ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΠΛΑΙΣΙΟΥ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΜΕΓΑΛΟΥ ΔΙΚΤΥΟΥ ΑΙΣΘΗΤΗΡΩΝ (ΔΙΑΔΙΚΤΥΟ ΠΡΑΓΜΑΤΩΝ)

ΑΙΚΑΤΕΡΙΝΗ Ε. ΠΛΕΥΡΑΚΗ

Μιχαήλ Θεολόγου
Ομότιμος Καθηγητής Ε.Μ.Π.

ΙΟΥΝΙΟΣ 2017

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΜΕΛΕΤΗ ΠΛΑΙΣΙΟΥ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝ ΜΕΓΑΛΟΥ ΔΙΚΤΥΟΥ ΑΙΣΘΗΤΗΡΩΝ (ΔΙΑΔΙΚΤΥΟ ΠΡΑΓΜΑΤΩΝ)

ΑΙΚΑΤΕΡΙΝΗ Ε. ΠΛΕΥΡΑΚΗ

Μιχαήλ Θεολόγου
Ομότιμος Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την .....

.....	.....	.....
Μιχαήλ Θεολόγου Ομότιμος Καθηγητής Ε.Μ.Π.	Δρ. Ευγενία Αδαμοπούλου	Δρ. Κωνσταντίνος Δεμέστιχας

ΙΟΥΝΙΟΣ 2017

ΠΕΡΙΛΗΨΗ

Το Διαδίκτυο των Πραγμάτων αναφέρεται στο διασυνδεδεμένο δίκτυο συσκευών που φέρουν κάποια μορφή τεχνητής νοημοσύνης. Τα καταναλωτικά προϊόντα, τα μέσα μεταφοράς, βιομηχανικά και βοηθητικά εξαρτήματα, οι αισθητήρες και άλλα καθημερινά αντικείμενα (διάφορα «πράγματα») επικοινωνούν μεταξύ τους και με το εξωτερικό περιβάλλον αποστέλλοντας και λαμβάνοντας δεδομένα. Τα αντικείμενα αυτά υπάρχουν εμφανώς ή μη εμφανώς σε κάθε πτυχή της καθημερινότητας και υπόσχονται να μετατρέψουν τον τρόπο εργασίας μας αλλά και την καθημερινή μας ζωή.

Την ίδια στιγμή ωστόσο, το Διαδίκτυο των Πραγμάτων δημιουργεί νέες σημαντικές προκλήσεις ασφαλείας, που θα μπορούσαν να σταθούν εμπόδιο στο δρόμο της κατάκτησης των δυνητικών οφελών. Ήδη οι ανησυχίες και οι φόβοι περί ασφάλειας και απορρήτου έχουν προσελκύσει τη δημόσια προσοχή. Συνεπώς για την πλήρη ανάπτυξη και εκμετάλευση αυτής της τεχνολογίας θα πρέπει να υπάρξει αρχικά μια κατανόηση της κατάστασης των χρηστών και των συσκευών τους, των αρχιτεκτονικών και των δικτύων επικοινωνίας, των εφαρμογών που θα επεξεργάζονται και θα αναλύουν τις πληροφορίες, αλλά και των πιθανών κινδύνων και απειλών προς αυτά, ώστε να μπορούν να σχεδιαστεί, εγκαθιδρυθεί και να διατηρηθεί ένα καθολικό επίπεδο προστασίας, ικανό να διασφαλίσει την ασφάλεια και την ιδιωτικότητα σε όλα τα επίπεδα του Διαδικτύου Πραγμάτων.

Σκοπός της παρούσας Διπλωματικής είναι η μελέτη εφαρμογής και αξιοποίησης τεχνολογιών και μεθοδολογιών προάσπισης της Ασφάλειας και της ιδιωτικότητας στο Διαδίκτυο των Πραγμάτων.

Αρχικά, αποτυπώνονται οι ορισμοί του Διαδικτύου Πραγμάτων, της Ασφάλειας και της Ιδιωτικότητας και στη συνέχεια αναλύονται τα συστατικά του Διαδικτύου Πραγμάτων για να είναι εφικτή η σύνδεση των πιθανών απειλών και κινδύνων με τα επίπεδα που το αποτελούν.

Εν συνεχεία παρουσιάζονται συγκεντρωτικά τόσο οι δυνητικές απειλές, όσο και οι πιθανές επιπτώσεις τους και παρουσιάζονται οι απαιτήσεις και οι περιορισμοί του ελληνικού και ευρωπαϊκού νομικού και κανονιστικού πλαισίου.

Έπειτα καταγράφονται οι απαιτήσεις που υπάρχουν αναφορικά με την Ασφάλεια και την Ιδιωτικότητα στο Διαδίκτυο των Πραγμάτων.

Λαμβάνοντας υπόψη όλα τα παραπάνω, προτείνονται τρόποι αντιμετώπισης και ελαχιστοποίησής των γνωστών απειλών, από το αρχικό επίπεδο των χρηστών μέχρι το τελικό επίπεδο των αποθηκευμένων δεδομένων.

Τέλος, με βάση ένα ευρωπαϊκό έργο που βρίσκεται σε εξέλιξη, διατυπώνονται προτάσεις σχετικά με τα όσα έχουν αναλυθεί και διατυπωθεί πρωτύτερα.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Διαδίκτυο Πραγμάτων, Ασφάλεια, Ιδιωτικότητα, Δίκτυο αισθητήρων, Κακόβουλες επιθέσεις

ABSTRACT

The Internet of Things refers to an interconnected network of devices that carry some form of artificial intelligence. Consumer products, means of transport, industrial and auxiliary components, sensors and other everyday objects (various "things") communicate with each other and the external environment by sharing and receiving data. These objects are becoming an important feature of every aspect of daily life, with the promise to transform our way of living.

At the same time, however, the Internet of Things creates significant challenges that could stand in the way of fully conquering the potential benefits. The public has already voiced concerns and fears about security and privacy. The first step towards the full development and exploitation of this technology is to understand the current situation of its users and their devices, the architectures and communication networks in effect, the applications that will process and analyze the data as well as the potential risks and threats to all these layers. The second step is to design, establish and maintain a universal level of protection capable of providing security and privacy across all levels of the Internet of Things.

The purpose of this Diploma Thesis is to study the application of technologies and methodologies to reinforce security and privacy in the Internet of Things.

In the introduction, the definitions of the Internet of Things, Security, and Privacy are given, and later on the components of the Internet of Things are analyzed so that the reader is able to to link potential threats and risks to the architectural levels.

The potential threats as well as their potential impact are summarized, and the requirements and constraints of the Greek and European legal and regulatory framework are presented. In the following chapters the requirements regarding Security and Privacy on the Internet of Things are presented.

Taking all of the previously provided information into consideration, possible solutions to address and minimize known threats are described, spreading across all levels of the Internet of Things, from users to stored data.

Finally, the Thesis offers some suggestions on a European project in progress, stemming from the analysis that has been provided in the previous chapters.

KEYWORDS: Internet of Things (IoT), Security, Privacy, Sensors network, Malicious attacks

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον καθηγητή κ. Μιχαήλ Θεολόγου για την ανάθεση της συγκεκριμένης διπλωματικής εργασίας και της ευκαιρίας που μου παρείχε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα. Επίσης θα ήθελα να εκφράσω τις θερμές ευχαριστίες μου στην Δρ. Ευγενία Αδαμοπούλου για την αμέριστη βοήθεια που μου παρείχε κατά τη διάρκεια της εκπόνηση της διπλωματικής εργασίας και τον Δρ. Κωνσταντίνο Δεμέστιχα που συνέβαλε στην ολοκλήρωση της. Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου για την στήριξη που μου παρέχει καθημερινά.

Αικατερίνη Πλευράκη

ΠΕΡΙΕΧΟΜΕΝΑ

1. Εισαγωγή 13
1.1. Βασικές έννοιες 14
1.1.1. Ορισμός του Διαδικτύου Πραγμάτων (IoT) 14
1.1.2. Ορισμός Ιδιωτικότητας 18
1.1.2.1. Βασικές Αρχές της Ιδιωτικότητας 20
1.1.3. Ορισμός Ασφάλειας 21
1.1.4. Η σχέση μεταξύ Ιδιωτικότητας και Ασφάλειας.....24
2. Διαδίκτυο Πραγμάτων (IoT) 29
2.1. Αρχιτεκτονική Διαδικτύου Πραγμάτων 29
2.1.1. Αρχιτεκτονική τριών και πέντε επιπέδων 29
2.1.2. Αρχιτεκτονικές βασισμένες στο Cloud και το Fog 31
2.2. Συστατικά του Διαδικτύου Πραγμάτων 33
2.2.1. Τα υλικά συστατικά του Διαδικτύου Πραγμάτων 34
2.2.1.1. Αισθητήρες Διαδικτύου Πραγμάτων 35
2.2.1.2. Wearable Ηλεκτρονικές Συσκευές 37
2.2.1.3. Τυπικές συσκευές.....38
2.2.2. Το επίπεδο επικοινωνίας του Διαδικτύου Πραγμάτων 38
2.2.3. Το επίπεδο εφαρμογών του Διαδικτύου Πραγμάτων 45
2.3. Πεδία όπου έχει εφαρμογή το Διαδίκτυο Πραγμάτων 47
3. Ιδιωτικότητα και ασφάλεια.....53
3.1. Ανάλυση Απειλών – Επιπτώσεων Ιδιωτικότητας σε εφαρμογές του Διαδικτύου Πραγμάτων 54
3.1.1. Κίνδυνοι έκθεσης του ιδιωτικού απορρήτου των χρηστών.....55
3.1.2. Απειλές κατά της ταυτότητας των χρηστών 56
3.1.3. Παρακολούθηση δεδομένων 56
3.1.4. Ιδιωτικότητα αποθηκευμένων δεδομένων 57
3.1.5. Απόρρητο τοποθεσίας χρηστών.....58
3.2. Ανάλυση Απειλών – Επιπτώσεων Ασφάλειας σε εφαρμογές του Διαδικτύου Πραγμάτων 59
3.2.1. Θέματα Ασφάλειας στο Διαδίκτυο Πραγμάτων σε συσχέτιση με το παραδοσιακό Διαδίκτυο.....59
3.2.2. Ευρύτερη Κατηγοριοποίηση απειλών προς την ασφάλεια.....61
3.2.3. Θέματα Ασφάλειας στο Διαδίκτυο Πραγμάτων ως προς τα τρία επίπεδά του ...62
3.2.3.1. Θέματα Ασφάλειας στα υλικά συστατικά του Διαδικτύου Πραγμάτων 63

3.2.3.2. Θέματα Ασφάλειας στο επίπεδο επικοινωνίας του Διαδικτύου Πραγμάτων...64
3.2.3.3. Θέματα Ασφάλειας στο επίπεδο εφαρμογών του Διαδικτύου Πραγμάτων.....67
3.3. Παραδείγματα ζητημάτων Ιδιωτικότητας και ασφάλειας σε συσκευές και εφαρμογές του Διαδικτύου πραγμάτων 70
3.4. Νόμοι και κανονισμοί 71
4. Απαιτήσεις Ιδιωτικότητας και Ασφάλειας στο Διαδίκτυο Πραγμάτων 79
4.1. Απαιτήσεις Ιδιωτικότητας 79
4.2. Απαιτήσεις Ασφάλειας 80
5. Μέτρα επίτευξης Ιδιωτικότητας και Ασφάλειας στο Διαδίκτυο Πραγμάτων και ελαχιστοποίησης απειλών-κινδύνων 83
6. Συμπεράσματα και προτάσεις για το έργο σε εξέλιξη 95
ΑΝΑΦΟΡΕΣ 105

1. Εισαγωγή

Η ανάπτυξη των τεχνολογιών κατέστησε αντιληπτή τη μετατροπή της κοινωνίας σε κοινωνία της πληροφορίας μέσω του διαδικτύου. Πλέον το διαδίκτυο τείνει να μετατραπεί από ένα μέρος όπου καταφεύγει ο χρήστης για να αναζητήσει κάποια πληροφορία, σε ένα μέρος όπου απλά βρίσκεται – το Διαδίκτυο των Πραγμάτων.

