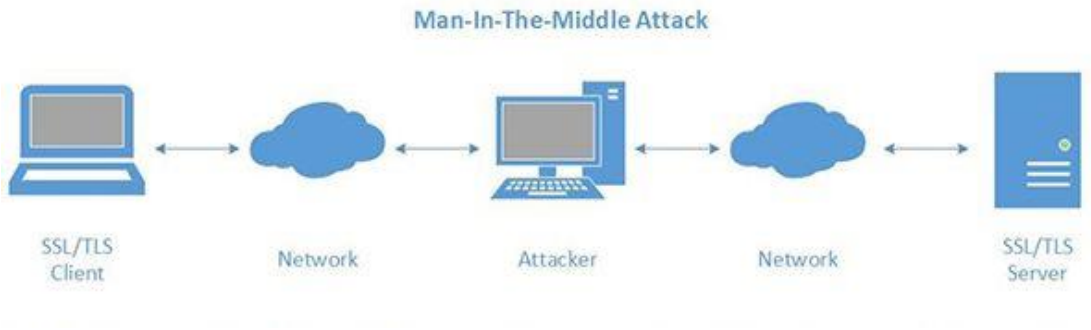
  Σε ένα IoT τα θέματα ασφάλειας εστιάζονται στις εικονικές και στις φυσικές απειλές οι οποίες συνοψίζονται στους παρακάτω πίνακες. Οι φυσικές απειλές αυξάνονται όσο περισσότερα «πράγματα» συνδέονται στο δίκτυο. Οι εικονικές απειλές είναι παρόμοιες με τις απειλές σε οποιοδήποτε άλλο IT-περιβάλλον. Η ανάλυση γίνεται σε τρία σημεία ενός IoT, στον τρόπο συνδεσιμότητας των «πραγμάτων», στα ίδια τα «πράγματα» και στην πύλη (gateway) – το κεντρικό σημείο συλλογής δεδομένων από διάφορους αισθητήρες που θεωρούνται ευάλωτα στις επιθέσεις.

Εικονικές απειλές που επηρεάζουν την ασφάλεια του IoT			
	Συνδεσιμότητα	**Συσκευές IoT**	**Πύλη**
Απειλές	- επιθέσεις άρνησης εξυπηρέτησης (DoS attack) - επίθεση man-in-the-middle (Man-in-the-middle attack) ***ανησυχίες σχετικά με την ιδιωτικότητα (privacy concerns)***	- εισβολή (intrusion) - εκμετάλλευση αδυναμιών (Exploitation) ***ανησυχίες σχετικά με την ιδιωτικότητα (privacy concerns)***	
Τρωτά σημεία (Vulnerabilities)	Ανεξέλεγκτη ή απροστάτευτη ροή δεδομένων	- Ανεπαρκής έλεγχος ταυτότητας ή εξουσιοδότησης - Ανασφαλείς διεπαφές χρήστη - Ανασφαλείς υπηρεσίες δικτύου - απροστάτευτα δεδομένα	
Επιπτώσεις / Συνέπειες	- σε κίνδυνο τα δεδομένα - απώλεια δεδομένων - απώλεια επικοινωνίας/σύνδεσης - αδυναμία ελέγχου της συσκευής	- σε κίνδυνο τα δεδομένα - απώλεια δεδομένων - αλλοίωση δεδομένων - απώλεια επικοινωνίας - αδυναμία ελέγχου της συσκευής	
Οι έννοιες της ασφάλειας που επηρεάζονται	- διαθεσιμότητα - εμπιστευτικότητα - ακεραιότητα - ιδιωτικότητα	- διαθεσιμότητα - εμπιστευτικότητα - ακεραιότητα - ιδιωτικότητα - αυθεντικότητα	
Αντίμετρα	κρυπτογράφηση των δεδομένων	- κρυπτογράφηση - ψηφιακή υπογραφή	

Φυσικές απειλές που επηρεάζουν την ασφάλεια του IoT			
	Συνδεσιμότητα	**Συσκευές IoT**	**Πύλη**
Απειλές	παρεμβολές (ηλεκτρομαγνητική συμβατότητα)	- απώλεια ισχύος - απώλεια δικτύου - κλοπή - τροποποίηση ή αντικατάσταση αισθητήρα/συσκευής	
Τρωτά σημεία (Vulnerabilities)	ασύρματη σύνδεση	- φυσική πρόσβαση στη συσκευή - ανεπαρκή έλεγχο ταυτότητας	
Επιπτώσεις / Συνέπειες	- απώλεια επικοινωνίας	- απώλεια επικοινωνίας - απώλεια δεδομένων - αλλοίωση δεδομένων	
Οι έννοιες της ασφάλειας που επηρεάζονται	διαθεσιμότητα	- διαθεσιμότητα - ιδιωτικότητα - ακεραιότητα - εμπιστευτικότητα	
Αντίμετρα	εναλλακτική σύνδεση δικτύου (wired network connection)	- εναλλακτική πηγή ενέργειας - εναλλακτική σύνδεση δικτύου - πιστοποίηση - μετακίνηση συσκευής σε δυπρόσιτη περιοχή δικτύου	

Όσον αφορά στην επικοινωνία σε ένα δίκτυο πραγμάτων σημαντικές απειλές κρίνονται η παρεμβολή και η υποκλοπή σήματος. Παρεμβολή συμβαίνει όταν η ροή της κυκλοφορίας των δεδομένων που προορίζονταν για τη σύνδεση, με κάποιο τρόπο διαταράσσεται ή τελείως εξαλείφεται λόγω άλλων ανεπιθύμητων ροών που καταλαμβάνουν τη φυσική σύνδεση. Ένα παράδειγμα είναι όταν εμφανίζεται μια επίθεση άρνησης υπηρεσίας η οποία μπορεί να είναι καταστροφική σε ένα περιβάλλον IoT που απαιτεί διαρκή επικοινωνία των «πραγμάτων». Παρεμβολή μπορεί επίσης να γίνει σε ένα φυσικό επίπεδο, για παράδειγμα με μπλοκάρισμα της ασύρματης επικοινωνίας μεταξύ των κόμβων.

Υποκλοπή σήματος μπορεί να γίνει σε διάφορα στάδια στην αλυσίδα της επικοινωνίας ανάλογα με το ποια συσκευή οι επιτιθέμενοι είναι σε θέση να ακούσουν, να αναμεταδώσουν κρυφά τα δεδομένα και σε ορισμένες περιπτώσεις να τροποποιήσουν την επικοινωνία μεταξύ δύο μερών. Η επίθεση αυτή του ενδιάμεσου κόμβου (Man in the middle attack) έχει ως στόχο την κλοπή ή και την αλλαγή πληροφοριών μεταξύ της επικοινωνίας. Επιτυγχάνεται με το να στείλει ο επιτιθέμενος δυο binding updates, ένα στον στόχο (π.χ πελάτη) και ένα στον server με τον όποιο επικοινωνεί.



***9.2.1** Επίθεση Ενδιάμεσου Κόμβου*
Πηγή: https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Αυτό γίνεται με τέτοιο τρόπο ώστε αλλάζει η ροή της πληροφορίας που ανταλλάσσουν μεταξύ τους με αποτέλεσμα να έχει πρόσβαση στο περιεχόμενο των μηνυμάτων τους. Σε μία IoT-συσκευή υπάρχουν κυρίως απειλές σε μορφή εισβολής ή/και εκμετάλλευσης στο εικονικό επίπεδο. Υπάρχει η δυνατότητα της εισβολής, όταν υπάρχει ανεπαρκής ή ανύπαρκτη ταυτότητα και εξουσιοδότηση για την πρόσβαση σε ένα σύστημα, συσκευή ή στα δεδομένα. Εκμετάλλευση υφίσταται το IoT-περιβάλλον κάθε φορά που ένας χρήστης έχει πρόσβαση σε ένα στοιχείο (συσκευή ή πύλη). Μπορεί να έχει τη μορφή της ανάγνωσης πληροφοριών, καταστρέφοντας τα ή παρεμβαίνοντας στην επικοινωνία. Όπως φαίνεται, οι φυσικές απειλές στα «πράγματα» επηρεάζουν σε μεγάλο βαθμό την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Η διαπραγμάτευση εμπιστοσύνης βασίζεται σε peer – to – peer αλληλεπιδράσεις και αποτελείται από επαναληπτική δημοσιοποίηση ψηφιακών πιστοποιητικών με σκοπό την επαλήθευση και την παγίωση αμοιβαίας εμπιστοσύνης. Ακεραιότητα δεδομένων περιλαμβάνει την προστασία σημαντικών δεδομένων κατά τη μετάδοση τους καθώς υπάρχει ο κίνδυνος οι hackers να χρησιμοποιούν μεθόδους παρακολούθησης. Η πύλη, ως ένα εκτεταμένο δίκτυο, περιέχει πολλούς αισθητήρες ή συσκευές που επικοινωνούν μεταξύ τους μέσω αυτής. Βασική απειλή είναι η τροποποίηση μεγάλων ποσοτήτων δεδομένων που μεταφέρονται από αυτήν.

Για τη προστασία από τις παραπάνω απειλές έχουν αναπτυχθεί δυο τρόποι σύνδεσης η end-to-end και η hop-by-hop σύνδεση. Η end – to - end επικοινωνία σημαίνει ότι μόνο τα τελευταία σημεία της σύνδεσης έχουν τη δυνατότητα να παρουσιάζουν τα δεδομένα σε μορφή απλού κειμένου ενώ τα ενδιάμεσα πράγματα φέρουν τα δεδομένα κρυπτογραφημένα. Με αυτό τον τρόπο ο εισβολέας δεν μπορεί να παραποιήσει τα μηνύματα που διαβιβάζονται στους διάφορους κόμβους. Με τη hop – by - hop προστασία τα δεδομένα που αποστέλλονται από μια συσκευή αποκρυπτογραφούνται, όταν πρόκειται για την πύλη, και στη συνέχεια κρυπτογραφούνται με τα κλειδιά της πύλης πριν από τη διαβίβαση. Με τον τρόπο αυτό μόνο η πύλη μπορεί να διαχειριστεί τα κλειδιά για αυτές τις συσκευές.

- **Μη εξουσιοδοτημένη πρόσβαση σε RFID**

Μια μη εξουσιοδοτημένη πρόσβαση σε ετικέτες που περιέχουν τα δεδομένα ταυτοποίησης είναι ένα μείζον ζήτημα του Ίντερνετ των πραγμάτων. Όχι μόνο η ετικέτα μπορεί να διαβαστεί από έναν οποιοδήποτε αναγνώστη αλλά μπορεί ακόμη και να τροποποιηθεί ή ενδεχομένως να καταστραφεί. Μερικές από τις απειλές των RFID περιλαμβάνουν κακόβουλη τροποποίηση δεδομένων, πλαστή ταυτότητα ετικέτας, απενεργοποίηση και αποκόλληση ετικέτας, παρακολούθηση, μπλοκάρισμα, παρεμβολή και πλαστή ταυτότητα αναγνώστη.

Πιο συγκεκριμένα σε μια πλαστή ταυτότητα ετικέτας ο επιτιθέμενος αποκτά τον σειριακό αριθμό της ετικέτας RFID και πιθανώς άλλα στοιχεία ασφαλείας συστήματος με σκοπό να εξαπατήσει τον αναγνώστη στο να δεχτεί μια άλλη ετικέτα RFID. Στην ουσία ο επιτιθέμενος κλωνοποιεί την ετικέτα RFID και την εισάγει στο σύστημα εξαπατώντας το. Τέτοιου είδους επιθέσεις εμφανίζονται στην εφοδιαστική αλυσίδα όπου γίνεται εφικτή η κλοπή προϊόντων με την εξαπάτηση του συστήματος. Στην παρακολούθηση τα δεδομένα που ανταλλάσσονται μεταξύ αναγνώστη και ετικέτας κατά την επικοινωνία τους υποκλέπτονται και αποκωδικοποιούνται. Ενώ για το μπλοκάρισμα μια ειδικά κατασκευασμένη ετικέτα δημιουργεί την εντύπωση στον αναγνώστη ότι πολύ μεγάλος αριθμός ετικετών διαβάζονται ταυτόχρονα οπότε ο αναγνώστης αυτο-μπλοκάρεται λόγω της σύγχυσης που δημιουργείται.

- **Παραβίαση ασφάλειας των κόμβων δικτύου αισθητήρων**

Τα ασύρματα δίκτυα αισθητήρων είναι ευάλωτα σε διάφορους τύπους επιθέσεων, μερικές από τις πιο πιθανές επιθέσεις είναι το Jamming, η αλλοίωση, το Sybil, flooding, οι οποίες συνοψίζονται παρακάτω:

A. Jamming: παρεμποδίζει το σύνολο του δικτύου παρεμβαίνοντας στις συχνότητες των κόμβων αισθητήρων.
B. Αλλοίωση είναι η μορφή της επίθεσης στην οποία τα δεδομένα μπορούν να τροποποιηθούν από τον επιτιθέμενο.
C. Sybil επίθεση: Σε μια επίθεση Sybil, ένας απλός κόμβος παρουσιάζει πολλαπλές ταυτότητες στους άλλους κόμβους στο δίκτυο.
D. Το flooding αφορά τη πλημμύρα των πακέτων σε μια δικτύωση που δημιουργεί προβλήματα στη ροή των δεδομένων. Δηλαδή, μπορεί να προκαλέσει διαταραχή στη ροή που κατεβαίνουν τα αρχεία από το δίκτυο, ροή αντίθετη της κανονικής με αποτέλεσμα την υπερχείλιση. Πρόκειται για ένα είδος επίθεσης DOS (denial of service).