Από τα πρώτα χρόνια της πορείας των επικοινωνιών και της επιστημονικής ανάπτυξης στον τομέα της πληροφορικής, ένα από τα πιο αξιοσημείωτα θέματα που εξακολουθεί να υφίσταται είναι η ασφάλεια του χρήστη, του συστήματος και των δεδομένων, αλλά και η διαχείριση των προσωπικών δεδομένων και η προστασία της ιδιωτικότητας του χρήστη. Η επίδραση του Διαδικτύου των Πραγμάτων αναφορικά με την ασφάλεια και την ιδιωτικότητα δεν έχει γίνει ακόμα πλήρως αντιληπτή. Σε σύγκριση με την έρευνα στο Internet και τα ασύρματα δίκτυα, οι μελέτες των αρχιτεκτονικών ασφαλείας του Διαδικτύου Πραγμάτων είναι σχετικά λίγες. Λόγω των ιδιαιτέρων χαρακτηριστικών του (ενσωμάτωση πολλών δικτύων, περιορισμένη δυνατότητα αποθήκευσης και υπολογιστικής λειτουργίας κάποιων τερματικών συσκευών) είναι δύσκολο να εφαρμοστεί το μοντέλο ελέγχου πρόσβασης του παραδοσιακού Internet στο διαδίκτυο.

Επίσης οι κανονισμοί και οι νομοθετικές ρυθμίσεις θέτουν κάποια όρια τα οποία δεν επαρκούν. Θα πρέπει να χρησιμοποιηθούν και οι κατάλληλες τεχνικές ενίσχυσης της ασφάλειας και της ιδιωτικότητας, ανάλογα πάντα με τα τεχνολογικά ζητήματα που προκύπτουν και τις απαιτήσεις του χρήστη και των εφαρμογών.

Αν η ασφάλεια παρομοιαστεί με μια πυραμίδα τότε σίγουρα την βάση αυτής αποτελεί η σχεδίαση και εφαρμογή μιας ολοκληρωμένης πολιτικής ασφαλείας. Απαραίτητες διαδικασίες για την υλοποίηση της είναι η ανάλυση ρίσκου και η αποτίμηση κινδύνων. Η πολιτική ασφάλειας καλείται να προβλέψει πιθανά συμβάντα και καταστάσεις, απειλητικές για την ασφάλεια αυτών, και να προτείνει μια σειρά μέτρων αντιμετώπισης τους. Εμπειρικά έχει αποδειχθεί ότι οι μηχανισμοί και οι τεχνικές από μόνα τους δεν συνιστούν μέτρα ασφαλείας.

Αυτά πρέπει να λειτουργούν κάτω από ένα μοντέλο ασφάλειας. Ωστόσο η πρόβλεψη κινδύνων σε οποιαδήποτε ενέργεια μας είναι αδύνατη, από την άποψη ότι οι πιθανοί συνδυασμοί ενεργειών που δύνανται να προκαλέσουν πρόβλημα είναι άπειροι ο δυσκολότερος παράγοντας είναι η ανθρώπινη φύση που κρύβει εκπλήξεις, άλλοτε ευχάριστες άλλοτε δυσάρεστες.

1.1. Βασικές έννοιες

1.1.1. Ορισμός του Διαδικτύου Πραγμάτων (IoT)

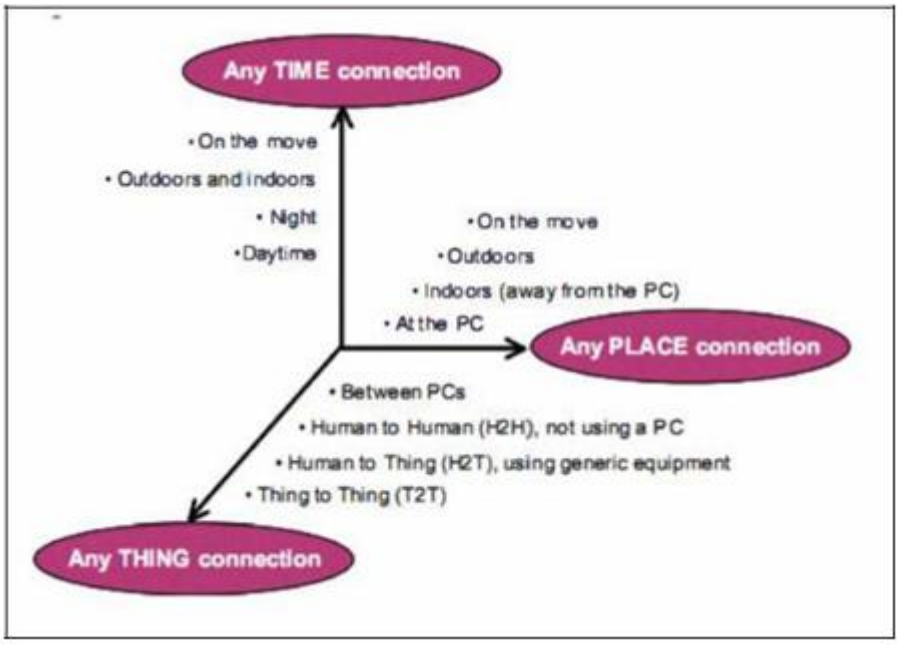
Καθώς η τεχνολογία εξελίσσεται και με την πάροδο του χρόνου οδηγούμαστε σε περιβάλλοντα που είναι συνέχεια συνδεδεμένα, ερευνώνται και εφαρμόζονται τεχνικές που σχετίζονται με το μελλοντικό Internet. Από εκεί προκύπτει και ο όρος Διαδίκτυο Πραγμάτων - Internet of Things (IoT) ο οποίος υπονοεί την σύνδεση πραγμάτων στον Παγκόσμιο Ιστό. Το Διαδίκτυο Πραγμάτων είναι η σύνδεση φυσικών συσκευών, οι οποίες με τη βοήθεια ενσωματωμένων τεχνολογιών (embedded technology), δίνουν την δυνατότητα επικοινωνίας αλλά και καταγραφής μεγεθών του εξωτερικού περιβάλλοντος και της εσωτερικής τους κατάστασης. Έτσι με τη συμβολή πρωτοκόλλων, αισθητήρων, φθηνότερων επεξεργαστών και κατάλληλων εφαρμογών, είναι δυνατή η αποτελεσματική αξιοποίηση της τεχνολογίας αυτής.

Τα χαρακτηριστικά των πραγμάτων που παίρνουν μέρος στο Διαδίκτυο Πραγμάτων είναι ότι μπορούν να ταυτοποιηθούν μοναδικά μέσα στον Ιστό, μπορεί κανείς να έχει πρόσβαση σε αυτά μέσω κάποιου δικτύου, να ξέρει την θέση και την κατάστασή τους και τα οποία μπορούν να συνδυαστούν μεταξύ τους με κατάλληλες υπηρεσίες. Όπως είναι προφανές, αυτό μπορεί να επηρεάσει την επαγγελματική, προσωπική και κοινωνική ζωή των ανθρώπων.

Η εξέχουσα σημασία του Διαδικτύου Πραγμάτων έγκειται στο γεγονός πως μπορεί να επηρεάσει πολλούς τομείς της καθημερινής ζωής των χρηστών, είτε αναφερόμαστε σε άτομα είτε σε επιχειρήσεις. Αν πρόκειται για άτομα τότε τα αποτελέσματα μπορούν να είναι άμεσα στην εργασιακή αλλά και οικιακή ζωή και πιο συγκεκριμένα σε τομείς όπως είναι η υγεία, η κοινωνική ζωή, η επικοινωνία και η μάθηση. Από την οπτική γωνία του κόσμου των επιχειρήσεων, οι τομείς που επηρεάζονται είναι η βιομηχανική παραγωγή, η διαχείριση των επιχειρησιακών διαδικασιών όπως και η έξυπνη μεταφορά ανθρώπων και αγαθών. Έτσι μελλοντικά, το IoT μπορεί να είναι ένας από τους παράγοντες που μπορεί να συνεισφέρει στην οικονομική ανάπτυξη των χωρών.

Το Διαδίκτυο Πραγμάτων μπορεί να περιγραφεί με τρείς έννοιες:

- τον προσανατολισμό στο Internet
- τον προσανατολισμό στα αντικείμενα
- τον προσανατολισμό στη σημασιολογία



Εικόνα 1.1 : Διαστάσεις Διαδικτύου Αντικείμενων (IoT)

Παρόλο που αυτοί οι ορισμοί είναι απαραίτητοι για την περιγραφή ενός διεπιστημονικού αντικειμένου όπως το Διαδίκτυο Πραγμάτων, για να μπορέσει να επέλθει πλήρης κατανόηση της χρησιμότητάς του θα πρέπει να υπάρξει πρακτική εφαρμογή προκειμένου να φανεί η συνύπαρξη αυτών των τριών προσανατολισμών.

Το RFID ορίζει το Διαδίκτυο Πραγμάτων ως: "Ένα παγκόσμιο δίκτυο διασυνδεδεμένων αντικειμένων, με μοναδική διευθυνσιοδότηση βασισμένη σε συγκεκριμένα πρωτόκολλα επικοινωνίας".

Με βάση Ευρωπαϊκές έρευνες, στο Διαδίκτυο Πραγμάτων τα αντικείμενα είναι ενεργά κομμάτια των επιχειρήσεων, της πληροφορίας και των κοινωνικών διεργασιών καθώς τους δίνεται η δυνατότητα να αλληλεπιδράσουν και να επικοινωνήσουν μεταξύ τους αλλά και με το περιβάλλον μέσω ανταλλαγής δεδομένων και πληροφοριών. Ενώ παράλληλα ενεργούν αυτόνομα σε γεγονότα του φυσικού κόσμου και έχουν επιρροή μέσω διεργασιών, οι οποίες πυροδοτούν δράσεις και δημιουργούν υπηρεσίες, χωρίς να είναι πάντα απαραίτητη η ανθρώπινη παρέμβαση.

Σύμφωνα με τον Forrester ένα έξυπνο περιβάλλον χρησιμοποιεί πληροφορίες και τεχνολογίες επικοινωνίας προκειμένου να δομήσει τα βασικά συστατικά και τις υπηρεσίες της οργάνωσης μιας πόλης, της εκπαίδευσης, των υπηρεσιών υγείας, της δημόσιας ασφάλειας, των μεταφορών και των δημοσίων υπηρεσιών, καθώς και να τα καταστήσει πιο διαδραστικά και αποτελεσματικά.

Ένας ακόμα ορισμός μπορεί να δοθεί για τη χρήση του Διαδικτύου Πραγμάτων σε ένα έξυπνο περιβάλλον, ο οποίος θα είναι πιο ανθρωποκεντρικός και δεν θα περιορίζεται από κανένα πρωτόκολλο επικοινωνίας, επιτρέποντας έτσι τη δημιουργία εφαρμογών

μεγάλης διαρκείας, που θα εκμεταλλεύονται κάθε φορά την παρούσα τεχνολογία για να αναπτυχθούν.

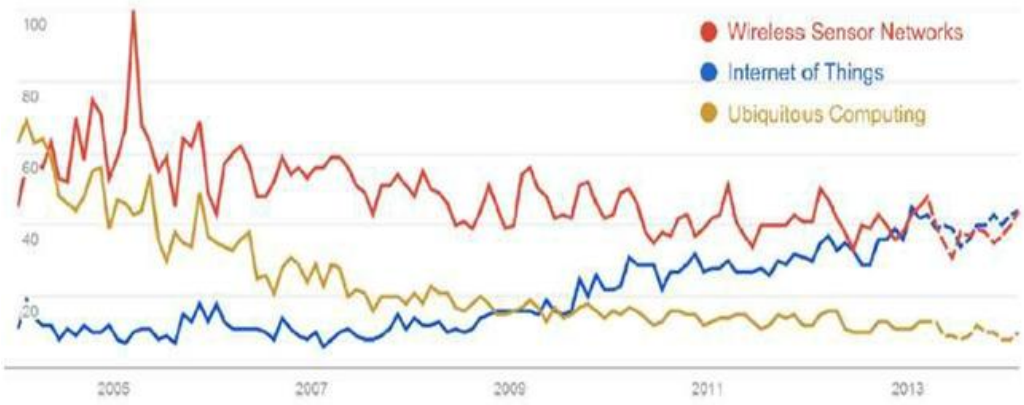
Το Διαδίκτυο Πραγμάτων ορίζεται λοιπόν και ως η διασύνδεση συσκευών παρακολούθησης και ενεργοποίησης, που παρέχει τη δυνατότητα διαμοιρασμού πληροφορίας και δημιουργίας ενός κοινού τρόπου ανάπτυξης πρωτοπόρων εφαρμογών. Αυτό επιτυγχάνεται μέσα από τη συνεχή λήψη και ανάλυση δεδομένων καθώς και την παρουσίαση πληροφοριών μέσω του Cloud.

Το Διαδίκτυο Πραγμάτων έχει οριστεί ως μία από τις πλέον αναπτυσσόμενες τεχνολογίες του IT όπως παρουσιάζεται στον Gartner's IT Hype Cycle (2016). Ο Hype Cycle ορίζεται ως ένας τρόπος παρουσίασης της ανάδειξης, της αποδοχής, της ωριμότητας και της επίδρασης διαφόρων τεχνολογιών σε εφαρμογές. Βάσει προβλέψεων η τεχνολογία του Διαδικτύου Πραγμάτων θα μπορέσει να γίνει πλήρως αποδεκτή από την αγορά μέσα σε 5-10 χρόνια, όπως φαίνεται στο αναλυτικό γράφημα που ακολουθεί.

Εικόνα 1.2: Gartner's IT Hype Cycle

Η δημοτικότητα των εφαρμογών διαφέρει με το πέρασμα του χρόνου. Η δημοτικότητα των αναζητήσεων στο διαδίκτυο, όπως μετρήθηκε από τη Google κατά την τελευταία 10ετία, σχετικά με τους όρο Internet of Things, Wireless Sensor Network και Ubiquitous Computing φαίνεται στην Εικόνα που ακολουθεί.

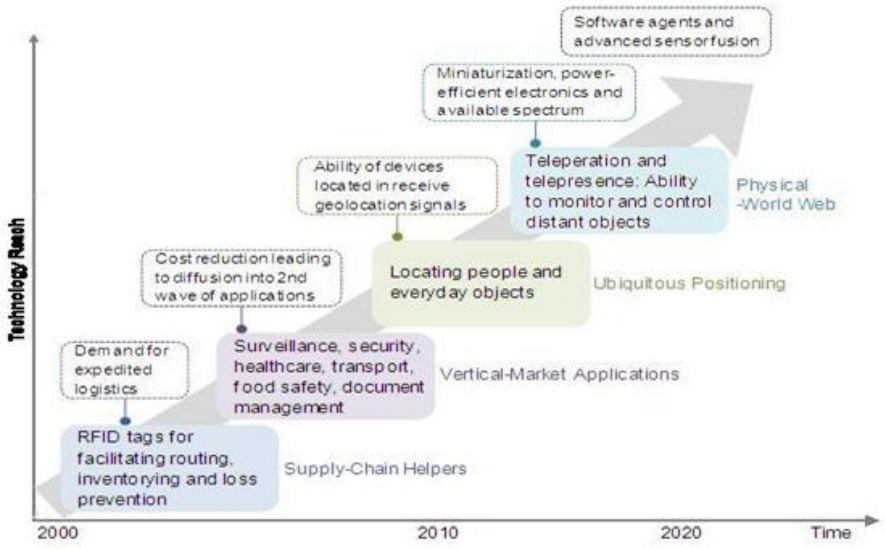
Όπως φαίνεται λοιπόν, από τότε που εμφανίστηκε η τεχνολογία του Διαδικτύου Πραγμάτων οι αναζητήσεις αυξάνονται συνεχώς, ενώ αυτές για τα Wireless Sensor Networks καθώς και για το Ubiquitous Computing ολοένα και μειώνονται.



Εικόνα 1.3: Δημοτικότητα αναζητήσεων όρων σχετικών με το IoT

Για τη λειτουργία των συστημάτων του Διαδικτύου Πραγμάτων, είναι απαραίτητο να αναφερθούν οι τεχνολογίες οι οποίες συντελούν σε αυτό. Είναι σημαντική η ύπαρξη τεχνολογιών που έχουν τη δυνατότητα συλλογής πληροφοριών από το περιβάλλον, τεχνολογιών που δίνουν τη δυνατότητα στις συσκευές να επεξεργαστούν τις πληροφορίες που έχουν συλλέξει από το περιβάλλον και τεχνολογιών που μπορούν να βελτιώσουν την ασφάλεια και την ιδιωτικότητα. Τα δύο πρώτα είναι αναπόσπαστα κομμάτια που προσδίδουν την «εξυπνάδα» στα αντικείμενα που παίρνουν μέρος στο Διαδίκτυο Πραγμάτων και ταυτόχρονα η ειδοποιός διαφορά από το Internet που είναι ευρέως γνωστό σήμερα.

Το τελευταίο, αν και όχι λειτουργικό κομμάτι, είναι σημαντική απαίτηση για να αποκτήσει το Διαδίκτυο Πραγμάτων τη διεισδυτικότητα για την οποία προορίζεται.



1.4 Technology roadmap: the Internet of Things

1.1.2. Ορισμός Ιδιωτικότητας

Η ιδιωτικότητα ως κοινωνικό και νομικό ζήτημα αποτέλεσε για πολύ καιρό μια από τις μεγαλύτερες ανησυχίες των κοινωνικών επιστημόνων, φιλοσόφων, και δικηγόρων. Μετά την άφιξη των υπολογιστών και των αυξανόμενων ικανοτήτων των σύγχρονων πληροφοριακών συστημάτων και δικτύων επικοινωνίας, η προσωπική ιδιωτικότητα κινδυνεύει όλο και περισσότερο, ειδικότερα τώρα, στη σύγχρονη εποχή, που οδεύουμε σε μια παγκόσμια κοινωνία πληροφοριών Η ιδιωτικότητα ως θεμελιώδες ανθρώπινο δικαίωμα που αναγνωρίστηκε στη Διακήρυξη των Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών, στο διεθνές Συνέδριο για τα Αστικά και Πολιτικά Δικαιώματα και σε πολλές άλλες διεθνείς και περιφερειακές συνθήκες [PI/EPIC 1999], πρέπει να προστατεύεται σε μια δημοκρατική κοινωνία. Γενικά, η ευθύνη της προστασίας της ιδιωτικότητας επιχειρείται από τα κάτωθι:

- Τους νόμους για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, οι οποίοι προωθούνται από την κυβέρνηση.
- Την αυτορρύθμιση από τους κώδικες δεοντολογίας σχετικά με τις δίκαιες πρακτικές πάνω σε πληροφορίες, που προωθούνται από τις επιχειρήσεις.
- Τις τεχνολογίες ενίσχυσης της ιδιωτικότητας που υιοθετούνται από τα άτομα.
- Την εκπαίδευση των καταναλωτών και των επαγγελματιών Πληροφορικής, σχετικά με την ιδιωτικότητα.

Ο πρώτος ορισμός της ιδιωτικότητας δόθηκε από τον Samuel D.Warren και τον Louis D.Brandeis στο περίφημο άρθρο τους “Το Δικαίωμα στην Ιδιωτικότητα” (“The Right to Privacy”). Οι δύο Αμερικανοί δικηγόροι καθόρισαν την ιδιωτικότητα ως “το δικαίωμα να είσαι μόνος”. Ο λόγος για αυτήν τη δημοσίευση ήταν η ανάπτυξη νέων μορφών τεχνολογιών που συνδέθηκε με άλλες εξελίξεις. Οι φωτογραφίες, για παράδειγμα, που χρησιμοποιούνταν από τον Κίτρινο Τύπο ήταν, σύμφωνα με την άποψη των συντακτών, μια επίθεση στην προσωπική μυστικότητα σύμφωνα με την άποψη του δικαιώματος να είσαι μόνος.

Ο πιο συνήθης ορισμός της ιδιωτικότητας που χρησιμοποιείται τώρα, είναι αυτός από τον Alan Westin: “Η ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων, να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους” [Westin 1967].

Σύμφωνα με τον ορισμό του Westin, τα φυσικά (άτομα) καθώς επίσης και τα νομικά πρόσωπα (ομάδες και ιδρύματα), έχουν δικαίωμα στην ιδιωτικότητα. Σε μερικές χώρες,

όπως στη Γαλλία, στην Αυστρία, στη Δανία, η δικαστική έννοια της προστασίας της ιδιωτικότητας επεκτείνεται στις ομάδες και στα ιδρύματα, ενώ στις περισσότερες άλλες, όπως στη Γερμανία, στις Η.Π.Α. ή στο Ηνωμένο Βασίλειο, περιορίζεται στα άτομα.
Γενικά, η έννοια της ιδιωτικότητας χωρίζεται σε τρεις μορφές:

- Εδαφική ιδιωτικότητα, που αφορά την προστασία της στενής φυσικής περιοχής που περιβάλλει ένα πρόσωπο, δηλαδή οικιακά και άλλα περιβάλλοντα όπως ο εργασιακός ή ο δημόσιος χώρος.
- Ιδιωτικότητα του ατόμου, που αφορά την προστασία ενός προσώπου από την αδικαιολόγητη παρέμβαση, όπως ο σωματικός έλεγχος, η δοκιμή φαρμάκων ή οι πληροφορίες που παραβιάζουν την ηθική αίσθησή του ατόμου.
- Πληροφοριακή ιδιωτικότητα, που αφορά τον έλεγχο του αν και πώς τα προσωπικά στοιχεία μπορούν να συγκεντρωθούν, να αποθηκευτούν, να υποστούν επεξεργασία ή να διαδοθούν επιλεκτικά.

Όταν λέμε Προσωπικά Δεδομένα, εννοούμε όλες τις πληροφορίες που αφορούν τις προσωπικές ή υλικές περιστάσεις ενός αναγνωρισμένου ή αναγνωρίσιμου προσώπου. Η προσωπική πληροφοριακή ιδιωτικότητα, έχει επίσης οριστεί από το Γερμανικό Συνταγματικό Δικαστήριο, στην Απόφαση Απογραφής του, το 1983, με τον όρο “το δικαίωμα της πληροφοριακής αυτοδιάθεσης”, που σημαίνει “το δικαίωμα ενός ατόμου να αποφασίσει για την αποκάλυψη και χρήση των προσωπικών του δεδομένων εκ πεποιθήσεως, κατά τη δική του κρίση”.

Η προστασία των δεδομένων, είναι η προστασία των προσωπικών δεδομένων, με σκοπό να εξασφαλιστεί η ιδιωτικότητα και αποτελεί ένα μόνο μέρος της έννοιας αυτής. Η ιδιωτικότητα, ωστόσο, δεν είναι ένα απεριόριστο και απόλυτο δικαίωμα, καθώς μπορεί να έρθει σε σύγκρουση με άλλα δικαιώματα ή νομικές αξίες, αλλά και επειδή τα άτομα δεν μπορούν να συμμετέχουν πλήρως στην κοινωνία χωρίς να αποκαλύπτουν κάποια από τα προσωπικά τους δεδομένα. Οι νόμοι Προστασίας της Ιδιωτικότητας και των Δεδομένων, μπορούν να βοηθήσουν στην προστασία των δικαιωμάτων ιδιωτικότητας, μόνο όταν γίνεται συλλογή, αποθήκευση ή επεξεργασία προσωπικών δεδομένων.

1.1.2.1. Βασικές Αρχές της Ιδιωτικότητας

Προκειμένου να προστατευθεί το δικαίωμα της πληροφοριακής αυτοδιάθεσης, οι εθνικοί νόμοι ιδιωτικότητας, οι κώδικες δεοντολογίας, οι κώδικες ηθικής των διαφόρων computer societies, καθώς επίσης και οι διεθνείς οδηγίες ή οι οδηγίες ιδιωτικότητας, απαιτούν την εξασφάλιση κάποιων βασικών αρχών ιδιωτικότητας, όταν πρόκειται να γίνει συλλογή ή επεξεργασία προσωπικών δεδομένων.

Οι περισσότερες από αυτές τις απαιτήσεις ιδιωτικότητας, διατυπώθηκαν επίσης από το Γερμανικό Συνταγματικό Δικαστήριο και είναι επιβεβλημένες από τον Γερμανικό Ομοσπονδιακό Νόμο Προστασίας των Δεδομένων, τις περισσότερες άλλες δυτικές πράξεις προστασίας των δεδομένων, την Οδηγία της Ευρωπαϊκής Ένωσης για την Προστασία των Δεδομένων, τις οδηγίες των Ηνωμένων Εθνών και (ως επί το πλείστον) από τις οδηγίες του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (Organization for Economic Cooperation and Development). Οι σημαντικότερες από αυτές τις αρχές ιδιωτικότητας είναι οι παρακάτω:

- **Αρχή της νομιμότητας και της δικαιοσύνης:** Τα προσωπικά δεδομένα θα πρέπει να συλλέγονται και να υπόκεινται σε επεξεργασία με δίκαιο και νόμιμο τρόπο.
- **Αρχή της προδιαγραφής και της αντιστοίχησης σκοπού (επίσης αποκαλούμενης και ως αρχή του περιορισμού σκοπού):** Οι σκοποί για τους οποίους πρόκειται να γίνει συλλογή και επεξεργασία προσωπικών δεδομένων, θα πρέπει να διευκρινίζονται και να είναι νόμιμοι. Η επακόλουθη χρήση των προσωπικών δεδομένων, περιορίζεται στους συγκεκριμένους σκοπούς, εκτός και αν υπάρχει ενημερωμένη συγκατάθεση από το άτομο στο οποίο ανήκουν τα δεδομένα.
- **Αρχή της αναγκαιότητας συλλογής και επεξεργασίας δεδομένων:** Η συλλογή και επεξεργασία των προσωπικών δεδομένων θα πρέπει να επιτρέπεται, μόνο αν είναι απαραίτητη για την επίτευξη των στόχων που εμπίπτουν στην ευθύνη της αρχής που τα συλλέγει και τα επεξεργάζεται.
- **Πληροφόρηση, ειδοποίηση και δικαιώματα πρόσβασης στα άτομα στα οποία ανήκουν τα δεδομένα:** Τα άτομα στα οποία ανήκουν τα δεδομένα, έχουν το δικαίωμα στην πληροφόρηση και στην ειδοποίηση, καθώς και το δικαίωμα στη διόρθωση, διαγραφή ή μπλοκάρισμα ανακριβών ή παράνομα αποθηκευμένων δεδομένων. Αυτά τα δικαιώματα δεν πρέπει να εξαιρεθούν ή να περιοριστούν από μια νομική συναλλαγή. Τα δικαιώματα στην πληροφόρηση και ειδοποίηση, βοηθούν στην παροχή διαφάνειας στην επεξεργασία δεδομένων.