Ο παρακάτω πίνακας συνοψίζει κάποιες επιθέσεις και τους μηχανισμούς που τις δέχονται στο WSN :

Επίθεση	**Μηχανισμός που δέχεται επίθεση**
Hello Flood Attack	Διαδικασία εγκατάστασης δικτύου
Denial – of- (DoS) attack	Μετάδοση δεδομένων
Selective Forwarding & Black hole attacks	Σωστή διαβίβαση των δεδομένων στο σταθμό βάσης
Wormhole attacks	Πρωτόκολλα δρομολόγησης
Sinkhole attacks	Πρωτόκολλα δρομολόγησης
Sybil attacks	Πρωτόκολλα συνάθροισης δεδομένων & δρομολόγησης

Για τις παραπάνω απειλές τα ασύρματα δίκτυα αισθητήρων πρέπει να διασφαλίζουν, τη βιωσιμότητα των υπηρεσιών του δικτύου, παρά την άρνηση των επιθέσεων στις υπηρεσίες (denial of service DOS) οι οποίες μπορούν να φορτωθούν σε οποιοδήποτε στρώμα των WSN. Για την διασφάλιση της διαθεσιμότητας της προστασίας μηνυμάτων, το ασύρματο δίκτυο αισθητήρων πρέπει να προστατεύει τις πηγές του. Η αυθεντικότητα πληροφορίας, επιτρέπει στον δέκτη, να επιβεβαιώσει ότι η πληροφορία, στάλθηκε από τον ισχυρίζονται αποστολέα. Ένα εμπιστευτικό μήνυμα αντιστέκεται στην αποκάλυψη της σημασίας του σε έναν εισβολέα. Ακόμη και οι απ' ευθείας πληροφορίες στα WSN, χρειάζονται να παραμένουν εμπιστευτικές, αφού μπορεί να έχουν χρησιμοποιηθεί, σε μία DOS απειλή. Η λύση είναι να κωδικοποιηθεί η πληροφορία, με ένα μυστικό κλειδί το οποίο θα έχουν στην κατοχή τους, μόνο οι δέκτες, ώστε να επιτευχθεί η εμπιστευτικότητα. Για να κατανοήσουμε το πρόβλημα που δημιουργεί η παραβίαση ασφάλειας σε ένα ευφυές δίκτυο όπως του σπιτιού παρατίθεται ένα παράδειγμα.

Παράδειγμα: *Απειλή στο ευφυές σπίτι.*

Τα ευφυή συστήματα επιτρέπουν να ανιχνευτεί τι κάνουν τα μέλη ενός νοικοκυριού στον ιδιωτικό χώρο του σπιτιού αναλύοντας έτσι λεπτομερώς τα χαρακτηριστικά όλων των ατόμων με βάση τις οικιακές τους δραστηριότητες. Με λίγα λόγια, μπορούν να συναχθούν πολλές πληροφορίες σχετικά με τη χρήση συγκεκριμένων αγαθών ή εξοπλισμού από τον καταναλωτή, τις καθημερινές συνήθειες, τις συνθήκες διαβίωσης, τις δραστηριότητες, τον τρόπο ζωής και τη συμπεριφορά του.

- **Κατάχρηση του Cloud Computing**

  Το Cloud Computing, όπως είναι γνωστό, επιτρέπει την κατανομή των πόρων μεταξύ των servers. Οι πόροι μπορούν να υποστούν πολλές απειλές για την ασφάλεια τους σύμφωνα με την Cloud Security Alliance (CSA), όπως η Man-in-the-middle επίθεση (MITM), δηλαδή η υποκλοπή/τροποποίηση μηνυμάτων (δεδομένων) από την πρόσβαση μη εξουσιοδοτημένου ατόμου.

9.3 ΑΣΦΑΛΕΙΑ ΣΥΣΚΕΥΩΝ

Η ασφάλεια των συσκευών στο Ίντερνετ των πραγμάτων πρέπει να παρέχεται σε όλη τη διάρκεια του κύκλου ζωής της συσκευής και αφορά:

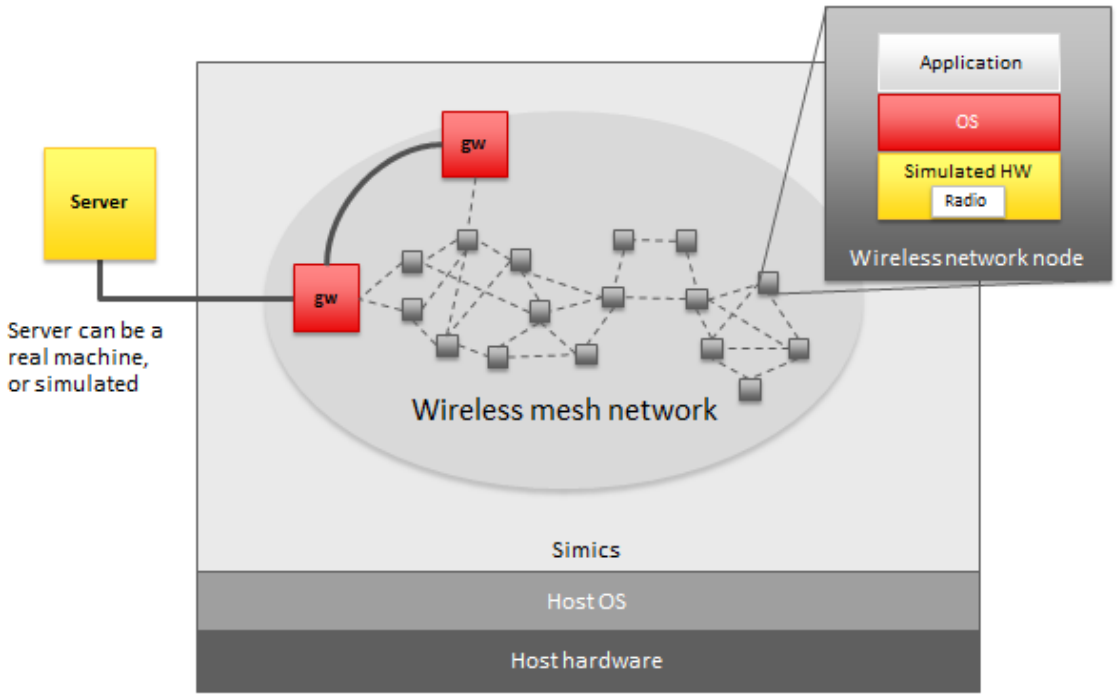
1. Ασφαλής εκκίνηση: Κάθε φορά που η συσκευή συνδέεται θα πρέπει να διασφαλίζεται η αυθεντικότητα και η ακεραιότητα του λογισμικού της με τη χρησιμοποίηση ψηφιακών υπογραφών.
2. Πρόσβαση: Απαραίτητη είναι η πρόσβαση στη συσκευή μόνο των πόρων που χρειάζονται για να κάνουν τη δουλειά τους παρέχοντας διαπιστευτήρια ότι η πρόσβαση θα είναι η ελάχιστη που απαιτείται για να εκτελεστεί μια λειτουργία, προκειμένου να ελαχιστοποιηθεί η παραβίαση της ασφάλειας.
3. Ταυτότητας συσκευής: Όταν η συσκευή είναι συνδεδεμένη στο δίκτυο, θα πρέπει να πιστοποιείται πριν από τη λήψη ή τη μετάδοση δεδομένων.
4. Firewalls και IPS: Η συσκευή χρειάζεται επίσης ένα τείχος προστασίας και το δικό του πρωτόκολλο επικοινωνίας με άλλες συσκευές.
5. Ενημερώσεις: οι συσκευές θα πρέπει να είναι σε θέση να κάνουν ενημερώσεις

10. Εργαλεία Προσομοίωσης

Εκτός από την δημιουργία των περίπλοκων συστημάτων και εφαρμογών για το Internet of Things, εξίσου περίπλοκο είναι και η δοκιμή, ενός project που η φυσική του έκταση μπορεί να είναι αρκετά μεγάλη, και θα αποτελείτε από τμηματικά – πολλά μέρη. Κάτι τέτοιο είναι ακατόρθωτο να δοκιμαστεί σε εργαστήρια, αλλά όχι και τόσο να δοκιμαστεί σε ένα εργαλείο προσομοίωσης.

Τα συστήματα που κατασκευάζονται για το IOT συνήθως είναι βασισμένα σε ένα δίκτυο τύπου *Mesh*, με *gateway nodes* και τον *Server*. Το δίκτυο Mesh, αποτελείτε από IOT-Enabled συσκευές οι οποίες είναι συνδεδεμένες στα **gateways**, τα οποία έχουν την δυνατότητα να συνδέσουν αυτές τις συσκευές στο διαδίκτυο, μεταξύ τους και αποτελείτε ένα τοίχος προστασίας για την προστασία του Mesh δικτύου από τον «έξω κόσμο». Επιπλέων, τα **gateways** συλλέγουν τις πληροφορίες από τις συσκευές, και τις προωθεί στον κεντρικό server για την επεξεργασία και αποθήκευση των πληροφοριών. Σε ένα πραγματικό παράδειγμα, αυτές οι συσκευές είναι εγκαταστημένες σε κτήρια και εργοστάσια και επικοινωνούν μεταξύ τους ασύρματα για την ανταλλαγή των δεδομένων, έτσι καθιστά κάθε ξεχωριστό κτίριο έναν παράμετρο για μελέτη σε ένα εργαστήριο από την ερευνητική ομάδα. Οι διεργασίες για την εγκατάσταση, την μεταφορά, την έρευνα και την μετεγκατάσταση των **gatewasy** καθιστά την διαδικασία χρονοβόρα και με αυξανόμενο κόστος. Αφού η εξέταση του δικτύου σε φυσικό μέρος, είναι ασύμφορη από όλες τις πλευρές, η διαδικασία της προσομοίωσης είναι μονόδρομος προς την υλοποίηση διαφορετικών υλοποιήσεων ή και σαν βοήθεια για την επιλογή αποφάσεων. Η αλλαγή παραμέτρων στο λογισμικό κομμάτι των gateways, γίνεται με την δημιουργία κώδικα, και εικονικά αναπτύσσεται και μεταδίδεται σε όλους του κόμβους μέσα από ένα script, έπειτα στην διαδικασία προσομοίωσής μπορεί να «τσεκαριστεί» η δυνατότητα της ασύρματης πρόσβασης.

Το εργαλείο που περιγράψαμε θα έχει την εξής μορφή:

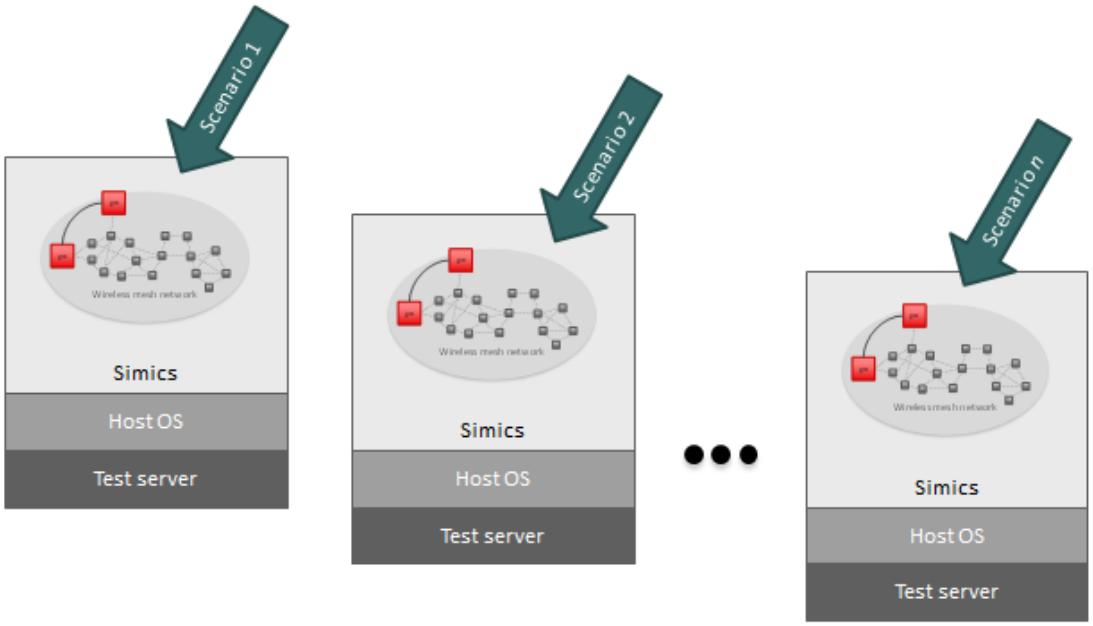


10.0.1 *Εργαλείο προσομοίωσης mesh με στοιχεία gateways.*

Κάθε κόμβος, από τα συστήματα προσομοίωσής θεωρείτε ξεχωριστή οντότητα και έχει τις τιμές: επεξεργαστεί, μνήμη, αριθμό υλικού, προσαρμογέα δικτύου, και ενδείξεις τύπου LED, και μια κάρτα συριακής μετάδοσης για την μεταφορά των δεδομένων του αισθητήρα, μέσα στο δίκτυο. Σημαντικό είναι να το τονίσουμε, ότι με τα τελευταία εργαλεία προσομοίωσής, το κάθε αντικείμενο τρέχει το ίδιο embedded OS και τις εφαρμογές αυτού, που είναι εγκαταστημένο στο φυσικό αντικείμενο/ σένσορα. Έτσι δίνεται η δυνατότητα να ελεγχθεί ολοκληρωτικά ένα IOT System καθώς και ενδοεταιρικούς αλγορίθμους που προέρχονται από το Mesh δίκτυο. Με ολόκληρο το δίκτυο ενθυλακωμένο στο πρόγραμμα προσομοίωσης, υπάρχει η δυνατότητα παράλληλων και ταυτόχρονων δοκιμών, ενώ η χρήση μιας συστοιχίας από servers μας επιτρέπει την δοκιμή, πολλαπλών εικονικών IOT

δικτύων με ανεξάρτητους παραμέτρους και σενάριο λειτουργείας.