- **Αρχή της ασφάλειας και της ακρίβειας:** Οι κατάλληλοι τεχνικοί και οργανωτικοί μηχανισμοί ασφάλειας θα πρέπει να ληφθούν, για να εξασφαλιστούν η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των προσωπικών δεδομένων. Τα προσωπικά δεδομένα θα πρέπει να κρατούνται ακριβή, κατάλληλα και ενημερωμένα, διαρκώς.
- **Επίβλεψη και κυρώσεις:** Μια ανεξάρτητη αρχή προστασίας των δεδομένων (επίσης αποκαλούμενη και ως αρχή επιτήρησης, επίτροπος προστασίας των δεδομένων ή διαμεσολαβητής), θα πρέπει να διοριστεί και να είναι υπεύθυνη για την επίβλεψη της τήρησης των παροχών ιδιωτικότητας. Σε περίπτωση παραβίασης των διατάξεων της νομοθεσίας περί ιδιωτικότητας, θα πρέπει να επιβάλλονται ποινικές ή άλλες κυρώσεις.

Σύμφωνα με την αρχή της ιδιωτικότητας για την αναγκαιότητα συλλογής και επεξεργασίας δεδομένων, τα προσωπικά δεδομένα δεν θα πρέπει να συλλέγονται ή να χρησιμοποιούνται για σκοπούς αναγνώρισης, όταν δεν είναι πραγματικά απαραίτητο. Συνεπώς, τα πληροφοριακά συστήματα θα πρέπει να εγγυώνται, αν αυτό είναι δυνατόν, ότι οι χρήστες θα μπορούν να ενεργούν και ανώνυμα. Η καλύτερη σχεδιαστική στρατηγική για να επιβληθεί αυτή η απαίτηση, είναι η αποφυγή ή (τουλάχιστον) η ελαχιστοποίηση των προσωπικών δεδομένων. Κατά συνέπεια, η απαίτηση για τεχνολογίες που ενισχύουν την ιδιωτικότητα, στην πραγματικότητα προέρχονται από τη βασική αρχή της ιδιωτικότητας για την αναγκαιότητα της συλλογής και επεξεργασίας δεδομένων.

1.1.3. Ορισμός Ασφάλειας

Η έννοια της ασφάλειας ενός πληροφοριακού συστήματος σχετίζεται με την ικανότητα ενός οργανισμού:

- να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του
- Να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν.

Στον όρο «**Ασφάλεια**» μπορούν να αποδοθούν πολλές ερμηνείες, κάθε μία από τις οποίες μπορεί να αποδώσει με ακρίβεια διαφορετικές καταστάσεις. Σύμφωνα με τον ορισμό του λεξικού της Οξφόρδης, «ασφάλεια είναι η ελευθερία από τον κίνδυνο ή το

φόβο». Διάφοροι άλλοι ορισμοί μπορούν να χρησιμοποιηθούν για να προσδιορίσουν την ασφάλεια όπως (βλ.λεξικό Μπαμπινιώτη):

- Η κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, όπου αισθάνεται κανείς ότι δεν απειλείται.
- Η αποτροπή κινδύνου ή απειλής, η εξασφάλιση σιγουριάς και βεβαιότητας.
- Υπηρεσία της Αστυνομίας.
- Ηλεκτρική διάταξη που αποτρέπει πιθανά ατυχήματα.
- Μηχανισμός στην πόρτα αυτοκινήτου.
- Συμφωνία μεταξύ ασφαλιστικής εταιρείας και πελάτη.
- Ιατροφαρμακευτική περίθαλψη.

Από μία πρακτική άποψη, η ασφάλεια μπορεί να έγκειται στην επαρκή προστασία ανθρώπων και αγαθών, για την οποία μπορεί να λαμβάνονται διάφορα μέτρα προστασίας από πιθανούς κινδύνους. Για παράδειγμα, η φυσική ασφάλεια ενός κτηρίου έγκειται στην αποτροπή εισόδου κακόβουλων ατόμων και στην αποτροπή ζημιών από φυσικές καταστροφές. Αντίστοιχα, η ασφάλεια μίας ηλεκτρονικής βάσης δεδομένων έγκειται στην προστασία των δεδομένων από καταστροφή, διαγραφή, αλλοίωση ή αποκάλυψη σε μη εξουσιοδοτημένους χρήστες.

Η Ασφάλεια Τεχνολογίας Πληροφορίας και Επικοινωνιών – **ασφάλεια ΤΠΕ** (Information and Communication Technology Security – **ICT Security**) περιλαμβάνει την ασφάλεια:

- Των υπολογιστικών συστημάτων και εφαρμογών, δηλαδή την προστασία από μη εξουσιοδοτημένες ενέργειες όπως αλλαγή δικαιωμάτων πρόσβασης, κακόβουλη εκτέλεση εντολών, τροποποίηση της διάρθρωσης του συστήματος, κακόβουλη ή λανθασμένη χρήση, διακοπή λειτουργίας, καθώς και τη φυσική προστασία των υπολογιστικών συστημάτων.
- Των δικτύων και των υποδομών, δηλαδή την προστασία από μη εξουσιοδοτημένη λογική πρόσβαση σε ένα δίκτυο, παράκαμψη ή τροποποίηση των κανόνων δρομολόγησης στο δίκτυο, παρακολούθηση του μέσου επικοινωνίας, διακοπή της επικοινωνίας, φυσική προστασία των υποδομών επικοινωνίας κτλ.
- Των πληροφοριών, δηλαδή την προστασία των δεδομένων ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους.

Το παρακάτω σχήμα επεξηγεί τη σχέση των διαφόρων τμημάτων της Ασφάλειας Τεχνολογίας Πληροφορίας και Επικοινωνιών.

Εικόνα 1.5: Σχέση διαφόρων τμημάτων της Ασφάλειας Τεχνολογίας Πληροφορίας και Επικοινωνιών.

Η επιστήμη της Ασφάλειας Υπολογιστών σχετίζεται με ένα πλήθος γνωστικών αντικειμένων, θεωριών και τεχνολογιών που σκοπό έχουν: “Την πρόληψη, ανίχνευση και αντιμετώπιση μη εξουσιοδοτημένων πράξεων, οι οποίες σχετίζονται με τη χρήση υπολογιστικών συστημάτων”.

Ο ρόλος του Η/Υ κατά την εκτέλεση των μη εξουσιοδοτημένων πράξεων συνήθως είναι διττός:

- Αποτελεί βασικό εργαλείο (αλλά όχι πάντα αποκλειστικό) για την τέλεση τους,
- Ο ίδιος ο Η/Υ (και συγκεκριμένα τα δεδομένα ή/και οι πληροφορίες που περιέχονται ή δημιουργούνται σε αυτόν) αποτελεί στόχο των πράξεων αυτών.

Οι μη εξουσιοδοτημένες πράξεις, ανάλογα με τις συνέπειες τους μπορούν να αποτελούν ή όχι ένα Ηλεκτρονικό Έγκλημα (e-crime, computer crime). Οι [Forester and Morrison, 1994] ορίζουν το Ηλεκτρονικό Έγκλημα ως: “Μία εγκληματική πράξη κατά την τέλεση της οποίας ο Η/Υ αποτελεί το βασικό εργαλείο”.

Η Ασφάλεια Υπολογιστών χρησιμοποιεί (χωρίς να περιορίζεται από) τη γνώση που πηγάζει από τη μελέτη αρκετών γνωστικών χώρων, όχι απαραίτητα αλληλοσυσχετιζόμενων, όπως η Πληροφορική, η Κρυπτογραφία και οι Κοινωνικές Επιστήμες. Συγκεκριμένα:

- **Πληροφορική**: Ανάπτυξη λογισμικού. Η γνώση βασικών τεχνικών προγραμματισμού κρίνεται απαραίτητη για την αντιμετώπιση των «εχθρών» του συστήματος (hackers, crackers κ.λ.π) οι οποίοι παράγουν κακόβουλο κώδικα με

σκοπό τη μη εξουσιοδοτημένη πρόσβαση στους πόρους του συστήματος ή εκμεταλλεύονται λάθη στον κώδικα των εφαρμογών του χρήστη-συστήματος. Διαχείριση Δικτύων-Internet & Τεχνολογίες Υλικού. Η κατανόηση των ηλεκτρονικών διατάξεων, των δικτυακών υποδομών, καθώς και των υπηρεσιών που τις χρησιμοποιούν (λογισμικό δικτύου, δικτυακές εφαρμογές και υπηρεσίες Internet, αρχιτεκτονικές πρωτόκολλων, κλπ.).

- **Κρυπτογραφία:** Η επιστήμη που ασχολείται με την προστασία της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας των δεδομένων και πληροφοριών κατά την αποθήκευση ή/και μεταφορά τους μεταξύ υπολογιστικών διατάξεων. Η κρυπτογραφία χρησιμοποιεί (χωρίς να περιορίζεται από) στοιχεία θεωρίας πληροφοριών (Information theory), μαθηματικά μοντέλα και στοιχεία θεωρίας γραμμικής άλγεβρας (linear algebra), θεωρίας αριθμών (number theory) κ.α., για το σχεδιασμό τεχνικών προστασίας των δεδομένων.

- **Κοινωνικές Επιστήμες:** Διοίκηση Ανθρώπινων Πόρων & Ψυχολογία. Η ασφάλεια αξιοποιεί βασικές γνώσεις της θεωρίας της ψυχολογίας (π.χ. προφίλ επιτιθέμενου & αμυνόμενου).

- **Δίκαιο και Ηθική του Κυβερνοχώρου:** Η νομοθεσία αποτελεί ίσως το σημαντικότερο μη τεχνικό (non-technical) μέσο για την πρόληψη επιθέσεων στην ασφάλεια Η/Υ. Ωστόσο, ζητήματα όπως η ανωνυμία των χρηστών, η ελευθερία έκφρασης και η προστασία των πνευματικών δικαιωμάτων σχετίζονται σε μεγάλο βαθμό και με την αποκαλούμενη ως Ηθική του Κυβερνοχώρου (Cyber Ethics).