***10.0.2** Διαφορά προσομοιωσης χωρις Hypersimulation, και με Hypersimulation*



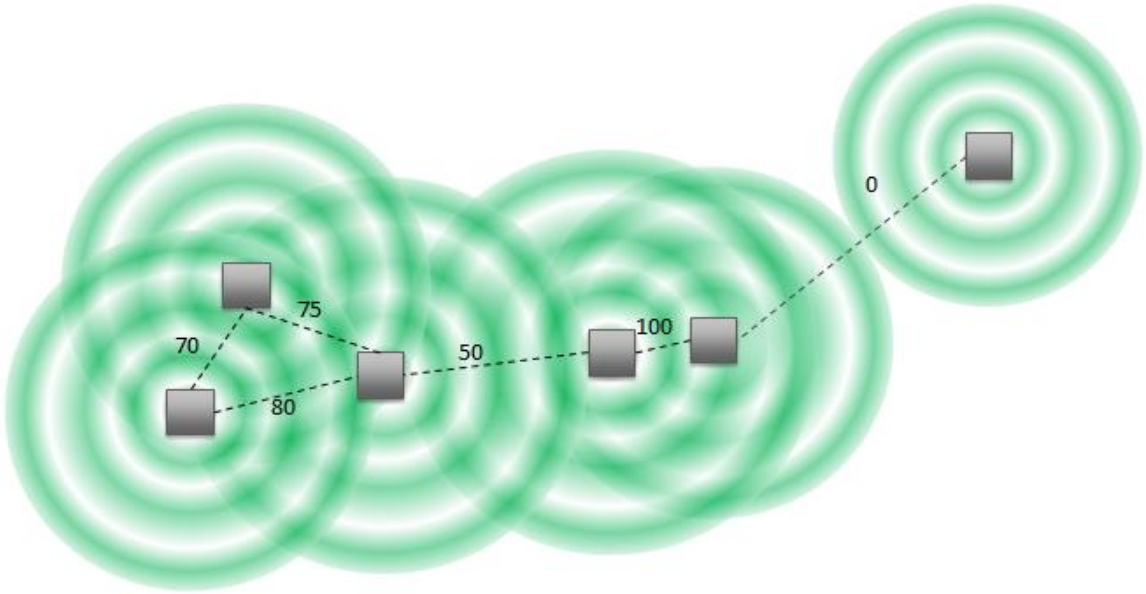
***10.0.3** Απεικόνιση διαφορετικών εκδοχών του συστήματος,*
με μορφή 'σεναρίων' για την διόρθωση προβλημάτων.

Εάν βρεθούν λάθη στις διαφορετικές εκδοχές του συστήματος, μπορούν να καταγραφούν, και να αναδιαταχθούν από τους developers του συστήματος. Το πλεονέκτημα είναι, ότι η διαδικασία τις αναδιάταξής ισχύει είτε για έναν μόνο μηχάνημα στο σύστημα ή για όλο το σύστημα καθ' αυτού. Πολλοί IT Managers, ταλαντεύονται σχετικά με την επιτυχία της παραπάνω αναφερόμενης λειτουργείας προσομοίωσης, σχετικά με την αποτελεσματικότητα και στην κατανάλωση χρόνου. Όσο στην αποτελεσματικότητα πολλά παραδείγματα έχουν εξακριβώσει την ορθή λειτουργεία και του ορθού αποτελέσματος από αυτήν, με τη χρήση εργαλείων προσομοίωσης IOT συστημάτων. Σχετικά με τον χρόνο, οι IOT κόμβοι στο Mesh δίκτυο, λειτουργούν με περιορισμένους κύκλους λειτουργείας καθώς και με περιορισμένες εντολές λειτουργικότητας, με αποτέλεσμα η διόρθωση λαθών γίνεται αρκετά γρήγορα λόγο αυτής της ιδιαιτερότητας. Κάθε καταγραφή που γίνεται από τον κόμβο, χρονομετρείτε σε δευτερόλεπτα, ενώ μπορεί να παραμένει ανενεργό για λεπτά ή και ώρες για θέματα εξοικονόμησης ενέργειας. Τα πλεονεκτήματα με τα εργαλεία προσομοίωσής, αυτού οι χρόνοι μπορούν να παραβληθούν για να επιταχύνουν την προσομοίωση με την τεχνική του idle-loop optimization & hypersimulation.

Η δυνατότητα του Hypersimulation καθιστά δυνατό να κλιμακώσει τους κόμβους, τα gateways και/ή τους servers για να πετύχει ταχύτερους χρόνους λειτουργικότητας ακόμα

και από την real time εκδοχή του συστήματος με συνέπεια ο διαχειριστής της προσομοίωσης μπορεί να ορίσει αυτοματοποιημένα τεστ μεγάλης διάρκειας.

Επιπλέον, με τα εργαλεία προσομοίωσης υπάρχει η δυνατότητα ρύθμισης της **δυνατότητας ισχύος, έ**να ακόμα πλεονέκτημα των εργαλείων αυτών, καθώς η ρύθμισης συχνότητας και ισχύος για τα ασύρματα δίκτυα είναι αρκετά προκλητική. Με την αφαίρεση λαθών στο θέμα τις συχνότητας, το ασύρματο δίκτυο παραμετροποιείται για μια πιο ορθή ενεργειακή λειτουργία και με την πρόσθεση λαθών για ερευνητικούς σκοπούς, δίνονται επιπλέων εκδοχές για τυχαίες λύσεις από την παρεμβολή ενέργειας.



10.0.4 *Παράδειγμα Παραμετροποίησης Δυνατότητας Ισχύος*

Στην παραπάνω εικόνα δίνεται ένα παράδειγμα παραμετροποίησης **δυνατότητας ισχύος**, καθώς οι κόμβοι σε κοντινή απόσταση μπορεί να μειωθεί η ισχύος που εκπέμπουν, ενώ οι πιο μακρινοί κόμβοι μπορούν να μεγαλώσουν την ισχύς για την ποιοτικότερη μετάδοση του σήματος. Οι αλλαγές μπορούν να γίνουν σε πραγματικό χρόνο προσομοίωσής.

Τέλος, τα εργαστήρια ελέγχου είναι σημαντικά και πρέπει να υπάρχουν για δοκιμές σε παραμέτρους που δεν μπορούν να υπολογιστούν από ένα εργαλείο προσομοίωσης όπως η συμπεριφορά των ραδιοσυχνοτήτων, καθώς και την αλληλοεπίδραση τους με τον φυσικό κόσμο.

Παρακάτω δίνεται μια λίστα εργαλείων για προσομοίωση σε IOT περιβάλλον τόσο δικτύων όσο cloud υπηρεσιών και εφαρμογών (IASS Company,2014).

10.1 ΛΙΣΤΑ ΕΡΓΑΛΕΙΩΝ

1. **Cooja Simulation**
2. **Omnet**
3. **NS2**
4. **Qulnet**
5. **NetSim**
6. **Simplelo Simulator**
7. **Xively**
8. **ThingSpeak**
9. **MatLAB**
10. **Atomiton**
11. **Mnubo**
12. **Oracle's Simulation Tool**
13. **Swarm**
14. **Axeda**
15. **Open Remote**
16. **Etherios**
17. **ioBridge**
18. **SAP IOT Solutions**
19. **Zatar**
20. **ThingWorx**
21. **Arrayent**
22. **Sine Wave**
23. **Ayla Network**
24. **Echelon**
25. **Evrythng**
26. **Exosite**
27. **Xively**
28. **Marvell**
29. **Carriots**
30. **Arkessa**
31. **GroveStreams**
32. **CeNSE by HP**
33. **ARM IOT Simulation Tool**
34. **Nimbits**
35. **Open Sen.se**
36. **Paraimpu**
37. **Sociot.at**

38. **NewAer**
39. **Yaler**
40. **Jasper**
41. **XobXob**
42. **Linkafy**
43. **Revolv**
44. **Wind River**
45. **Wovyn**
46. **Microsoft Research Lab of Things**
47. **InfoBright**
48. **Contiki**
49. **2lemetry**
50. **AllJoyn**
51. **InterDigital**
52. **Superflux**
53. **HarvestGeek**
54. **MediaTek Labs Tools**
55. **Streamlite LTE**
56. **Bosch Software Innovation Suite**
57. **Rio Tboard**

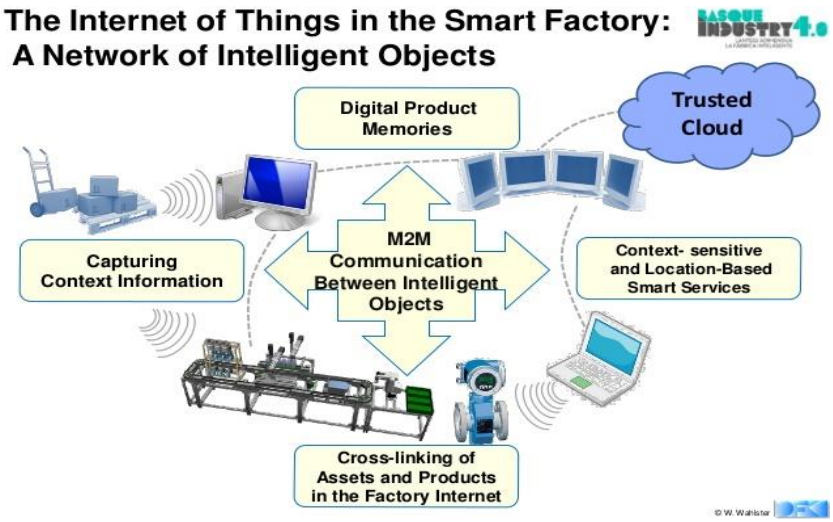
11. Πεδία Εφαρμογής

Ο συνδυασμός της τεχνολογίας IoT, με το Cloud Computing (υπηρεσίες πληροφορικής στο σύννεφο), τα Big Data (ανάλυση τεράστιων όγκων δεδομένων) και τις wearable συσκευές (ηλεκτρονικές συσκευές που φοριούνται από τους χρήστες) δημιουργούν ένα πολύ έξυπνο περιβάλλον υπερσυνδεσιμότητας που φέρνει νέες υπηρεσίες και δυνατότητες συνδυασμού με τεχνολογίες.

Ερευνώντας την εφαρμογή του IoT στο **πεδίο της αγοράς** διαπιστώνεται ότι απευθύνεται σε κάθε επιχειρηματικό κλάδο όπως βιομηχανική παραγωγή, κατασκευές, μεταφορές, διαχείριση ενέργειας, εφοδιαστική αλυσίδα κ.α.

11.1 ΒΙΟΜΗΧΑΝΙΚΗ ΠΑΡΑΓΩΓΗ

Συγκεκριμένα, το διαδίκτυο πραγμάτων στη βιομηχανία παρέχει αυτόματες διαδικασίες αναγνώρισης προϊόντων μέσω ετικετών ραδιοσυχνοτήτων RFID, συντήρησης των μηχανημάτων μέσω των συνδεδεμένων αισθητήρων επιτρέποντας την παρακολούθηση σε πραγματικό χρόνο, της καλής λειτουργίας και της απόδοσης του εξοπλισμού του εργοστασίου και παραγωγή προϊόντων.