- **Ιστορία:** Η μελέτη των γεγονότων (στα στρατιωτικά και διπλωματικά μέτωπα) κατά τους Α’ και Β’ Παγκόσμιους πολέμους (κώδικες, επιθέσεις σε συστήματα κρυπτογράφησης επικοινωνιών) καθώς και η γνώση που απορρέει από τη μελέτη περιπτώσεων παραβίασης συστημάτων Η/Υ και επικοινωνιών από τα μέσα της δεκαετίας του 1980 και μετά (δημιουργία και εξάπλωση κακόβουλου λογισμικού)

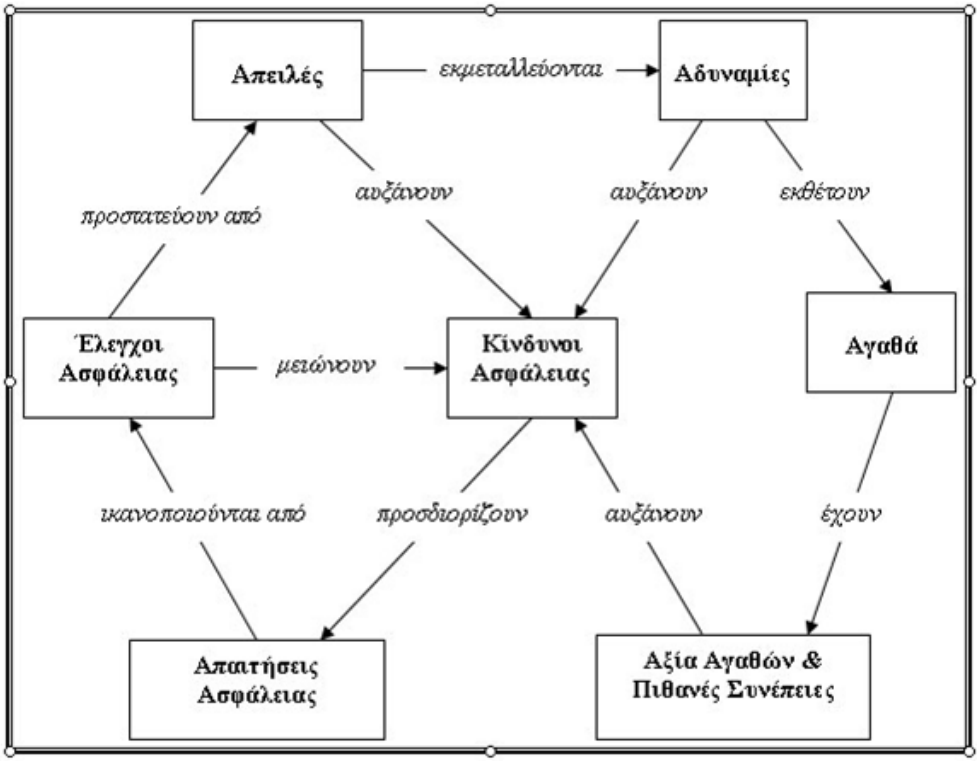
1.1.4. Η σχέση μεταξύ Ιδιωτικότητας και Ασφάλειας

Η έννοια της Πληροφοριακής Ιδιωτικότητας καθίσταται εξαιρετικά σημαντική στη διαχείριση και λειτουργία των πληροφοριακών συστημάτων, κυρίως εξαιτίας τόσο του

χαρακτήρα των εργασιών που επιτελούνται, όσο και του σημαντικού όγκου δεδομένων που συλλέγονται, επεξεργάζονται και αποθηκεύονται σε αυτά. Για την προστασία δεδομένων, η Ευρωπαϊκή Οδηγία 1995/46/ΕΚ ορίζει τις αρχές της νομιμότητας και της δικαιοσύνης, την αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν, την αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων, την αρχή της παροχής πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων, την αρχή της ασφάλειας και της ακεραιότητας, καθώς και την αρχή της εποπτείας και επικύρωσης. Είναι σημαντικό να τονίσουμε ότι μια επίθεση σε ένα πληροφοριακό σύστημα δεν προσβάλει απαραίτητα το απόρρητο της επεξεργασίας προσωπικών δεδομένων. Τα αντίμετρα προστασίας τα οποία χρησιμοποιεί ένα πληροφοριακό σύστημα πολλές φορές δεν καλύπτουν τις ανάγκες προστασίας και ενίσχυσης της ιδιωτικότητας.

Η προστασία της ιδιωτικότητας είναι ένα ζήτημα το οποίο πολλές φορές μπορεί να έρθει σε σύγκρουση με τη χρήση άλλων μηχανισμών ασφάλειας. Για παράδειγμα, σε ένα εργασιακό χώρο είναι πιθανό η εταιρική πολιτική να ορίζει τη χρήση κάμερας για επιτήρηση ενός χώρου, κάτι όμως το οποίο παραβιάζει την ιδιωτικότητα των εργαζομένων. Άλλη παρόμοια περίπτωση συμβαίνει με την αξιοποίηση της τεχνολογίας DRM (digital rights management), όπου μπορεί να γίνεται αξιοποίηση μηχανισμών προσδιορισμού ταυτότητας, καταγραφής ηλεκτρονικών ιχνών και κατά συνέπεια εντοπισμού των χρηστών. Η επιβολή της απαραίτητης ισορροπίας είναι μια δύσκολη υπόθεση, καθώς η πληροφορία αποτελεί ένα σημαντικό παράγοντα ανάπτυξης και εδραίωσης για κάθε οργανισμό ή κράτος. Σε κάθε περίπτωση, οι μηχανισμοί ασφάλειας που υλοποιούνται θα πρέπει να είναι συμβατοί με τις βασικές αρχές μιας δημοκρατικής κοινωνίας, όπως ορίζεται από τον ΟΟΣΑ: «Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency».

Μία από τις πιο συνήθεις προσλήψεις της έννοιας της ιδιωτικότητας είναι ότι αυτή συνίσταται στον απόρρητο χαρακτήρα ορισμένων ζητημάτων και υπό αυτήν την έννοια η ιδιωτικότητα προσβάλλεται με την αποκάλυψη απόρρητης πληροφορίας[i]. Ιδίως η «κλασική» προσέγγιση της ιδιωτικότητας ως refugium (καταφυγίου) παρουσιάζει στοιχεία ταύτισης ή και σύγχυσης με την έννοια του απορρήτου (secrecy) και της εμπιστευτικότητας (confidentiality).



Εικόνα 1.6: Σύνδεση όρων ανάλυσης και διαχείρισης κινδύνου.

Οι όροι αυτοί, αν και συχνά γίνονται αντιληπτοί και χρησιμοποιούνται ως ισοδύναμοι, εκφράζοντας σε τελευταία ανάλυση παρεμφερείς αξιώσεις προστασίας, εντούτοις δεν ταυτίζονται: Η έννοια του απόρρητου (secrecy) αναφέρεται είτε στη μη προσπελασιμότητα ορισμένων πληροφοριών που εμπίπτουν στη σφαίρα επιρροής ενός ατόμου είτε στο καθήκον ή την υποχρέωση προσώπων ή οργανισμών να διαφυλάσσουν πληροφορίες που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας γενικότερης σχέσης εμπιστοσύνης (όπως το ιατρικό απόρρητο ή το τραπεζικό απόρρητο) είτε τις κατέχουν επί τη βάσει της θέσης και της αρμοδιότητάς τους (όπως το υπηρεσιακό απόρρητο). Εάν μάλιστα πρόκειται για πληροφορία που εμπίπτει στη δημόσια σφαίρα δεν είναι νοητή η προστασία από το απόρρητο. Για να είναι απόρρητη/εμπιστευτική η πληροφορία θα πρέπει να είναι σε μία κατάσταση περιορισμένης προσβασιμότητας από πρόσωπα, ομάδες κ.λπ.

Το “απόρρητο” αποκλείει τους (περαιτέρω) τρίτους από τη γνώση, τη χρήση και αξιοποίηση των πληροφοριών, εφόσον δεν συντρέχει κάποιος νόμιμος λόγος και η αντίστοιχη διαδικασία που επιτρέπουν την άρση του απορρήτου. Αξίζει πάντως να σημειωθεί ότι σε ορισμένες έννομες τάξεις, όπως αυτή των ΗΠΑ, ήδη το γεγονός ότι ένα πρόσωπο εμπιστεύεται μία πληροφορία που το αφορά σε ένα άλλο πρόσωπο ή οργανισμό οδηγεί στη στέρηση της προστασίας που επιφυλάσσεται στην ιδιωτικότητα. Η άποψη αυτή συνδέεται με κρίσιμες για τα πρόσωπα συνέπειες, όπως π.χ. το εύρος και οι προϋποθέσεις για περαιτέρω κοινοποίηση των πληροφοριών αυτών. Το Supreme Court

(Ανώτατο Δικαστήριο των ΗΠΑ) έκρινε ότι ένα πρόσωπο δεν έχει εύλογη προσδοκία ιδιωτικότητας (reasonable expectation of privacy), όσον αφορά πληροφορίες που αποκάλυψε εθελοντικά σε ένα τρίτο πρόσωπο ή οργανισμό και στη συνέχεια διαβιβάστηκαν από αυτό σε μία δημόσια αρχή, ακόμη και εάν η πληροφορία δόθηκε αρχικά με την υπόθεση ότι θα χρησιμοποιηθεί για έναν περιορισμένο σκοπό (υποθέσεις US v. Miller, Smith v. Maryland). Στο σημείο αυτό εντοπίζεται μία βασική ατέλεια της επίκλησης της ιδιωτικότητας ως πληροφοριακής απομόνωσης: η χρησιμότητά της (και συνακόλουθα η προστασία του υπό συζήτηση αγαθού) εν τέλει παύει να υφίσταται κατά τη στιγμή που η πληροφορία “παραδίδεται” σε κάποιον άλλον, “διαφεύγει” από το πρόσωπο που αφορά και παύει να είναι “μυστική”.

Ως προς την ευρωπαϊκή προσέγγιση, ο απόρρητος χαρακτήρας των προσωπικών πληροφοριών δεν συνάγεται μόνο από τη φύση τους αλλά προβλέπεται και ρητά στο σχετικό κανονιστικό πλαίσιο. Το άρθρο 16 της Οδηγίας 95/46/ΕΚ για την προστασία προσωπικών δεδομένων περιέχει μία -ιδιότυπης αρνητικής διατύπωσης – ρύθμιση για το απόρρητο, καθώς ορίζει ότι όποιος επεξεργάζεται δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας ή του εκτελούντος επεξεργασία το πράττει μόνο κατ’ εντολή του υπεύθυνου επεξεργασίας. Ο ελληνικός νόμος για την προστασία προσωπικών δεδομένων (ν. 2472/97) στο άρθρο 10.1 περιέχει μεν μία ανάλογη διατύπωση αλλά ταυτόχρονα προσδιορίζει συνολικά την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως απόρρητη.

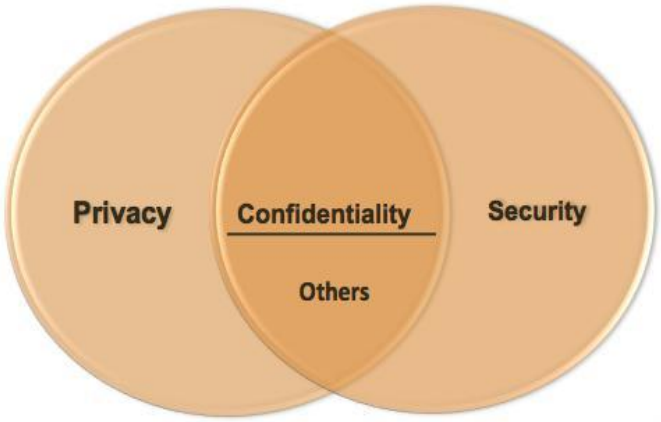
Το απόρρητο υπό την έννοια της εμπιστευτικότητας σχετίζεται επίσης με την ασφάλεια των πληροφοριών (information security) αλλά δεν ταυτίζεται με αυτή. Η ασφάλεια της πληροφορίας δεν εξυπηρετείται μόνο από την εγγύηση της εμπιστευτικότητας. Η εμπιστευτικότητα αποτελεί μόνο μία από τις παραμέτρους που συγκροτούν την ασφάλεια των πληροφοριών, στην οποία περιλαμβάνεται η εγκυρότητα, η αυθεντικότητα, η ακεραιότητα και η διαθεσιμότητα. Η ασφάλεια προϋποθέτει ένα οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευτούν τα στοιχεία ενός πληροφοριακού συστήματος και προφανώς δεν διασφαλίζεται μόνο, ίσως ούτε καν κυρίως, από νομικές επιταγές.

Σε κάθε περίπτωση, τόσο η κοινοτική όσο και η ελληνική νομοθεσία για την προστασία προσωπικών δεδομένων απαιτούν τη λήψη «κατάλληλων» μέτρων ασφάλειας, ώστε να προστατεύονται τα δεδομένα από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Ο νομοθέτης επάγει μάλιστα στον υπεύθυνο επεξεργασίας την υποχρέωση

να εξασφαλίζει επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων. Αξίζει να επισημανθεί ότι ο Έλληνας νομοθέτης συνδέει την υποχρέωση της εμπιστευτικότητας με τις υπόλοιπες διαστάσεις της ασφάλειας, επιλέγοντας μάλιστα να περιλάβει τις υποχρεώσεις απορρήτου και ασφαλείας σε ένα άρθρο (άρθρο 10 ν. 2472/97).

Η ιδιωτικοτητα δεν ταυτίζεται με την ασφάλεια ως έννοιες, μια βάση δεδομένων με προσωπικά στοιχεία μπορεί να σχεδιαστεί με όση ασφάλεια απαιτείται, ωστόσο αυτό δεν σημαίνει ότι δεν μπορεί να παραβιάζει την ιδιωτικότητα των ατόμων που τα στοιχεία τους βρίσκονται εκεί, πχ αν δεν έχουν συλλεχθεί με διαφάνεια και με την σύμφωνη γνώμη τους και πραγματικά γιατί εξυπηρετούν κάποια ανάγκη.

Τελικά υπάρχει αμοιβαία σχέση μεταξύ **Ασφάλειας** και **Ιδιωτικότητας**, αυτή ονομάζεται **Εμπιστευτικότητα** και βρίσκεται στην τομή των εννοιών της Ασφάλειας και της Ιδιωτικότητας.