11.1.1 *Το Διαδίκτυο των Πραγμάτων στην Έξυπνη Βιομηχανία*
Πηγή: http://www.slideshare.net/SPRICOMUNICA/basque-industry-40-the-fourth-industrial-revolution-based-on-smart-factories

11.2 ΑΛΥΣΙΔΕΣ ΕΦΟΔΙΑΣΜΟΥ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΠΡΟΪΟΝΤΩΝ/ ΜΕΤΑΦΟΡΕΣ

Κύριες δραστηριότητες των έξυπνων μεταφορών αποτελούν :

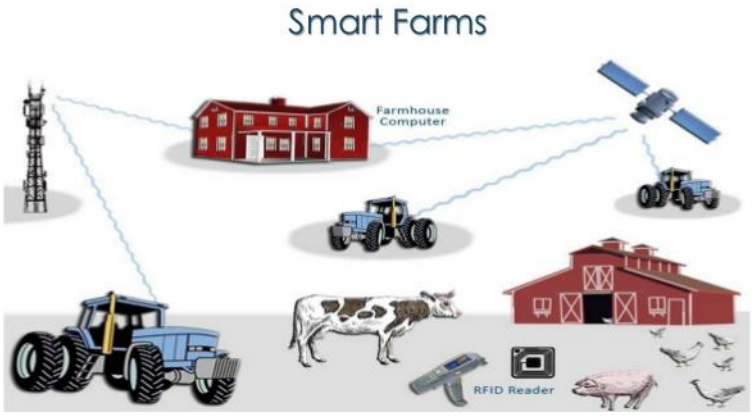
- η διαχείριση στόλου,
- η έξυπνη παρακολούθηση εμπορευμάτων,
- ο έξυπνος επιμερισμός φορτίου
- η παρακολούθηση της θερμοκρασίας και των διαφόρων συνθηκών καθώς και ο έλεγχος των διαδρομών που ακολουθούν ευαίσθητα προϊόντα

Επίσης, το IoT επιφέρει θετικές αλλαγές στην αλυσίδα εφοδιασμού μέσω της :

- διαχείρισης απογραφής εμπορευμάτων
- διαχείρισης αποθήκης
- ολοκλήρωσης κύκλου ζωής προϊόντος

11.3 ΓΕΩΡΓΊΑ

Στο τομέα της κτηνοτροφίας το IoT χρησιμεύει στην παρακολούθηση της αλυσίδας προσφοράς τροφίμων, στην παρακολούθηση των ζώων, στην φυτοπροστασία με σκοπό τον έλεγχο των συνθηκών των φυτών προκειμένου να παρθεί η μέγιστη απόδοση καλλιεργειών καθώς και την παρακολούθηση της φάρμας των ζώων για να διασφαλιστεί η επιβίωση και η υγεία των ζώων.



***11.3.1** Έξυπνη φάρμα*
Πηγή: http://www.slideshare.net/AnkurPipara/internet-of-things-iot-2014

- **Έξυπνο σύστημα άρδευσης.**

Το έξυπνο σύστημα άρδευσης λαμβάνει υπόψιν του την υγρασία του εδάφους ή τις μετεωρολογικές προγνώσεις ώστε να ενημερώνει τον γεωργό σε καθημερινή βάση για τη συχνότητα του ποτίσματος. Ένα βασικό εξάρτημα του συστήματος, από άποψη hardware, είναι οι μετρητές υγρασίας, οι οποίοι τοποθετούνται διάσπαρτα στο χωράφι και σε διάφορα βάθη από το έδαφος.

Οι μετρητές συνδέονται ανά ομάδες μέσω καλωδίων με κεραίες, οι οποίες μεταδίδουν τα δεδομένα ασύρματα σ' έναν server. Εκεί το αντίστοιχο λογισμικό επεξεργάζεται τις μετρήσεις για την υγρασία στο έδαφος συνδυάζοντάς τις με τις πληροφορίες για τις καιρικές συνθήκες που θα επικρατήσουν στο χωράφι τις επόμενες ώρες. Το λογισμικό συμβουλεύεται επίσης ένα ηλεκτρονικό αρχείο που περιέχει στοιχεία για τη συγκεκριμένη καλλιέργεια όπου είναι εγκατεστημένο το σύστημα. Τα στοιχεία αυτά έχουν να κάνουν με το πόσο νερό χρειάζεται η εν λόγω καλλιέργεια στις διάφορες φάσεις ανάπτυξής της, αφού οι ανάγκες σε άρδευση μεταβάλλονται ανάλογα με την ηλικία των φυτών. Απ' όλες αυτές τις παραμέτρους, οι αλγόριθμοι μπορούν να συμπεράνουν αν το χωράφι χρειάζεται ή όχι πότισμα και πόσο, εμφανίζοντας τις σχετικές πληροφορίες στον υπολογιστή ή το τηλέφωνο του γεωργού.

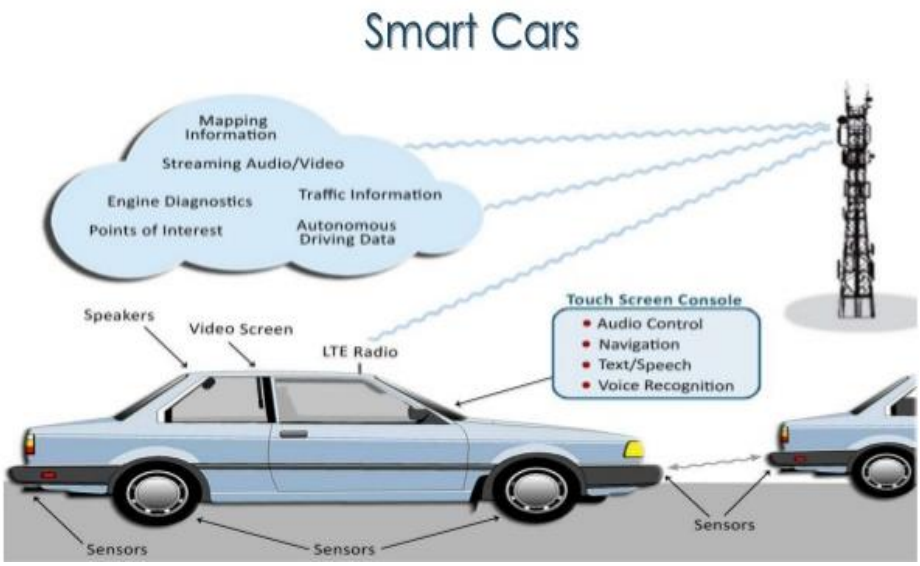
- **Το Internet of Things στο αμπέλι**

Το έξυπνο σύστημα καταγράφει τα θρεπτικά συστατικά του χώματος, την υγρασία και τη θερμοκρασία εδάφους και αέρα, την ένταση των ανέμων, την ώρα και την ένταση της ηλιοφάνειας και μεταδίδει τα δεδομένα στο Cloud. Μέσω ειδικής εφαρμογής ο καλλιεργητής παρακολουθεί τα πάντα στην οθόνη του κινητού του.

11.4 ΑΥΤΟΚΙΝΗΤΟΒΙΟΜΗΧΑΝΙΑ

Ο στόχος του έξυπνου αυτοκινήτου είναι η σύνδεση του αυτοκινήτου στο σύστημα IoT, και ο διαμοιρασμός δεδομένων και πληροφοριών μεταξύ των συσκευών, με στόχο την δημιουργία καλύτερων εμπειριών για τους χρήστες, είτε βρίσκονται στον δρόμο, είτε στο σπίτι τους. Παράδειγμα, η εταιρεία κατασκευής ελαστικών Continental δημιούργησε μια σειρά αισθητήρων που θα βρίσκονται ενσωματωμένοι στα ελαστικά του αυτοκινήτου και θα ελέγχουν την πίεση του αέρα, το φορτίο και την κατάσταση του ελαστικού πέλματος. Το «έξυπνο» αυτό σύστημα παρακολουθεί τις αλλαγές στην κατάσταση των ελαστικών με το πέρασμα του χρόνου και έχει τη δυνατότητα να ειδοποιεί τον οδηγό όταν τα λάστιχα χρειάζονται αντικατάσταση. Σημαντική διευκόλυνση κάθε οδηγού και κυρίως στις μεγάλες πόλεις αποτελεί ο αισθητήρας στάθμευσης ο οποίος είναι τοποθετημένος στο οδόστρωμα και προειδοποιεί τον οδηγό αν η θέση parking είναι ελεύθερη. Επιπρόσθετα, αισθητήρες στο μπροστινό και στο πίσω μέρος του αυτοκινήτου βοηθούν στη συνεργασία οχήματος με

όχημα ώστε να κρατιούνται οι κατάλληλες αποστάσεις. Τέλος οδικές υπηρεσίες πληροφοριών μπορούν να παρέχονται.



***11.4.1** Έξυπνο αυτοκίνητο*
Πηγή: http://www.slideshare.net/AnkurPipara/internet-of-things-iot-2014

11.5 ΒΕΛΤΙΩΣΗ ΣΤΟ ΟΔΙΚΟ & ΣΙΔΗΡΟΔΡΟΜΙΚΟ ΔΙΚΤΥΟ, ΔΙΚΤΥΟ ΥΔΡΕΥΣΗΣ ΚΑΙ ΗΛΕΚΤΡΟΔΟΤΗΣΗΣ

Στην περίπτωση του οδικού δικτύου το IoT μέσω της τεχνολογίας RFID θα ενημερώνει συνεχώς τον οδηγό για διάφορα θέματα με πιο σημαντικά την επιπλέον απόσταση που έχει διανύσει μέχρι τον προορισμό του, τους σταθμούς διοδίων, για τα σημεία στα οποία έχουν συμβεί ατυχήματα, για το πιο κοντινό πρατήριο καυσίμων, ακόμα και για κλειστούς δρόμους λόγω εργασιών. Στον τομέα της παραγωγής ενέργειας, το IoT μπορεί να χρησιμοποιηθεί για την παρακολούθηση της μονάδας, των κατανεμημένων σταθμών ηλεκτροπαραγωγής, της περιοχής των σταθμών παραγωγής, των ρύπων και των εκπομπών αερίων και της ενεργειακής κατανάλωσης.

11.6 Ο ΤΟΜΕΑΣ ΤΗΣ ΕΞΥΠΝΗΣ ΕΝΕΡΓΕΙΑΣ (SMARTGRIDS)

Περιλαμβάνει τα έξυπνα δίκτυα, τους έξυπνους μετρητές, το έξυπνο νερό, αλλά και την έξυπνη διαχείριση σκουπιδιών. Η αποκομιδή των απορριμμάτων αποτελεί ένα διαχρονικό πρόβλημα στα μεγάλα αστικά κέντρα, ιδιαίτερα σε περιοχές με πολύ πυκνό πληθυσμό. Σε μία έξυπνη πόλη, οι κάδοι έχουν ενσωματωμένους αισθητήρες, ώστε να ειδοποιούνται αυτόματα οι αρμόδιοι φορείς όταν υπάρχει ανάγκη. Τα ευφυή συστήματα μέτρησης συλλέγουν και μεταφέρουν δεδομένα μέσω επικοινωνίας μεταξύ του μετρητή και των προμηθευτών ενέργειας, των διαχειριστών δικτύων και τρίτων. Αυτό το ευφυές δίκτυο είναι ένα δισδιάστατο δίκτυο παροχής ηλεκτρικής ενέργειας που συνδυάζει πληροφορίες από χρήστες του δικτύου με στόχο την αποτελεσματική και οικονομικότερη παροχή ηλεκτρικής ενέργειας. Σκοπός αποτελεί η έξυπνη παραγωγή, διανομή και χρήση της ενέργειας.

11.7 Η ΣΥΜΒΟΛΗ ΤΟΥ ΙΟΤ ΣΤΗΝ ΠΕΡΙΒΑΛΛΟΝΤΙΚΗ ΠΡΟΣΤΑΣΙΑ

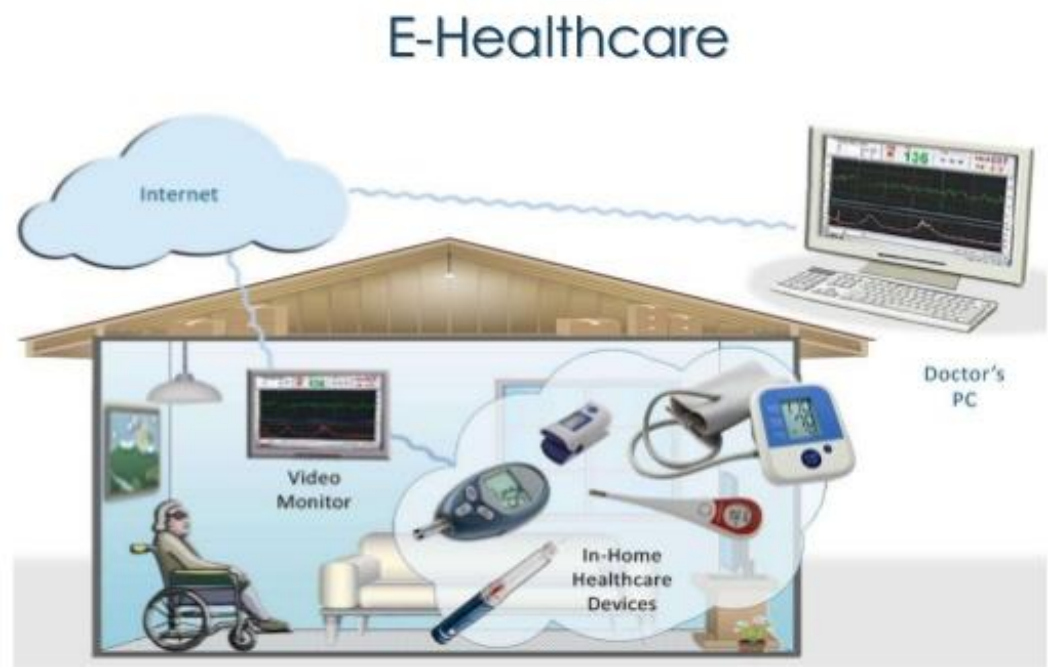
Με τη συλλογή και αξιοποίηση των πληροφοριών από :

- μετεωρολογικό έλεγχο
- ανίχνευση ακτινοβολίας
- έλεγχος των κυμάτων και των ακτών
- παρακολούθηση του επιπέδου των ποταμών
- έλεγχος ρύπανσης των υδάτων
- πυρανίχνευση δασικών περιοχών
- έλεγχος σε συγκεκριμένες περιοχές δονήσεων για ανίχνευση σεισμών

Με αυτό τον τρόπο μπορεί να προστατεύσει τους πολίτες, αλλά και την πολιτεία από καταστάσεις έκτακτης ανάγκης και φυσικών καταστροφών.

11.8 ΕΦΑΡΜΟΓΕΣ ΤΟΥ IOT ΣΤΟΝ ΙΑΤΡΙΚΟ ΚΛΑΔΟ ΚΑΙ ΤΗΝ ΥΓΕΙΑ

Η παρακολούθηση του ιστορικού της υγείας των ανθρώπων είναι μια άλλη πτυχή του IoT. Η τεχνολογία αισθητήρων παρέχει πληροφορίες σε πραγματικό χρόνο για ζωτικά σημεία και για άλλους δείκτες (σφυγμό, θερμοκρασία, πίεση) σχετικά με την υγεία και τη κατάσταση ενός ατόμου καθώς και την ταυτοποίηση και παρακολούθηση φαρμακευτικής αγωγής. Αυτά τα συστήματα βρίσκουν εφαρμογή στα νοσοκομεία, σε συστήματα παρακολούθησης της υγείας στο σπίτι, στα ιατρεία και στη φροντίδα ηλικιωμένων.



***11.8.1** Εφαρμογή IoT στην υγεία*
Πηγή: http://www.slideshare.net/AnkurPipara/internet-of-things-iot-2014

Με τη γένεση του Ίντερνετ των πραγμάτων δηλαδή την επέκταση ηλεκτρονικών υπηρεσιών που χρησιμοποιούνται άμεσα από τους **πολίτες** έχουν ως στόχο την βελτίωση της καθημερινότητας των ανθρώπων κάνοντας την πιο λειτουργική και αποδοτική.

11.9 ΈΞΥΠΝΕΣ ΠΟΛΕΙΣ

Οι ευφυείς πόλεις υπόσχονται μέγιστη ασφάλεια και αποτελεσματικότητα για το σύνολο των κατοίκων τους. Αισθητήρες τοποθετημένοι στα αυτοκίνητα, τα φώτα των οδικών αξόνων, ακόμα και στους κάδους απορριμμάτων συλλέγουν δεδομένα με στόχο τη μείωση του ενεργειακού κόστους και την παροχή καλύτερων υπηρεσιών σε άτομα και επιχειρήσεις. Αφορά κυρίως τη βελτίωση των πόλεων στην επίλυση προβλημάτων. Παρακάτω θα δοθούν τρία παραδείγματα ο έξυπνος φωτισμός, η έξυπνη εξυπηρέτηση ατόμων με ειδικές ανάγκες και οι έξυπνες στάσεις δείχνοντας την υψηλή σημασία της εξέλιξης και της χρήσης του IoT.

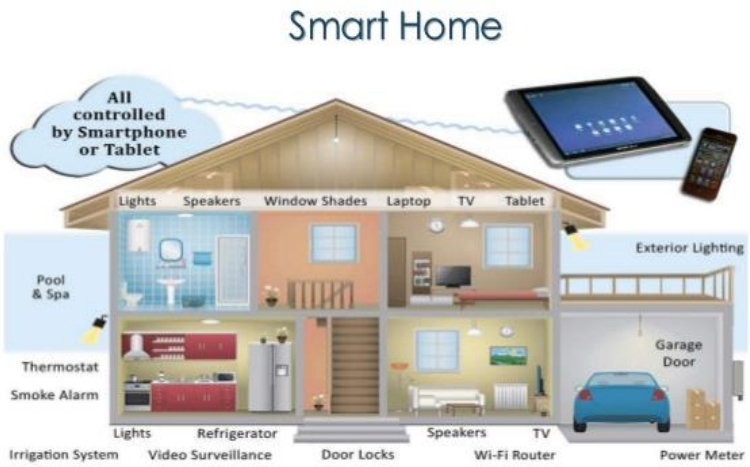
- **Έξυπνη φωταγώγηση (Smart Lighting)**
  Πρόκειται για μια λύση στην απομακρυσμένη διαχείριση δημόσιας φωταγώγησης που θα ελέγχεται από συνδυασμό δεδομένων που θα προκύπτουν από αισθητήρες φωτός, βροχής και κίνησης μέσω των οποίων θα ρυθμίζεται το άναμμα και το σβήσιμό τους. Πιθανές επιπρόσθετες δυνατότητες είναι η διαφοροποίηση λειτουργίας του συστήματος σε κατοικημένες περιοχές και σε μη κατοικημένες περιοχές, καθώς επίσης και η προσαρμοσμένη συμπεριφορά του συστήματος σε περιπτώσεις έκτακτης ανάγκης.

Επίσης, σε κάθε συσκευή θα υπάρχουν αισθητήρες φωτός, κίνησης και υγρασίας για τη ρύθμιση των λαμπτήρων, ενώ κάθε επιμέρους συσκευή θα συνδέεται, μέσω Zigbee τεχνολογίας σε ένα gateway, όπου και θα γίνεται η αποστολή των δεδομένων που θα συλλέγονται από τους αισθητήρες, προκειμένου να πραγματοποιηθεί η περαιτέρω συγκέντρωσή τους σε βάση δεδομένων, η επεξεργασία – διαχείριση και η παροχή ή η παρουσίαση τους σε κάθε φορέα, αρχή ή φυσικό πρόσωπο που το επιθυμεί.

- **Οι πόλεις με IoT εξυπηρετούν τα άτομα με ειδικές ανάγκες.**
  Επιπλέον, οι πόλεις με την τεχνολογία IoT είναι πολύ φιλικές για τα άτομα με ειδικές ανάγκες. Για παράδειγμα, τα κινητά αξιοποιώντας την **beacon technology** θα παρέχουν οδηγίες στους χρήστες που έχουν απώλεια όρασης για το πώς θα φτάσουν στον προορισμό τους.
- **Έξυπνες στάσεις.**
  Επιπρόσθετα, οι «έξυπνες» στάσεις θα παρέχουν ακριβής πληροφόρηση, με ακρίβεια δευτερολέπτου, σε ότι αφορά τα δρομολόγια.

11.10 ΟΙΚΙΑΚΟΙ ΑΥΤΟΜΑΤΙΣΜΟΙ/ΕΞΥΠΝΟ ΣΠΙΤΙ

Το έξυπνο σπίτι είναι το σύνολο των αυτοματισμών, με τους οποίους ομαδοποιούνται, οργανώνονται και αυτοματοποιούνται οι λειτουργίες μιας κατοικίας, ανάλογα με τις καθημερινές ανάγκες και συνήθειες που έχει ο εκάστοτε ιδιοκτήτης. Η δυνατότητα παρακολούθησης και διαχείρισης όλων των χώρων και εγκαταστάσεων μιας κατοικίας γίνεται με οποιοδήποτε τρόπο επικοινωνίας όπως μέσω σταθερού τηλεφώνου, κινητού τηλεφώνου ή/ και διαδικτύου.



***11.10.1** Έξυπνο σπίτι*

Πηγή: http://www.slideshare.net/AnkurPipara/internet-of-things-iot-2014

Ορισμένες από τις λειτουργίες ενός σπιτιού που μπορούν να αυτοματοποιηθούν είναι:

- Έλεγχος φωτισμού
- Κεντρικό σύστημα συναγερμού
- Κεντρικό σύστημα θέρμανσης
- Κεντρικό σύστημα διανομής εικόνας και ήχου
- Δίκτυο οικιακών συσκευών : με τη χρήση της «έξυπνης» πρίζας προσαρμόζεται και ρυθμίζεται απλά και εύκολα η λειτουργία των συσκευών. Ουσιαστικά με το πάτημα ενός κουμπιού π.χ. από το κινητό μας τηλέφωνο , μέσω Wi-Fi. μπορούμε να συνδέσουμε οτιδήποτε: από καφετιέρα, μέχρι τηλεόραση και λαμπτήρες και έτσι να ελέγχουμε πότε θα ενεργοποιηθούν ή θα απενεργοποιηθούν.
- Απομακρυσμένη παρακολούθηση κλειδαριών
- Διαχείριση ενέργειας
- Σύστημα ποτίσματος

- Έλεγχος ζεστού νερού
- Έλεγχος τροφίμων – έξυπνα ψυγεία

12. Επιχειρησιακά Οφέλη

Το IOT επηρεάζει κάθε πτυχή της ανθρώπινης ιδιαιτερότητας, σαν συνέπεια να επηρεάζει θετικά και το μέλλον των επιχειρήσεων. Τα έξυπνα κινητά τηλέφωνα και οι συσκευές του IOT θα αλλάξουν τους τύπους των συσκευών που συνδέονται στα συστήματα της εταιρείας, θα εμπλουτιστούν σε κατηγορίες και ποσότητες καθώς ανάλογα θα βελτιώνεται και η παραγωγικότητα των υπαλλήλων. Το IOT θα βοηθήσει στην απόδοση κέρδους των επιχειρήσεων, την αξιοποίηση πληροφοριών από ένα ευρύ φάσμα εξοπλισμού, τη βελτίωση της λειτουργίας και την αύξηση της ικανοποίησης των πελατών. Το IOT θα έχει επίσης μια βαθιά επίδραση στις ζωές των υπαλλήλων. Θα βελτιώσει τη δημόσια ασφάλεια, τις μεταφορές και την υγειονομική περίθαλψη, με την καλύτερη πληροφόρηση και την ταχύτερη επικοινωνία των πληροφοριών. Ενώ υπάρχουν πολλοί τρόποι που το IoT θα μπορούσε να επηρεάσει την κοινωνία και τις επιχειρήσεις, υπάρχουν τουλάχιστον τρία σημαντικά οφέλη του IOT που θα επηρεάσουν όλες τις επιχειρήσεις, τα οποία περιλαμβάνουν: την επικοινωνία, τον έλεγχο και την εξοικονόμηση κόστους.

Επικοινωνία (Communication). Το IOT μεταδίδει πληροφορίες σε ανθρώπους και συστήματα, για την σωστή λειτουργική κατάσταση του εξοπλισμού και τα δεδομένα από αισθητήρες μπορούν να παρακολουθούν και να προτείνουν την βέλτιστη χρονική σήμανση για συντήρηση και επισκευή της μηχανής. Στις περισσότερες περιπτώσεις οι επιχειρήσεις δεν έχουν πρόσβαση σε αυτές τις πληροφορίες πριν ή αυτές συλλεχθούν χειροκίνητα από το ανθρώπινο δυναμικό. Για παράδειγμα, ένα σύστημα IOT -enabled HVAC μπορεί να αναφέρει αν το φίλτρο αέρα είναι καθαρό και λειτουργεί σωστά. Σχεδόν κάθε εταιρεία έχει μια κατηγορία μηχανημάτων που θα μπορούσε να παρακολουθείτε ανά τακτά χρονικά διαστήματα. Mobile εξοπλισμός της επιχείρησης με σύστημα GPS μπορούν να ανακοινώνουν την τρέχουσα θέση και την κίνησή τους καθώς η πληροφορία της τοποθεσία είναι άκρως σημαντική αλλά είναι επίσης εφαρμόσιμη για τον εντοπισμό αντικειμένων μέσα σε μια οργάνωση και συστοιχία από άλλο τεχνικό εξοπλισμό. Στον τομέα της υγείας, το IOT μπορεί να βοηθήσει ένα νοσοκομείο να παρακολουθεί τη θέση του νοσοκομειακού εξοπλισμού, από αναπηρικά αμαξίδια μέχρι καρδιακούς απινιδωτές στους χειρούργους. Στον κλάδο των μεταφορών, μια επιχείρηση μπορεί να προσφέρει παρακολούθηση σε πραγματικό χρόνο για την κατάσταση των δεμάτων και παλετών. Για παράδειγμα, η Maersk μπορεί να χρησιμοποιεί αισθητήρες για να εντοπίσει τη θέση ενός πλοίου και το ποσοστό καυσίμου που του απομένει.

Ελέγχου και Αυτοματισμού (Control and Automation). Σε έναν συνδεδεμένο κόσμο, μια επιχείρηση θα έχει ορατότητα στην κατάσταση μιας συσκευής. Σε πολλές περιπτώσεις, μια επιχείρηση ή ένας καταναλωτής θα είναι επίσης σε θέση να ελέγχει από απόσταση μια συσκευή. Για παράδειγμα, μια επιχείρηση μπορεί να μετατρέψει εξ 'αποστάσεως ή να κλείσει ένα συγκεκριμένο κομμάτι του εξοπλισμού ή να ρυθμίσει τη θερμοκρασία σε ένα κλίματοελεγχόμενο περιβάλλον.