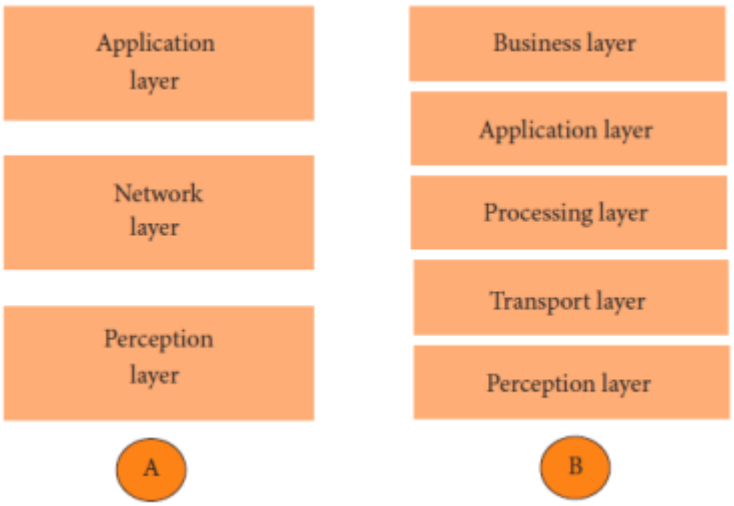
Εικόνα 1.7: Εμπιστευτικότητα, η τομή μεταξύ Ασφάλειας και Ιδιωτικότητας.

2. Διαδίκτυο Πραγμάτων (IoT)

2.1. Αρχιτεκτονική Διαδικτύου Πραγμάτων

Δεν υπάρχει κοινή συναίνεση σχετικά με την αρχιτεκτονική για το Διαδίκτυο Πραγμάτων, η οποία να συμφωνείται σε παγκόσμιο επίπεδο. Διαφορετικές αρχιτεκτονικές έχουν προταθεί από διάφορους ερευνητές.

2.1.1. Αρχιτεκτονική τριών και πέντε επιπέδων



Εικόνα 2.1 Αρχιτεκτοντική του IoT. Α) 3 επιπέδων και Β) 5 επιπέδων

Η πιο βασική αρχιτεκτονική είναι η τριών επιπέδων όπως φαίνεται στην Εικόνα 2.1. Εισήχθη στα αρχικά στάδια της έρευνας σε αυτόν τον τομέα. Έχει τρία επίπεδα, δηλαδή τα επίπεδα αντίληψης, δικτύου και εφαρμογών:

- Το **επίπεδο αντίληψης** είναι το φυσικό στρώμα, το οποίο διαθέτει αισθητήρες για την ανίχνευση και τη συλλογή πληροφοριών σχετικά με το περιβάλλον. Καταγράφει φυσικές παραμέτρους ή εντοπίζει άλλα έξυπνα αντικείμενα στο περιβάλλον.
- Το **επίπεδο δικτύου** είναι υπεύθυνο για τη σύνδεση με άλλα έξυπνα πράγματα, συσκευές δικτύου και servers. Τα χαρακτηριστικά του χρησιμοποιούνται επίσης για τη μετάδοση και την επεξεργασία δεδομένων από αισθητήρες.
- Το **επίπεδο εφαρμογής** είναι υπεύθυνο για την παροχή συγκεκριμένων υπηρεσιών εφαρμογής στον χρήστη. Ορίζει διάφορες εφαρμογές στις οποίες μπορεί να αναπτυχθεί το Διαδίκτυο Πραγμάτων, για παράδειγμα, έξυπνες κατοικίες, έξυπνες πόλεις και η έξυπνη υγεία.

Η αρχιτεκτονική των τριών επιπέδων ορίζει την κύρια ιδέα του Διαδικτύου Πραγμάτων, αλλά δεν αρκεί για την έρευνα μας, διότι η έρευνα συχνά επικεντρώνεται σε λεπτότερες πτυχές του. Αυτός είναι ο λόγος για τον οποίο προτείνουμε στη βιβλιογραφία πολυάριθμες πολυεπίπεδες αρχιτεκτονικές. Το ένα είναι η αρχιτεκτονική πέντε επιπέδων, η οποία περιλαμβάνει επιπλέον τα επίπεδα επεξεργασίας και επιχειρήσεων. Τα πέντε στρώματα είναι τα επίπεδα αντίληψης, μεταφοράς, επεξεργασίας, εφαρμογής και επιχειρήσεων. Ο ρόλος των επιπέδων αντίληψης και εφαρμογής είναι ο ίδιος με την αρχιτεκτονική με τρία στρώματα. Περιγράφουμε τη λειτουργία των υπόλοιπων τριών στρωμάτων.

- Το **στρώμα μεταφοράς** μεταφέρει τα δεδομένα αισθητήρα από το στρώμα αντίληψης στο στρώμα επεξεργασίας και αντίστροφα μέσω δικτύων όπως το wireless, το 3G, το LAN, το Bluetooth, το RFID και το NFC.
- Το **στρώμα επεξεργασίας** είναι επίσης γνωστό ως επίπεδο middleware. Αποθηκεύει, αναλύει και επεξεργάζεται τεράστια ποσά δεδομένων που προέρχονται από το στρώμα μεταφοράς. Μπορεί να διαχειρίζεται και να παρέχει ένα ποικίλο σύνολο υπηρεσιών στα χαμηλότερα επίπεδα. Χρησιμοποιεί πολλές τεχνολογίες, όπως βάσεις δεδομένων, cloud computing και big data modules.
- Το **επιχειρηματικό στρώμα** διαχειρίζεται όλο το σύστημα Διαδικτύου Πραγμάτων, συμπεριλαμβανομένων των εφαρμογών, των μοντέλων και κερδών, καθώς και της ιδιωτικότητας των χρηστών. Το επιχειρηματικό στρώμα δεν θα αναλυθεί περαιτέρω στην παρούσα εργασία.

Μια άλλη αρχιτεκτονική που προτείνεται από τον Ning και τον Wang εμπνέεται από τα στρώματα επεξεργασίας στον ανθρώπινο εγκέφαλο. Είναι εμπνευσμένο από τη νοημοσύνη και την ικανότητα των ανθρώπων να σκέφτονται, να αισθάνονται, να θυμούνται, να λαμβάνουν αποφάσεις και να αντιδρούν στο φυσικό περιβάλλον. Αποτελείται από τρία μέρη. Πρώτον, ο ανθρώπινος εγκέφαλος, ο οποίος είναι ανάλογος με τη μονάδα επεξεργασίας δεδομένων και διαχείρισης δεδομένων ή το κέντρο δεδομένων. Δεύτερο είναι ο νωτιαίος μυελός, ο οποίος είναι ανάλογος με το κατανεμημένο δίκτυο κόμβων επεξεργασίας δεδομένων και έξυπνων πυλών. Το τρίτο είναι το δίκτυο των νεύρων, το οποίο αντιστοιχεί στα στοιχεία δικτύωσης και τους αισθητήρες.

2.1.2. Αρχιτεκτονικές βασισμένες στο Cloud και το Fog

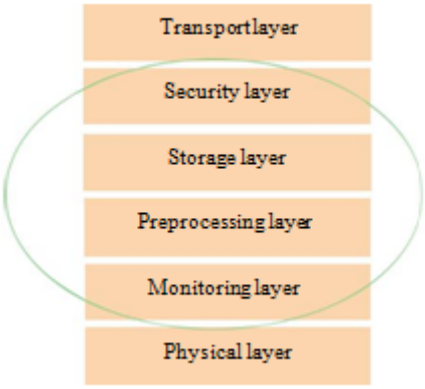
Ας δούμε τώρα δύο είδη αρχιτεκτονικών συστημάτων: το Cloud και το Fog. Να σημειωθεί ότι αυτή η ταξινόμηση είναι διαφορετική από την ταξινόμηση στην προηγούμενη ενότητα, η οποία έγινε με βάση τα πρωτόκολλα.

Τον τελευταίο καιρό υπάρχει μια κίνηση προς μια άλλη αρχιτεκτονική συστήματος, το fog computing, όπου οι αισθητήρες και οι πύλες δικτύου αποτελούν μέρος της επεξεργασίας δεδομένων και των αναλύσεων. Μια αρχιτεκτονική fog παρουσιάζει μία πολυεπίπεδη προσέγγιση όπως φαίνεται στην επόμενη εικόνα, το οποίο εισάγει στρώματα παρακολούθησης, προεπεξεργασίας, αποθήκευσης και ασφάλειας μεταξύ του φυσικού και του στρώματος μεταφοράς. Το επίπεδο παρακολούθησης παρακολουθεί την ισχύ, τους πόρους, τις απαντήσεις και τις υπηρεσίες.

Το στρώμα προεπεξεργασίας εκτελεί φιλτράρισμα, επεξεργασία και ανάλυση δεδομένων αισθητήρων. Το επίπεδο προσωρινής αποθήκευσης παρέχει λειτουργίες αποθήκευσης όπως αναπαραγωγή, διανομή και αποθήκευση δεδομένων. Τέλος, το επίπεδο ασφαλείας εκτελεί κρυπτογράφηση / αποκρυπτογράφηση και διασφαλίζει την ακεραιότητα και την ιδιωτικότητα των δεδομένων. Η παρακολούθηση και η προεπεξεργασία πραγματοποιούνται τελευταία πριν από την αποστολή δεδομένων στο cloud.

Συχνά οι όροι “fog computing” και “edge computing” χρησιμοποιούνται εναλλακτικά. Ο τελευταίος όρος προηγείται του πρώτου και θεωρείται ότι είναι γενικότερος. Το fog computing που ονομάστηκε έτσι από τη Cisco αναφέρεται σε έξυπνες πύλες και έξυπνους αισθητήρες, ενώ το edge computing είναι λίγο πιο διεισδυτικό. Αυτό το παράδειγμα προβλέπει την προσθήκη έξυπνων δυνατοτήτων προεπεξεργασίας δεδομένων σε φυσικές συσκευές όπως κινητήρες, αντλίες ή φώτα. Στόχος είναι να γίνει όσο το δυνατόν μεγαλύτερη δυνατή προεπεξεργασία δεδομένων σε αυτές τις συσκευές, οι οποίες βρίσκονται στην άκρη του δικτύου. Όσον αφορά την αρχιτεκτονική του συστήματος, το αρχιτεκτονικό διάγραμμα δεν διαφέρει αισθητά από την επόμενη Εικόνα. Ως εκ τούτου, δεν περιγράφουμε ξεχωριστά το edge computing.

Τέλος, η διάκριση μεταξύ αρχιτεκτονικών πρωτοκόλλων και αρχιτεκτονικών συστημάτων δεν είναι πολύ καθαρή. Συχνά τα πρωτόκολλα και το σύστημα κωδικοποιούνται. Θα χρησιμοποιήσουμε τη γενική αρχιτεκτονική Διαδικτύου Πραγμάτων των 3 επιπέδων στα επόμενα κεφάλαια.



Εικόνα 2.2 Fog αρχιτεκτονική μιας έξυπνης πύλης IoT

Βασικά στοιχεία

Σε ένα τυπικό κοινωνικό περιβάλλον Διαδικτύου Πραγμάτων, αντιμετωπίζουμε τις συσκευές και τις υπηρεσίες ως bots όπου μπορούν να δημιουργήσουν σχέσεις μεταξύ τους και να τις τροποποιήσουν με την πάροδο του χρόνου. Αυτό θα μας επιτρέψει να αφήσουμε αδιάλειπτα τις συσκευές να συνεργάζονται μεταξύ τους και να επιτύχουν ένα πολύπλοκο έργο. Για να γίνει ένα τέτοιο μοντέλο, πρέπει να έχουμε πολλά διαλειτουργικά στοιχεία. Ας δούμε μερικά από τα βασικά συστατικά ενός τέτοιου συστήματος.

1. **ID**: χρειαζόμαστε μια μοναδική μέθοδο αναγνώρισης αντικειμένων. Ένα ID μπορεί να αντιστοιχιστεί σε ένα αντικείμενο βασισμένο σε παραδοσιακές παραμέτρους, όπως το MAC ID, το IPv6 ID, ένας γενικός κωδικός προϊόντος ή κάποια άλλη προσαρμοσμένη μέθοδο.
2. **Μετα-πληροφόρηση**: μαζί με ένα ID, χρειαζόμαστε κάποια μετά-πληροφόρηση σχετικά με τη συσκευή που περιγράφει τη μορφή και τη λειτουργία της. Αυτό απαιτείται για να δημιουργηθούν οι κατάλληλες σχέσεις με τη συσκευή και επίσης να τοποθετηθεί κατάλληλα στο σύμπαν των συσκευών Διαδικτύου Πραγμάτων.
3. **Έλεγχοι ασφαλείας**: αυτό είναι παρόμοιο με τις ρυθμίσεις "φίλων" στο Facebook. Ένας κάτοχος μιας συσκευής ενδέχεται να θέτει περιορισμούς στα είδη συσκευών που μπορούν να συνδεθούν σε αυτό. Αυτά συνήθως αναφέρονται ως έλεγχοι ιδιοκτήτη.
4. **Ανακάλυψη υπηρεσίας**: ένα τέτοιο σύστημα είναι σαν ένα service cloud, όπου πρέπει να έχουμε ειδικούς καταλόγους που αποθηκεύουν λεπτομέρειες για συσκευές που παρέχουν ορισμένες υπηρεσίες. Γίνεται πολύ σημαντικό να είναι ενημερωμένοι αυτοί οι κατάλογοι ώστε οι συσκευές να μπορούν να μάθουν για άλλες συσκευές.

5. **Διαχείριση σχέσεων**: αυτή η ενότητα διαχειρίζεται σχέσεις με άλλες συσκευές. Επίσης, αποθηκεύει τους τύπους των συσκευών με τις οποίες μια συγκεκριμένη συσκευή πρέπει να προσπαθήσει να συνδεθεί με βάση τον τύπο των παρεχόμενων υπηρεσιών. Για παράδειγμα, έχει νόημα ένας light controller να μπορεί να κάνει μια σχέση με έναν light sensor.
6. **Σύνθεση υπηρεσίας**: αυτή η ενότητα μεταφέρει το μοντέλο κοινωνικού Διαδικτύου Πραγμάτων σε νέο επίπεδο. Ο απώτερος στόχος ενός τέτοιου συστήματος είναι η παροχή καλύτερων ολοκληρωμένων υπηρεσιών στους χρήστες. Για παράδειγμα, εάν ένα άτομο διαθέτει έναν αισθητήρα ισχύος με το κλιματιστικό του και αυτή η συσκευή δημιουργεί μια σχέση με μια μηχανή ανάλυσης (analytics engine), τότε είναι δυνατό να αποδοθούν πολλά δεδομένα σχετικά με τα μοντέλα χρήσης του κλιματιστικού αυτού. Αν το κοινωνικό μοντέλο είναι πιο εκτεταμένο και υπάρχουν πολλές περισσότερες συσκευές, τότε είναι δυνατόν να συγκρίνουμε τα δεδομένα με τα πρότυπα χρήσης άλλων χρηστών και να βρούμε ακόμη πιο σημαντικά δεδομένα. Για παράδειγμα, οι χρήστες μπορούν να μάθουν αν είναι οι μεγαλύτεροι καταναλωτές ενέργειας στην κοινότητά τους ή στους φίλους τους στο Facebook.

2.2. Συστατικά του Διαδικτύου Πραγμάτων

Εδώ θα παρουσιάσουμε, από μία υψηλού επιπέδου οπτική, μια ταξινόμηση των στοιχείων που θεωρούνται απαραίτητα για την ανάπτυξη του Διαδικτύου Πραγμάτων και τα οποία είναι συνοπτικά :

- **Τα υλικά συστατικά του Διαδικτύου Πραγμάτων.** Φυσικά αντικείμενα (π.χ. φυσικές συσκευές) που συλλέγουν, εντοπίζουν και παρακολουθούν πληροφορίες σχετικά π.χ. με άτομα με ειδικές ανάγκες στο περιβάλλον τους. Οι φυσικές συσκευές συνδέονται με το Διαδίκτυο και μετατρέπουν τις πληροφορίες που λαμβάνονται στον φυσικό κόσμο σε δεδομένα για τον ψηφιακό κόσμο.
- **Το επίπεδο επικοινωνίας του Διαδικτύου Πραγμάτων**. Σε αυτήν την ενότητα θα παρουσιαστούν οι τεχνολογίες δικτύου που μπορούν να βοηθήσουν στην μεγάλης κλίμακας ανάπτυξη του Διαδικτύου Πραγμάτων. Στη σημερινή εποχή πλέον έχουμε να διαλέξουμε από μια πολύ μεγάλη γκάμα τεχνολογιών όπως ethernet, bluetooth, zigbee, z-wave, wifi, UMTS/LTE, Dash7 κοκ
- **Το επίπεδο εφαρμογών του Διαδικτύου Πραγμάτων** υλοποιεί τους βασικούς τομείς δικτύωσης και δράσης μέσω διαφόρων platforms, embedded συστημάτων, partner συστημάτων καθώς και middleware. Αυτές οι εφαρμογές είναι υπεύθυνες

για τη συλλογή δεδομένων, την ενσωμάτωση συσκευών, την ανάλυση σε πραγματικό χρόνο και την επέκταση εφαρμογής και διαδικασίας στο δίκτυο Διαδικτύου Πραγμάτων. Ολοκληρώνονται με κρίσιμα επιχειρηματικά συστήματα (π.χ. συστήματα παραγγελιών, ρομποτική, προγραμματισμό και άλλα) κατά την εκτέλεση των σχετικών εργασιών.

2.2.1. Τα υλικά συστατικά του Διαδικτύου Πραγμάτων

Για να γίνει αντιληπτός ο ορισμός του Διαδικτύου Πραγμάτων, πρέπει αρχικά να οριστεί το είδος των αντικειμένων/συσκευών που θα δικτυωθούν. Για τη δημιουργία των αντικειμένων όπως παρουσιάζεται και στη προηγούμενη παράγραφο χρησιμοποιείται η υπάρχουσα φτηνή και ευρέως γνωστή τεχνολογία (**RFID tags, sensors, μικροεπεξεργαστές** κτλ). Παρακάτω δίδεται ο ορισμός των αντικείμενων που θα χρησιμοποιηθούν.

Τα έξυπνα αντικείμενα (**smart objects**) ή οι έξυπνες συσκευές δεν είναι απλά αισθητήρες ανίχνευσης (**sensors**), αλλά χρησιμοποιούν την απαραίτητη τεχνολογία (**RFID tags**, **sensors**, **μικροεπεξεργαστές**) ώστε να ανασχηματιστούν από συσκευές με μία λειτουργία, σε εργαλεία με τα οποία ο χρήστης μπορεί να αλληλεπιδράσει και των οποίων η κύρια λειτουργία είναι να βοηθούν τους ανθρώπους στις καθημερινές τους ανάγκες. Ο χαρακτηρισμός των παραπάνω αντικειμένων με τον όρο «έξυπνα» δεν είναι τυχαίος και οφείλεται ακριβώς στη δυνατότητα τους και για την μεταξύ τους επικοινωνία αλλά και με τον εκάστοτε χρήστη.

Επομένως τα αντικείμενα αυτά δεν αποτελούν μόνο άλλη μια τεχνολογική συσκευή με βελτιωμένα τεχνικά χαρακτηριστικά, αλλά η αλληλεπίδραση με το εξωτερικό περιβάλλον είναι που αποδίδει στα έξυπνα αντικείμενα υβριδική φύση ή με αλλά λόγια μπορούν να θεωρηθούν ως μηχανές με δύο υποστάσεις, δηλαδή είναι οντότητες με φυσική αλλά και ψηφιακή μορφή.

Λειτουργίες «Έξυπνων» Συσκευών

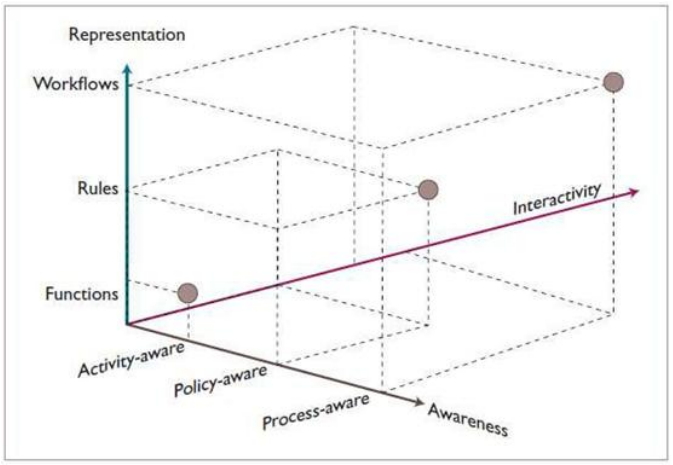
Για να μπορέσουν οι έξυπνες συσκευές να επικοινωνήσουν μεταξύ τους αλλά και να αλληλεπιδράσουν με τον άνθρωπο οι παραπάνω συσκευές θα πρέπει από αρχιτεκτονικής πλευράς να χαρακτηρίζονται από τις παρακάτω στοιχειώδεις λειτουργίες:

- **Αντίληψη (Awareness).** Η συγκεκριμένη λειτουργία αναφέρεται στη αναγκαία ικανότητα που πρέπει να έχουν τα έξυπνα αντικείμενα ώστε να μπορούν να ανιχνεύουν, να ερμηνεύουν, και να ανταποκρίνονται σε ερεθίσματα από γεγονότα ή

από την ανθρώπινη δραστηριότητα. Γενικά να είναι σε θέση να αντιλαμβάνονται το περιβάλλον που βρίσκονται.

- **Απεικόνιση (Representation).** Η λειτουργία της απεικόνισης αναφέρεται στα προγράμματα και τις εφαρμογές τα οποία υλοποιούνται από το υλικό της ηλεκτρονικής συσκευής.
- **Αλληλεπίδραση (Interaction).** Τέλος, η λειτουργία της αλληλεπίδρασης δηλώνει την ικανότητα του αντικειμένου να αλληλεπιδρά με το χρήστη όσον αφορά την εισαγωγή δεδομένων και την παρουσίαση των ζητούμενων αποτελεσμάτων. Επιπλέον αναφέρεται και στη δημιουργία ροής ελέγχου της συσκευής, όπως και την ανάδραση (feedback) της συσκευής προς το χρήστη.

Στο παρακάτω διάγραμμα παρουσιάζονται οι παραπάνω τρεις στοιχειώδεις λειτουργίες σε ένα ορθοκανονικό σύστημα συντεταγμένων.

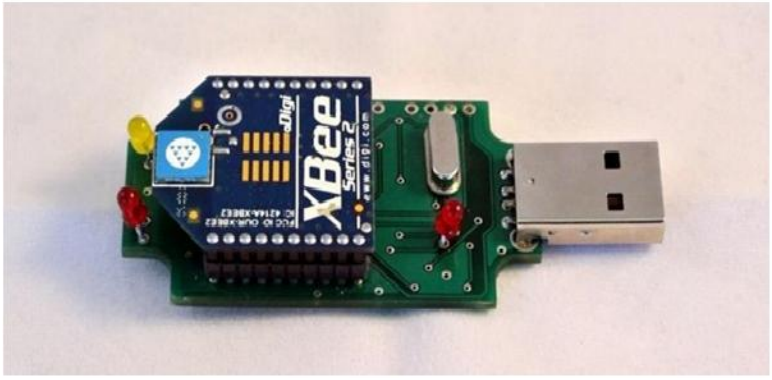


Εικόνα 2.3 Οι 3 διαστάσεις των "έξυπνων" αντικειμένων

Ο χωρισμός και η διάκριση μεταξύ των λειτουργιών οδηγεί σε μία δομημένη και εύκολη λύση για το σχεδιασμό «έξυπνων» αντικειμένων. Η κατάλληλη χρήση και ανάλυση των τριών λειτουργιών εξαρτάται από τις απαιτήσεις των εφαρμογών, έτσι ώστε να μπορούν να παρέχονται επιλογές και εναλλακτικές για κάθε περίσταση. Συμπερασματικά δε θα ήταν ανούσιο να αναφερθεί ότι τα παραπάνω αντικείμενα μπορούν να χαρακτηριστούν ως ανθρωποκεντρικά, έχοντας όντας ως βασική τους αρχή την αλληλεπίδραση με τον άνθρωπο και την εξυπηρέτηση των απαιτούμενων αναγκών του.

2.2.1.1. Αισθητήρες Διαδικτύου Πραγμάτων

Το πιο σημαντικό υλικό στο Διαδίκτυο Πραγμάτων είναι οι αισθητήρες του. Αυτές οι συσκευές αποτελούνται από μονάδες ενέργειας, μονάδες διαχείρισης ισχύος, μονάδες RF και αισθητήρες. Οι μονάδες RF διαχειρίζονται τις επικοινωνίες μέσω της επεξεργασίας σημάτων, WiFi, ZigBee, Bluetooth, duplexers και BAW.



Η μονάδα ανίχνευσης διαχειρίζεται την ανίχνευση μέσω διαφόρων ενεργών και παθητικών συσκευών μέτρησης. Ακολουθεί μια λίστα με μερικές από τις συσκευές μέτρησης που χρησιμοποιούνται στο Διαδίκτυο Πραγμάτων.

Συσκευές	
επιταχυνσιόμετρα	αισθητήρες θερμοκρασίας
μαγνητόμετρα	αισθητήρες εγγύτητας
γυροσκόπια	αισθητήρες εικόνας
ακουστικοί αισθητήρες	αισθητήρες φωτός
αισθητήρες πίεσης	αισθητήρες RFID αερίων
αισθητήρες υγρασίας	αισθητήρες μικρο-ροής

Εικόνα 2.4 Λίστα αισθητήρων.