Η εξοικονόμηση κόστους (Cost Savings). Πολλές εταιρείες θα υιοθετήσουν το IOT για να εξοικονομήσουν χρήματα. Οι επιχειρήσεις, ιδίως των βιομηχανικών εταιριών, χάνουν χρήματα όταν αποτυγχάνει ο εξοπλισμός. Με τις νέες πληροφορίες των αισθητήρων, το IOT μπορεί να βοηθήσει μια επιχείρηση να εξοικονομήσει χρήματα από τη βλάβη του εξοπλισμού καθώς επιτρέπει στην επιχείρηση να εκτελέσει την προγραμματισμένη συντήρηση. Οι αισθητήρες μπορούν επίσης να κάνουν αποτίμηση των στοιχείων, όπως την οδηγική συμπεριφορά και την ταχύτητα, για τη μείωση των εξόδων καυσίμων και της φθοράς. Αυτά είναι μόνο μερικά παραδείγματα για το πώς μπορεί να βοηθήσει το IOT μια επιχείρηση στην εξοικονόμηση χρημάτων, την αυτοματοποίηση των διαδικασιών και την αύξηση της καλής εικόνας της επιχείρησης. Για να υπάρχουν τα οφέλη που μπορεί να προσφέρει το IOT , μια επιχείρηση θα πρέπει να καλύπτει τουλάχιστον τα ακόλουθα τέσσερα στοιχεία:

Ορίστε τι θα θέλατε να μάθετε από τους αισθητήρες. Κατά τη διάρκεια των επόμενων τριών ετών, η πλειοψηφία των συσκευών που θα αγοράζονται θα διαθέτουν αισθητήρες και πολλές συσκευές που ήδη υπάρχουν μπορούν να εξοπλιστούν με αισθητήρες. Αυτό θα παράγει ένα ευρύ φάσμα νέων πηγών δεδομένων για τους ανθρώπους και τα συστήματα θα τα χρησιμοποιούν για να βελτιώσουν τη ζωή μας και τις υφιστάμενες επιχειρηματικές διαδικασίες. Μέσα σε ένα εταιρικό περιβάλλον, πρέπει να καθορίζουν ποια είδη πληροφοριών μπορεί να που προέρχονται από αυτούς τους αισθητήρες και να συνεργαστούν με τους ηγέτες των επιχειρήσεων για να καθορίζουν τις επιχειρηματικές διαδικασίες που μπορούν να βελτιωθούν με αυτές τις νέες πληροφορίες. Για παράδειγμα, τα δεδομένα των αισθητήρων που αναδεικνύουν ανωμαλίες του εξοπλισμού, μπορεί να χρησιμοποιηθούν για να προβλεφθεί και να αποφευχθεί μία αποτυχία του εξοπλισμού.

Φτιάξτε ένα δίκτυο IOT και το θεμέλιο της ασφάλειας. Πολλές βιομηχανικές αναπτύξεις IOT έχουν χρησιμοποιήσει ιδιόκτητα δίκτυα. Αντί της οικοδόμησης ιδιόκτητων δικτύων, θα πρέπει να συνδεθούν με συσκευές IOT που βασίζονται σε πρότυπα δίκτυα IP. Ένα δίκτυο που βασίζεται σε IP θα βοηθήσει τις επιχειρήσεις να προσφέρουν τις επιδόσεις, την αξιοπιστία και της λειτουργικότητα που απαιτούνται για την υποστήριξη ενός παγκόσμιου IOT δικτύου και των συνδέσεων με άλλα οικοσυστήματα. Επιπλέον,

πολλές επιχειρήσεις επικεντρώνεται στην ανάπτυξη στρατηγικών για την ασφάλεια των smartphones και των tablets, αλλά αυτό είναι μόνο μία πτυχή της νέας κινητής τηλεφωνίας στον κόσμο. Ο πολλαπλασιασμός των συνδεδεμένων αισθητήρων και εξοπλισμού παρέχει νέες ανησυχίες για την ασφάλεια. Για αυτό θα πρέπει να βεβαιωθεί ότι έχει δημιουργήσει ασφαλιστικές δικλείδες, συμπεριλαμβανομένων των διαδικασιών ασφαλείας, όπως κρυπτογράφηση, φυσική ασφάλεια κτιρίων και του δικτύου ασφαλείας για τα δεδομένα κατά τη μεταφορά.

Συλλέξτε όσο το δυνατόν περισσότερα δεδομένα. Επιχειρήσεις που δεν προγραμματίζουν προσεκτικά για το IOT θα είναι συγκλονισμένες με τον όγκο και την ποικιλία των δεδομένων που το IOT θα δημιουργήσει. Ενώ κάθε αισθητήρας μπορεί να παράγει μόνο μία μικρή ποσότητα δεδομένων, η εταιρεία θα συλλέγει δεδομένα από χιλιάδες έως εκατομμύρια αισθητήρες. Οι επιχειρήσεις πρέπει να οικοδομήσουν μια συλλογή δεδομένων και μία στρατηγική αναλυτικών δεδομένων που υποστηρίζουν αυτό το νέο χείμαρρο πληροφοριών σε μια κλιμακούμενη και οικονομικά αποδοτική μορφή. Μεγάλες τεχνολογίες δεδομένων, όπως Hadoop και NoSQL, μπορεί να δοθεί στις εταιρίες η ικανότητα ταχείας συλλογής, αποθήκευσης και ανάλυσης μεγάλων όγκων δεδομένων. Μια εταιρεία θα πρέπει να συλλέγει όλα τα δεδομένα που είναι σχετικά με τις υφιστάμενες διαδικασίες. Αν είναι δυνατόν και οικονομικά αποδοτικό, μια εταιρεία θα πρέπει επίσης, να συλλέγει πρόσθετα στοιχεία που θα επιτρέψουν στην επιχείρηση να απαντήσει σε νέες ερωτήσεις στο μέλλον.

Εξετάστε το μέγεθος και την κλίμακα των παρόχων IOT . Το IOT είναι ένα περίπλοκο τοπίο με τις πολυάριθμες κατηγορίες και πολλούς προμηθευτές στην κάθε κατηγορία. Οι τέσσερις κύριες κατηγορίες του IOT είναι: Ο αισθητήρας (-ες) και η κεραία (ες) που συχνά βρίσκεται στο μηχάνημα, μία M2M συσκευή διαχείρισης, μία πλατφόρμα διανομής και εφαρμογές που επιτρέπουν σε συσκευές IOT να αναφέρουν ή να ενεργούν για δεδομένα. Ενώ υπάρχουν πολλοί προμηθευτές, ελάχιστοι προμηθευτής δεν προσφέρει μια ολοκληρωμένη λύση, χωρίς την οικοδόμηση εταιρικών σχέσεων.

12.1 ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΠΙΧΕΙΡΗΣΕΩΝ

Η **HP**, καθώς έχει μελετήσει τα επιχειρησιακά οφέλη που προσφέρει το IOT και στο νέο πλαίσιο της ολοένα και μεγαλύτερης ανάπτυξης της τεχνολογίας χάρη στο Internet of Things, η Hewlett Packard φιλοδοξεί να κάνει πιο έξυπνο το δίκτυο των επιχειρήσεων. Το Hewlett Packard Enterprise εφαρμόζει τα Edgeline Internet of Things Systems, τα οποία έρχονται να βοηθήσουν την είσοδο δεδομένων από το Διαδίκτυο των Πραγμάτων στο data center με σκοπό την καλύτερη και ταχύτερη αξιοποίηση των δεδομένων αυτών. Ο σκοπός της Hewlett Packard είναι να γίνει πιο γρήγορη η λειτουργία των επιμέρους

εφαρμογών του Internet of Things, ενώ ταυτόχρονα υπάρχει η δυνατότητα για την μείωση του κόστους από την συγκέντρωση και την ανάλυση των δεδομένων από τις υποδομές μίας επιχείρησης. Στο πλαίσιο αυτό, η Hewlett Packard παρουσιάζει τα συστήματα EL10 και EL20, το πρώτο απευθύνεται σε entry level απαιτήσεις και το δεύτερο αποσκοπεί στην μεγαλύτερη ανάλυση δεδομένων για το επιχειρηματικό data center. Οι εφαρμογές της Hewlett Packard απευθύνονται σε επιχειρήσεις βιομηχανικές, logistics, μεταφορών, υγείας, σε κυβερνητικές εφαρμογές και λύσεις σημείων πώλησης. Υπάρχει η πιστοποίηση λειτουργίας με το Microsoft Azure. Οι Internet of Things λύσεις της Hewlett Packard υποστηρίζουν την αρχιτεκτονική Moonshot για μικρότερες απαιτήσεις ενέργειας και χώρου σε σχέση με έναν κανονικό server. Η Hewlett Packard θεωρεί ότι μπορούν να αναπτυχθούν πολλές εφαρμογές για το Internet of Things από τις επιχειρήσεις με τη χρήση των λύσεών της. Αντίθετος η **Intel** δίνει έμφαση στο πεδίο του Internet of Things με την παρουσίαση των Quark chips και ενός δωρεάν λειτουργικού συστήματος για όλες τις συσκευές. Η Intel θέλει να διευκολύνει κατά πολύ τους developers στην διαδικασία ανάπτυξης των εφαρμογών τους, καθώς ισχυρίζεται ότι με το λογισμικό της θα μπορούν να ξεκινήσουν τη δημιουργία των εφαρμογών τους μέσα σε ένα δεκάλεπτο.

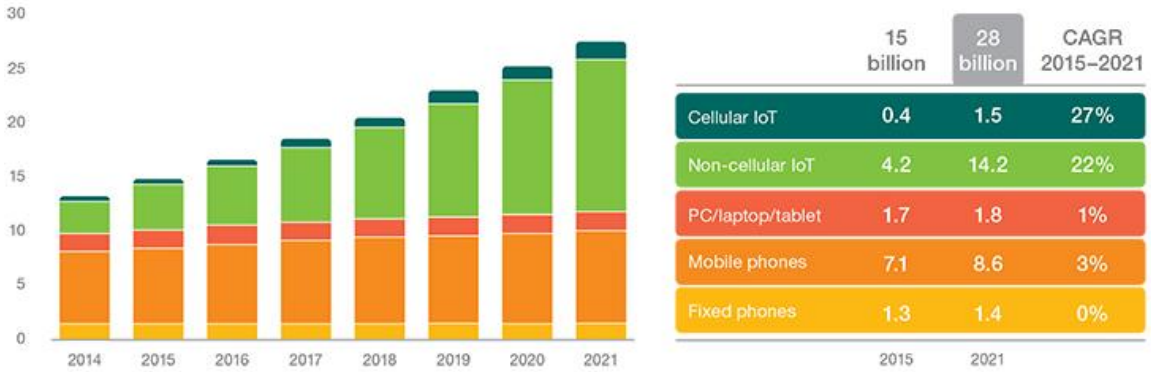
Οι επεξεργαστές Quark είναι ελάχιστα απαιτητικοί σε ενέργεια, στοιχείο που τους καθιστά ιδανικούς για ενσωμάτωση σε συσκευές μικρού μεγέθους, ενώ σύμφωνα με το IT World, η ARM είναι έτοιμη να παρουσιάσει τη δική της οικογένεια επεξεργαστών για το Internet of Things.Τα Quark Systems on Chips αναμένεται να κάνουν την εμφάνισή τους στο πρώτο μισό του επόμενου έτους, μαζί με τα πρώτα controllers που παρουσίασε η Intel. Μέσω της θυγατρικής της Wind River, η Intel παρουσίασε δύο διαφορετικά λειτουργικά συστήματα για το Internet of Things, το Rocket που απαιτεί micro controllers στα 32 bit, ενώ το Pulsar Linux είναι μία περισσότερο ολοκληρωμένη πρόταση λογισμικού που μπορεί να συνεργαστεί και με CPUs στα 64 Bit. Παράλληλα, η Intel παρουσίασε μία σειρά από cloud υπηρεσίες για τη διευκόλυνση της λειτουργίας του Internet of Things, με το brand Helix, για να τη διαχείριση δεδομένων και την δημιουργία εφαρμογών.

13. Στατιστικά

Όπως έγινε απόλυτα κατανοητό, το Internet of Things, είναι η επόμενη επανάσταση μετά την εποχή του Internet, και θα αλλάξει όχι μόνο τον τρόπο που εργαζόμαστε, και επικοινωνούμε, αλλά θα επηρεάσει κατά κόρων, την ανθρώπινη υπόστασή. Παρακάτω, έχουν καταγραφεί στατιστικά στοιχειά, και προβλέψεις για το κύμα την αλλαγής που ονομάζεται Internet of Things. Η μελέτη της ΣΕΠΕ υπολογίζει ότι οι IOT συσκευές θα ξεπεράσουν σε αριθμό, τα έξυπνα κινητά τηλέφωνα το 2018 και θα προκαλέσει ανατροπή στην παγκόσμια αγορά συσκευών, καθώς η αλλαγή θα «πυροδοτήσει» το οικοσύστημα του Internet of Things (IoT), ως αποτέλεσμα, σε λιγότερο από δύο χρόνια από σήμερα, οι συσκευές που σχετίζονται με το Internet των Πραγμάτων αναμένεται να ξεπεράσουν σε αριθμό τα κινητά τηλέφωνα και θα αποτελεί την πολυπληθέστερη κατηγορία συνδεδεμένων συσκευών. Το IoT βρίσκεται στο επίκεντρο της διαδικασίας ψηφιοποίησης της οικονομίας και της κοινωνίας, με το οικοσύστημα, που δημιουργεί γύρω του, να μεγεθύνεται τάχιστα. Σύμφωνα με το τελευταίο Ericsson Mobility Report, που δόθηκε στη δημοσιότητα, ο αριθμός των IoT συσκευών θα αυξάνεται μεταξύ 2016 και 2021 με μέσο ετήσιο ρυθμό 23%. Με βάση αυτές τις εκτιμήσεις, η παγκόσμια αγορά θα μετρά, έως το 2021, 28 δις συνδεδεμένες συσκευές, εκ των οποίων τα 16 δις θα σχετίζονται με το IoT.

Η ΣΕΠΕ τονίζει, ότι η έκθεση της Ericsson προβλέπει ότι η Δυτική Ευρώπη θα αποτελέσει την “καρδιά ” της ανάπτυξης για τις IoT συσκευές, εκτιμώντας ότι ο αριθμός τους θα πενταπλασιαστεί στην περιοχή έως το 2021. Την ανάπτυξη του IoT στην περιοχή της Ευρώπης δεν θα καθοδηγήσει, πάντως, η προερχόμενη από τους απλούς καταναλωτές ζήτηση. Οι αναλυτές προβλέπουν ότι τα συνδεδεμένα αυτοκίνητα, οι “έξυπνοι” μετρητές ενέργειας, οι εφαρμογές για το “έξυπνο” σπίτι θα είναι οι τομείς, που θα τονώσουν τη ζήτηση για IoT συσκευές επί ευρωπαϊκού εδάφους.

Τη δυναμική του IoT τόσο στην περιοχή της Ευρώπης, όσο και σε παγκόσμιο επίπεδο, αναμένεται να ενισχύσει η πτώση του κόστους των συσκευών, καθώς και το λανσάρισμα νέων καινοτόμων εφαρμογών. Επιπλέον, η εμπορική ανάπτυξη δικτύων της τεχνολογίας 5G, από το 2020, αναμένεται να παρέχει πρόσθετες δυνατότητες, οι οποίες είναι κρίσιμες για IoT, καθώς ανοίγουν το δρόμο για τη διασύνδεση περισσότερων συσκευών στο Διαδίκτυο, αλλά και μεταξύ τους.



13.0.1 *Στατιστικά Συνδεδεμένων Συσκευών (Δισεκατομμύρια)*

Ένα εξίσου ενδιαφέρον εύρημα του Ericsson Mobility Report είναι ότι, από το 3ο τρίμηνο του 2016, ο αριθμός των χρηστών smartphone θα ξεπεράσει, για πρώτη φορά, αυτόν των κατόχων συμβατικών κινητών τηλεφώνων. Μάλιστα, ήδη τα smartphone αντιπροσώπευαν το 80% της αγοράς των κινητών τηλεφώνων το 1ο τρίμηνο του τρέχοντος έτους. Σε απόλυτους αριθμούς, η αγορά σχεδόν θα διπλασιαστεί για να φτάσει τα 6,3 δις το 2021 (από 3,4 δις συσκευές σήμερα).Επιπλέον, ήδη από το 2021, η τεχνολογία του 5G θα αρχίσει να αποκτά οπαδούς ανά τον κόσμο, με τον παγκόσμιο πήχη να τοποθετείται στα 150 εκατ. Συνδρομές. Εκτός από την Ericson, η κολοσσιαία Dell, δημιουργεί νέο επιχειρησιακό πρόγραμμα, το Dell Internet of Things Solutions Partner Program με σκοπό να βοηθήσει τους ενδιαφερόμενους εταιρικούς πελάτες να αναγνωρίσουν τις ανάγκες τους, να επιλέξουν και να χτίσουν το κατάλληλο σύστημα IoT για αυτούς. Η συνεργασία της Dell γίνεται με περισσότερες από 25 εταιρείες στις οποίες περιλαμβάνονται οι GE, η Microsoft, η Software AG, η SAP, η OSIsoft. Πολλές από αυτές τις εταιρείες χρησιμοποιούν τη σειρά Dell Edge Gateway 5000 στις δικές τους λύσεις IoT. ***Ericsson***

Εκτός από την Dell ένας πανευρωπαϊκός φορέας ο AIOTI (Alliance for Internet of Things Innovation) αποτελεί τον θεσμό της Ευρωπαϊκής Ένωσης, ο οποίος συντονίζει την έρευνα και τη χρηματοδότηση για την παρουσίαση καινοτόμων προτάσεων στον τομέα του Internet of Things στο πλαίσιο της πρωτοβουλίας Horizon 2020 της Ε.Ε. Όπως αποκαλύπτεται στην ατζέντα του AIOTI για την περίοδο 2016 και 2017, οι τομείς στους

οποίους θα δοθεί προσοχή είναι οι διάφορες εφαρμογές καινοτομίας που θα εμπλέκουν το Internet of Things.

Έμφαση θα δοθεί στα οικοσυστήματα καινοτομίας, όπου οι εφαρμογές του Internet of Things θα έχουν ενεργό ρόλο, ενώ ιδιαίτερης αξίας είναι η διαδικασία προτυποποίησης του πλαισίου μέσα στο οποίο θα μπορούν να λειτουργούν οι διάφορες εφαρμογές του Internet of Things. Τα ζητήματα ιδιωτικότητας, ασφάλειας και αξιοπιστίας που προκύπτουν από την χρήση του Internet of Things αποτελούν ένα ξεχωριστό πεδίο έρευνας, με απώτερο σκοπό την υιοθέτηση ενός πλάνου πολιτικής για τις εν λόγω εφαρμογές. Τέλος, τόσο το ζήτημα της καλυτέρευσης των συνθηκών ζωής όσο και της καλλιέργειας τροφής, γεωργίας, λειτουργίας των έξυπνων πόλεων, των wearables και του smart mobility, μαζί με την χρήση του Internet of Things για την διαδικασία της παραγωγής βρίσκονται ψηλά στην ατζέντα των φορέων της Ευρωπαϊκής Ένωσης για το Horizon 2020.

Σύμφωνα και με τα στοιχεία της IDC, η δαπάνη για το Internet of Things εντός του 2015 έφτασε στο ποσό των 699 δισεκατομμυρίων δολαρίων. Η δαπάνη αυτή εκτιμάται ότι θα εκτοξευτεί στο ποσό των 1,3 τρισεκατομμυρίων δολαρίων μέχρι το έτος 2019. Η περιοχής της Ασίας και του Ειρηνικού βρίσκεται στην αιχμή της τεχνολογίας και φαίνεται να κινεί τα νήματα για την επικράτηση του Internet of Things σε διάφορες εκδοχές της καθημερινότητας. Ο κατασκευαστικός και ο τομέας των μεταφορών είναι εκείνοι που οδηγούν την κούρσα των εξελίξεων στο Internet of Things. Η Λατινική Αμερική είναι ένα γεωγραφικό σημείο που εκτιμάται ότι θα γνωρίσει ανάπτυξη στον τομέα του Internet of Things κατά τη διάρκεια της επόμενης πενταετίας. Πεδία στα οποία το Internet of Things θα βλέπει ολοένα και μεγαλύτερη ανάπτυξη είναι οι ασφάλειες, η υγεία και η μελέτη των συνηθειών των καταναλωτών. Αυτή τη στιγμή η περιοχή της Ασίας και του Ειρηνικού πραγματοποιεί το 40% των επενδύσεων στο Internet of Things, ενώ ακολουθούν η Βόρεια Αμερική και η Δυτική Ευρώπη. Η κατάσταση αυτή δεν αναμένεται να αλλάξει, απλώς όλες οι περιοχές εκτιμάται ότι θα δώσουν μεγαλύτερη έμφαση στο Internet of Things στο μέλλον.

Έτσι και στον Ελλαδικό χώρο, Ελληνικές ομάδες συμμετείχαν στο πρόγραμμα *Ορίζοντας 2020 με θέμα το Internet Of Things* και αποσπάσανε χρηματοδότηση σε τέσσερα έργα έρευνας και ανάπτυξης, αντλώντας 3,36 εκατ. ευρώ από τη συνολική κοινοτική συγχρηματοδότηση 51,5 εκατ. ευρώ. Το project SymbIoTe που συντονίζεται από ελληνικό φορέα (Intracom A.E.) έλαβε την υψηλότερη βαθμολογία στη συγκριτική αξιολόγηση. Τα αποτελέσματα αυτά παρουσιάστηκαν στην ενημερωτική ημερίδα με θέμα «Χρηματοδότηση και καινοτομία μέσω του Internet of Things (IoT) στην Ελλάδα» την οποία διοργάνωσε το

Εθνικό Κέντρο Τεκμηρίωσης (ΕΚΤ) και η Ευρωπαϊκή Συμμαχία για το Διαδίκτυο των Πραγμάτων (Alliance for the Internet of Things Innovation) με την υποστήριξη της Ευρωπαϊκής Επιτροπής.
Τα υπόλοιπα που επελέγησαν είναι το AGILE Project με επικεφαλής τον Χάρη Δούκα της Create-net, το VICINITY Project με επικεφαλής τον Θανάση Τρυφερίδη, ΕΚΕΤΑ, και το BIG IT, ECONAIS. (Λέττα Καλαμαρά, 2016). Αντίθετα, στο εξωτερικό και συγκεκριμένα στην Ολλανδία η οποία είναι η πρώτη χώρα, η οποία επιτρέπει στο δίκτυο κινητής τηλεφωνίας της χώρας, επιτρέπει την μεταφορά δεδομένων των IOT αντικειμένων και αισθητήρων, όπως οι αισθητήρες στο λιμάνι του Άμστερνταμ και οι βαλίτσες επιβατών του διεθνή αεροδρομίου της πόλης. Το δίκτυο LoRa επιτρέπει στις συσκευές να συνδέονται στο Διαδίκτυο ακόμα και χωρίς Wi-Fi, χρησιμοποιώντας ένα σύστημα που λειτουργεί συμπληρωματικά στο δίκτυο κινητής τηλεφωνίας. Μια επιπλέον μικρή κεραία που προστίθεται στους σταθμούς βάσης των δικτύων κινητής επιτρέπει τη μετάδοση και λήψη ραδιοσημάτων χαμηλής ισχύος αλλά μεγάλης εμβέλειας. Το δίκτυο ενεργοποιήθηκε σε πιλοτική βάση το Νοέμβριο στη Χάγη και το Ρότερνταμ, επεκτάθηκε όμως γρήγορα σε όλη την Ολλανδία λόγω «σημαντικού ενδιαφέροντος», λέει η KPN.Η εταιρεία έχει εξασφαλίσει συμφωνίες για τη σύνδεση 1,5 εκατομμυρίων συσκευών, αριθμός που αναμένεται να αυξηθεί μετά τη διάθεση της υπηρεσίας σε όλη την Ολλανδία.
Δοκιμές πραγματοποιούνται στο αεροδρόμιο Σίπολ του Άμστερνταμ για την παρακολούθηση των αποσκευών, ενώ ο σιδηροδρομικός σταθμός της Ουτρέχτης πειραματίζεται με το IoT για την παρακολούθηση των μηχανισμών που επιτρέπουν στα τρένα να αλλάζουν ράγες. (Βαγγέλης Πρατικάκης, 2016).

Η έρευνα διεξήχθη από τη Samsung Electronics Europe σε περισσότερους από 10.000 Ευρωπαίους σε 18 χώρες, συμπεριλαμβανομένης της Ελλάδας, για να διερευνήσει πώς η σχέση με την τεχνολογία αλλάζει, καθώς αυτή εξελίσσεται, σύμφωνα με σχετική ανακοίνωση, η μελέτη «αποκαλύπτει πως, παρόλο που ο ρυθμός της καινοτομίας επιταχύνει, οι Ευρωπαίοι δίνουν αγώνα για να συμβαδίσουν με τη γλώσσα της τεχνολογίας, που αλλάζει διαρκώς. Η μελέτη αυτή δείχνει ότι, ενώ ο ενθουσιασμός σχετικά με την τεχνολογία αυξάνεται, η βιομηχανία αντιμετωπίζει τον αυξανόμενο κίνδυνο του να αφήσει πίσω τους καταναλωτές με μια συγκεχυμένη τεχνολογική ορολογία».

Τα νούμερα για τους Έλληνες κουνούνται, στο 17% του πληθυσμού ότι δεν θα μπορούσαν να ζήσουν χωρίς τις ευκολίες της τεχνολογίας, και 58% ότι χρησιμοποιεί περισσότερο την

τεχνολογία συγκριτικά με 2 χρόνια πριν, ενώ ένα ποσοστό του 80% προσποιείται ότι κατανοεί τους όρους Cloud Computing & IOT. Πανευρωπαϊκά "για να εξασφαλίσει ότι οι μελλοντικές γενιές θα είναι εξοικειωμένες με την τελευταία λέξη της τεχνολογίας, η Samsung συνεργάζεται με σχολεία και πανεπιστήμια, προκειμένου να διευκολύνει την προηγμένη εκμάθηση ψηφιακών δεξιοτήτων μέσα από δύο βασικά προγράμματα: τις Ψηφιακές Τάξεις και τα Ινστιτούτα Τεχνολογίας.

14. Παράδειγμα για μία Internet of Things συσκευή

Οι δυνατότητες του Internet of Things, είναι αναμφίβολο ότι θα εισχωρήσουν στον τρόπο που αλληλοεπιδρούμε με τα αντικείμενα στην καθημερινότητα μας και θα φέρει μεγάλη αλλαγή με τον τρόπο με τον οποίο ζούμε. Θα δημιουργήσουν ένα κύμα αλλαγής τόσο στο συμπεριφοριακό κομμάτι του ανθρώπου όσο και στον τρόπο παραγωγικότητας και επικοινωνίας. Καθώς οι επιχειρήσεις και οι οργανισμού σε παγκόσμια κλίμακα αλλάζουν και εξελίσσονται εσωτερικά, θα αναγκαστούν «να τρέξουν σε έναν αγώνα ταχύτητας» για την υιοθέτηση του εξοπλισμού που θα τους επιτρέψει να είναι μέρος στην αγορά της νέας τεχνολογικής επανάστασης του Internet of Things. Εκτός από τον εξοπλισμό, σταδιακά θα αναπτυχθεί και ένα μέρος από το συμπεριφοριακό κομμάτι των ανθρώπων για την αλληλεπίδραση με τα enabled αντικείμενα του Internet of Things. Στα πλαίσια της έρευνας, αυτής της πτυχιακή μας, μας βοήθησε στο να οραματιστούμε το μέλλον και να εμπνευστούμε από τις δυνατότητες, αυτής τις τεχνολογικής επανάστασης, και να σκιαγραφήσουμε την καθημερινότητα μας και με τον τρόπο που επικοινωνούμε, εργαζόμαστε, αλληλοεπιδρούμε με τα ψηφιακά μέσα & υπολογιστές και βελτιώνουμε την ζωή μας με την βοήθεια της επιστήμης. Στο επαγγελματικό σύστημα, η εξέλιξη των εργαλείων που χρησιμοποιεί ο μέσος επαγγελματίας και εργαζόμενος αναμφισβήτητα θα εμπλουτιστούν με τεχνολογίες IOT. Από το πιο μικρό εργαλείο έως πληροφορικών συστημάτων μπορούν να φέρουν βελτιώσεις. Δυνατότητες αναγνώρισης ακουστικού λαβυρίνθου από ακουστικά Bluetooth για την ταυτοποίηση των εργαζομένων με βάση ασύρματης επικοινωνίας με το πληροφοριακό σύστημα της επιχείρησης. Μπορεί να

θεωρείτο σενάριο επιστημονικής φαντασίας, αλλά είναι ένα ασφαλές σύστημα για την αδειοδότηση πρόσβασης, σε χώρους ενός οργανισμού και πληροφοριακά συστήματα ενός οργανισμού και όλα τα παραπάνω, να μην εμποδίζει την συνηθισμένη λειτουργικότητα του ασύρματου Bluetooth ακουστικού.

Επιπλέων, οι καθρέπτες μπορούν να εξελιχθούν με την υποστήριξη λειτουργικότητας Internet of Things, για την υποστήριξη παρουσίασης ενημερώσεων ή γραφημάτων τόσο στο εσωτερικό χώρο της επιχείρησης για την ενημέρωση τον εργαζομένων, όσο και στον εξωτερικό χώρο για λόγους εταιρικής διαφήμισης. Η δυνατότητα υποστήριξης αφής σε αυτούς τους εξειδικευμένους καθρέπτες επιτρέπει λειτουργικότητα και καθιστά ένα αντικείμενο/δομικό υλικό, να είναι μέρος συστήματος της επιχείρησης. Στο κομμάτι εξοπλισμού, η αλλαγή μπορεί να έρθει από τα δύσκολα επαγγέλματα, που η χρήση της τεχνολογίας είναι ζωτικής σημασίας, με παράδειγμα την κατάδυση στους ωκεανούς, με σκοπό την έρευνα της θαλάσσιας ζωής και πόρων. Οι συσκευές Internet of Things για τους καταδύτες θα φανούν εξαιρετικά χρήσιμες καθώς η δυνατότητα επικοινωνίας με άλλες συσκευές που θα φοράει ο καταδύτης είναι σημαντική.

Ένα παράδειγμα, είναι ότι αισθητήρες θα μπορούν να αναλύουν και να ειδοποιούν τον καταδύτη για επικίνδυνα ρεύματα ή την αλλαγή βάθους. Με την χρήση εξειδικευμένης κάμερας θα υπάρχει δυνατότητα για ανάλυση θαλάσσιας πανίδας & χλωρίδας, καταγραφή για νέα είδη, καθώς και σε συνδυασμό της επαυξημένης πραγματικότητας, ενσωματωμένη στην μάσκα του καταδύτη θα μπορεί να βλέπει κρίσιμες πληροφορίες από τους αισθητήρες αλλά και από την περίγυρο του, στον βυθό.

Τέλος υποβρύχιες κάμερες εξοπλισμένες με ικανότητα ασύρματης δορυφορικής επικοινωνίας, εντάσσονται στα πλαίσια της τεχνολογικής – IOT επανάστασης, καθώς αυτόνομα θα λειτουργούν για την διεκπεραίωση προγραμματισμένων εντολών. Στο εκπαιδευτικό σύστημα, ένα από τα σημαντικά εργαλεία για την εκπαίδευση των μαθητών ήταν ο μαυροπίνακας. Η δυνατότητα αναπαραγωγής οπτικό και ακουστικό περιεχόμενο που αναπαράγεται από τον πίνακα, καθώς και δυνατότητες προβολής χάρτες, γραφήματα, υποστήριξη γραφίδας και αφής, αναμφισβήτητα θα βοηθήσει τους εκπαιδευόμενους στην κατανόηση και τους εκπαιδευτικούς στην επεξήγηση. Αυτή η σκέψη, της αναβάθμισης του μέσου εκπαίδευσης ήρθε, από μια έρευνα του Πανεπιστημίου Πειραιά με την παρουσίαση τον αποτελεσμάτων στο πλαίσιο ημερίδας για την Εκπαίδευση από τον Καθηγητή Συμεών Ρετάλη (Εφημερίδα Πρώτο Θέμα, 27/5/16).

Στην μόδα, οι τεχνολογίες του Internet of Things θα εισχωρήσουν αρκετά εύκολα, και θα γίνει δίοδος για την εξοικείωση των ανθρώπων με το Internet of Things. Σαν πρωτοπόρος αυτής της σκέψης, είναι τα περίφημα wearables που αναπτύσσονται σε γρήγορους ρυθμούς και δίνουν μια νότα αισθητικής και φυσικής λειτουργικότητας. Η πλοήγηση σε χάρτες, η αποστολή email και η τηλεφωνική επικοινωνία γίνονται -ήδη- με μια κίνηση του χεριού. Επιπλέων η αναγνώριση των παλμών της καρδιάς, υποστηρίζεται ακόμα και σήμερα σε αρκετές wearable συσκευές, και με την δύναμη του Internet of Things, η λειτουργικότητα αυτών θα αναπτυχθεί παραπάνω, όπως στο ξεκλείδωμα εισόδων ενός κτηρίου ή παραχώρηση πρόσβασης σε ηλεκτρονικούς υπολογιστές μέσο ταυτοποίησης από την wearable συσκευή.

Στα οικιακά, όπως έχει γίνει αναφορά και στα παραπάνω κεφάλαια, θα έρθει ένα μεγάλο κύμα αλλαγών στον τρόπο που διαχειριζόμαστε τις καθημερινές μας δραστηριότητες, λόγο της ένταξης IOT τεχνολογίας σε όλες τις πτυχές που αποτελούν ένα σπίτι, και στην εξέλιξη αυτού σε ένα «έξυπνο».

Σαν συνέπεια όλων των παραπάνω, η τεχνολογία του Internet of Things, δεν είναι μόνο ένα αντικείμενο το οποίο μπορεί να χαρακτηρίσει την βασική έννοια και τους σκοπούς λειτουργικότητας που προσφέρει αυτή η τεχνολογία. Το Internet of Things αποτελείται από ένα νεφέλωμα ιδεών που σταδιακά θα καλύψει και θα δημιουργήσει ανάγκες, για μια καλύτερη ποιότητα ζωής. Πολλές τεχνολογίες, εταιρίες και διαφορετικές αντιλήψεις, στο τέλος θα ενοποιηθούν για να δημιουργήσουν την εικόνα του αύριο, που μελετάμε σήμερα, με το όνομα Internet of Things.

15. Βιβλιογραφία

- Alessandro Bassi, Martin Bauer, Martin Fiedler, Thorsten Kramp, Rob van Kranenburg, Sebastian Lange, Stefan Meissner. (2013) **Enabling Things to Talk: Designing IOT solutions with the IOT Architectural Reference Model**. New York: Springer.

- RFC Forum (2005**) Basic Transition Mechanisms for IPv6 Hosts and Routers** < http://www.rfc-base.org/rfc-4213.html > τελευταία επίσκεψη: 26/5/2016

- IPv6 Wikipedia, 2016 < https://en.wikipedia.org/wiki/IPv6#Deployment >, τελευταία επίσκεψη 26 ου 2016)

- Peter Mell & Tim Grace(2009) **Definition of Cloud Computing.** ΗΠΑ: NIST

- Sebastian Anthony(2012) **How Big is the Cloud** ΗΠΑ

- ΣΕΠΕ (2016) **Οι συσκευές IoT θα ξεπεράσουν σε αριθμό τα κινητά τηλέφωνα το 2018** < http://www.sepe.gr/gr/research-studies/article/6338364/oi-suskeues-iot-tha-xeperasoun-se-arithmo-ta-kinita-tilefona-to-2018/> τελευταία επίσκεψη: 09/6/2016

- Νίκος Καιμακάμης (2015) **Η Hewlett Packard Enterprise κοντά στο Internet of Things,** Αθήνα.

- Νίκος Καιμακάμης (2015) **ΑΙΟΤΙ: Στόχοι της έρευνας για το Internet of Things,** Αθήνα.

- Google (2016) **Brillo & Weave** <developers.google.com/brillo>, τελευταία επίσκεψη: 09/6/2016
- Microsoft (2016) **Δείτε τι μπορεί να κάνει το Cloud για την επιχείρηση σας** <https://technet.microsoft.com/el-gr/ff934854.aspx> τελευταία επίσκεψη: 26/6/2016
- Jakob Engblom (2014) **Internet of Things Automatic Testing – Using Simulation,** ΗΠΑ.
- William Toll (2014) **Tools For The Internet Of Things, ΗΠΑ.**

- Λέττα Καλαμαρά, (2016) '**Ελληνικά τα τέσσερα από τα επτά έργα IOT' στην** *Ναυτεμπορική* Αθήνα
- Βαγγέλης Πρατικάκης (2016) **Η Ολλανδία λανσάρει το πρώτο εθνικό δίκτυο για το Internet of Things** Αθήνα
- Tschofenig H, Arkko J, Thaler D, McPherson D. Architectural Considerations in Smart Object Networking Internet Architecture Board (IAB) Mar. 2015 https://tools.ietf.org/html/rfc7452
- Hong Zhou, BingWu Liu, and PingPing Dong D. Li and Y. Chen (Eds.): The Technology System Framework of the Internet of Things and Its Application Research in Agriculture CCTA 2011, Part I, IFIP AICT 368, pp. 293–300, 2012.
- Atzori L., Iera A., Morabito G., (2010). The Internet of Things: A survey. Computer Networks, Vol.54, pp. 2787–2805.
- http://www.gsma.com/connectedliving/narrow-band-internet-of-things-nb-iot/
- M.U. Farooq, Muhammad Waseem, Sadia Mazhar, Anjum Khairi, Talha Kamal. International Journal of Computer Applications (2015) "A Review on Internet of Things (IoT)". International Journal of Computer Applications, 113, March 2015
- Dejan Jurejevcic, IoT tech deep-dive: The rise of beacon technology September 3, 2015 , https://iot-analytics.com/rise-of-beacon-technology/
- HP Enterprise Security, Internet of Things Research Study 2014 ISSA: October 2014 • The Internet of Things (IoT)
- https://el.wikipedia.org/wiki/TLS
- https://en.wikipedia.org/wiki/Man-in-the-middle_attack
- http://www.slideshare.net/SPRICOMUNICA/basque-industry-40-the-fourth-industrial-revolution-based-on-smart-factories
- http://www.slideshare.net/AnkurPipara/internet-of-things-iot-2014

- http://blog.ots.gr/tag/internet-of-things/#.V5W19IOLTIU
- Gil Reiter. Wireless connectivity for the Internet of Things. 2014 Texas Instruments Incorporated
- The internet of things: An Overview. Understanding the Issues and Challenges of a More Connected World. By Karen Rose, Scott Eldridge, Lyman Chapin (2015) page 13-18, www.internetsociety.org
- SECURITY IN THE INTERNET OF THINGS : Lessons from the Past for the Connected Future/ by AJ Shipley 2015 Wind River Systems, Inc., http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf
- Internet of Things *Exploring and Securing a Future Concept* by Cristian Bude and Andreas Kervefors Bergstrand KTH Royal Institute of Technology School of Information and Communication Technology (ICT). pages 21-25
- https://en.wikipedia.org/wiki/ZigBee
- https://el.wikipedia.org/wiki/WiMAX
- http://whatis.techtarget.com/definition/ultra-wideband
- http://www.techradar.com/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410
- http://ic.mycdt.se/projectweb/42c13bdf2e759/Flash%20OFDM.html