Αισθητήρες RFID

Η τεχνολογία RFID (**R**adio **F**requency **Id**entification) χρησιμοποιείται για την αυτοματοποιημένη ανίχνευση αντικειμένων και ανθρώπων και είναι μια μετεξέλιξη του κλασικού γραμμωτού κώδικα (barcode). Μια συσκευή RFID, που επιπλέον ονομάζεται ετικέτα RFID (**RFID tag**), είναι ένας μικρός επεξεργαστής ο οποίος έχει σχεδιαστεί να μεταδίδει δεδομένα ασύρματα. Η στοιχειώδης λειτουργία του είναι να μεταδίδει δεδομένα (απαντήσεις) σε τυχόν ερωτήσεις από μία συσκευή ανάγνωσης (RFID Reader).

Οι ετικέτες RFID μπορούν να είναι παθητικές, ενεργητικές ή παθητικές με μπαταρία. Μια ενεργητική ετικέτα διαθέτει ενσωματωμένη μπαταρία και μεταδίδει περιοδικά το σήμα αναγνώρισής της. Μια ετικέτα RFID παθητικής μπαταρίας (BAP) διαθέτει μια μικρή

μπαταρία και ενεργοποιείται στην ύπαρξη αναγνώστη RFID. Στην Εικόνα 2.3 παρουσιάζονται οι προαναφερόμενοι ανά κατηγορία RFID αισθητήρες.

Εικόνα 2.5 Αισθητήρες RFID

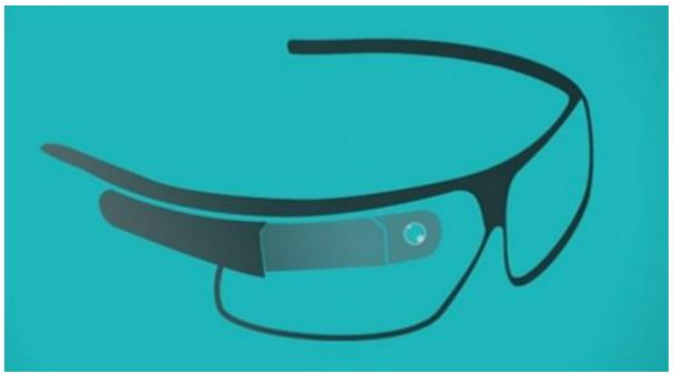
2.2.1.2. Wearable Ηλεκτρονικές Συσκευές

Οι παραπάνω αναφερόμενοι αισθητήρες έχουν ενσωματωθεί σε ηλεκτρονικές συσκευές για πολλές και διάφορες χρήσεις τις οποίες πλέον έχουν καταστήσει «έξυπνες». Λέγονται wearable και είναι συνήθως μικρές συσκευές που φοριούνται στο κεφάλι, στο λαιμό, στους βραχίονες, στον κορμό και στα πόδια.

Εικόνα 2.6 Τα smartwatches δεν μας βοηθάνε μόνο να είμαστε συνδεδεμένοι, αλλά ως μέρος του IoT επιτρέπουν πρόσβαση σε εφαρμογές που βελτιώνουν την παραγωγικότητα.

Οι τρέχουσες φορητές έξυπνες συσκευές περιλαμβάνουν:

- Κεφαλή - Κράνη, γυαλιά
- Λαιμός - Κοσμήματα, περιλαίμια
- Βραχίονας - Ρολόγια, βραχιόλια, δαχτυλίδια
- Κορμός - Ρούχα, σακίδια
- Πόδια - Κάλτσες, παπούτσια



Εικόνα 2.7 Τα έξυπνα γυαλιά μας επιτρέπουν να απολαμβάνουμε περισσότερες από τις υπηρεσίες που μας αρέσουν και, όταν αποτελούν μέρος ενός συστήματος IoT, επιτρέπουν μια νέα προσέγγιση στην παραγωγικότητα.

2.2.1.3. Τυπικές συσκευές

Ο υπολογιστής, το tablet και το κινητό τηλέφωνο παραμένουν αναπόσπαστα μέρη του Διαδικτύου Πραγμάτων ως κέντρο εντολών αλλά και τηλεχειριστήρια.

- Ο **υπολογιστής** παρέχει στον χρήστη το υψηλότερο επίπεδο ελέγχου για το σύστημα και τις ρυθμίσεις του.
- Το **tablet** παρέχει πρόσβαση στα βασικά χαρακτηριστικά του συστήματος με τρόπο που μοιάζει με την επιφάνεια εργασίας και παρέχει επίσης απομακρυσμένη λειτουργικότητα.
- Το **κινητό τηλέφωνο** επιτρέπει μερικές βασικές τροποποιήσεις των ρυθμίσεων και παρέχει επίσης απομακρυσμένη λειτουργικότητα.

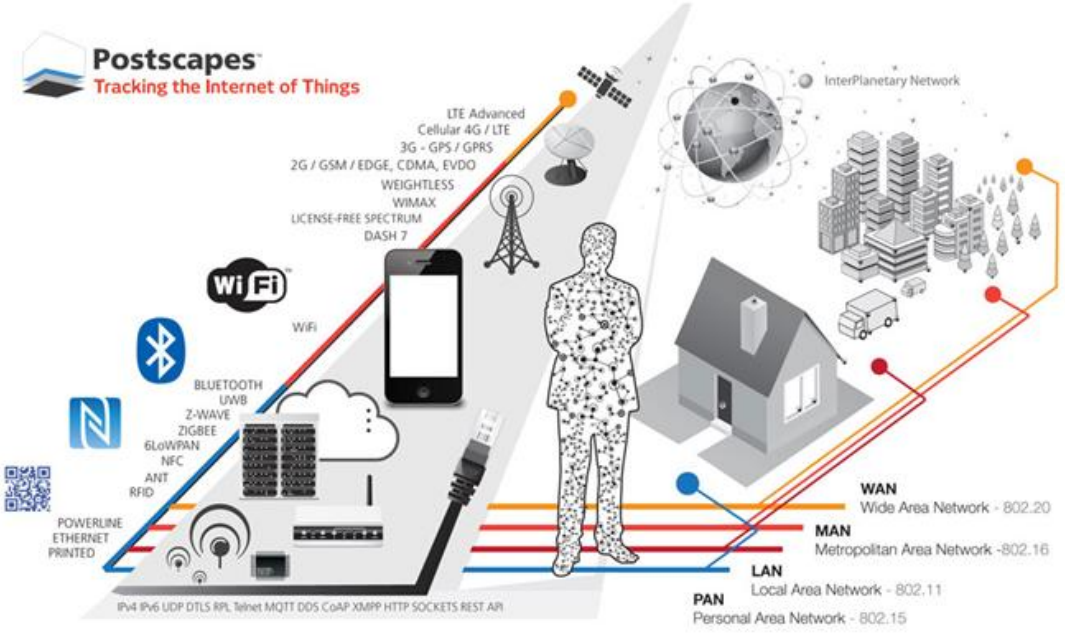
Άλλες βασικές συνδεδεμένες συσκευές περιλαμβάνουν τυποποιημένες συσκευές δικτύου όπως δρομολογητές και διακόπτες.

2.2.2. Το επίπεδο επικοινωνίας του Διαδικτύου Πραγμάτων

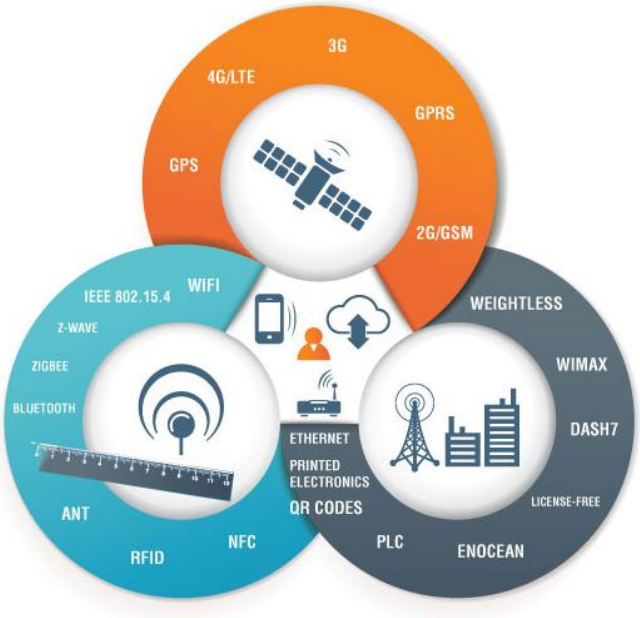
Σε αυτήν την ενότητα θα παρουσιαστούν οι τεχνολογίες δικτύου που μπορούν να βοηθήσουν στην μεγάλης κλίμακας ανάπτυξη του Διαδικτύου Πραγμάτων. Εφόσον η κάθε συσκευή ενδέχεται να χρειάζεται να επικοινωνήσει με άλλες σε οποιαδήποτε απόσταση και με διαφορετικό μέσο επικοινωνίας, υπάρχουν συγκεκριμένες κατάλληλες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

- PAN (Personal Area Network) από 10 έως 100 m
- LAN (Local Area Network) από 0,1 ως 10 km
- MAN (Metropolitan Area Network) από 10 έως 100 km

- WAN (Wide Area Network) από 100 ως 1000 km



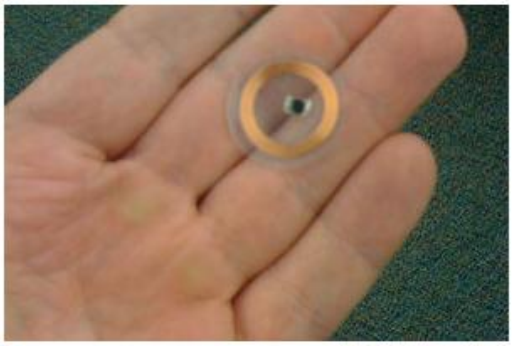
Εικόνα 2.8 Τεχνολογίες επικοινωνίας ανάλογες τις απόστασης.



Εικόνα 2.9 Τεχνολογίες επικοινωνίας

1. **RFID:** Ένα σύστημα αναγνώρισης ραδιοσυχνοτήτων χρησιμοποιεί ετικέτες ή ετικέτες που επισυνάπτονται στα αντικείμενα που πρέπει να ταυτοποιηθούν. Οι αμφίδρομοι πομποδέκτες ραδιοσυχνοτήτων που ονομάζονται αναγνώστες στέλνουν ένα σήμα στην

ετικέτα και διαβάζουν την απάντησή της. Οι αναγνώστες γενικά μεταδίδουν τις παρατηρήσεις τους σε ένα υπολογιστή που χρησιμοποιεί λογισμικό RFID ή middleware
Συχνότητα: 120-150 kHz (LF), 13,56 MHz (HF), 433 MHz (UHF), 865-868 MHz (Ευρώπη) 902-928 MHz (Βόρεια Αμερική) UHF, 2450-5800 MHz GHz
Εύρος: 10cm έως 200m
Παραδείγματα: Οδικά τέλη, Πρόσβαση κτιρίου, Απογραφή



2. **EnOcean**: Η τεχνολογία EnOcean είναι μια ασύρματη τεχνολογία συγκομιδής ενέργειας που χρησιμοποιείται κυρίως σε συστήματα αυτοματισμού κτιρίων. Αλλά εφαρμόζεται και σε άλλες εφαρμογές στη βιομηχανία, τις μεταφορές, τα logistics και τις έξυπνες κατοικίες. Οι μονάδες που βασίζονται στην τεχνολογία EnOcean συνδυάζουν μικροενισχυτές με ηλεκτρονικά εξαιρετικά χαμηλής ισχύος και ενεργοποιούν ασύρματες επικοινωνίες μεταξύ ασύρματων αισθητήρων, διακόπτες, ελεγκτές και πύλες χωρίς μπαταρίες.
   Συχνότητα: 315 MHz, 868 MHz, 902 MHz
   Εύρος: 300μ εκτός κτηρίων, 30μ εντός κτηρίων
   Παραδείγματα: Ασύρματοι διακόπτες, αισθητήρες και χειριστήρια

3. **NFC:** Το NFC είναι ένα σύνολο ασύρματων τεχνολογιών μικρής εμβέλειας, που συνήθως λειτουργούν σε απόσταση 10cm ή λιγότερο. Το NFC λειτουργεί στα 13,56 MHz κατά ISO/IEC 18000-3 και σε ταχύτητες που κυμαίνονται από 106 kbit/s έως 424 kbit/s.

Το NFC συνεπάγεται πάντα έναν εκκινητή και έναν στόχο. Ο εκκινητής δημιουργεί ενεργά ένα πεδίο RF που μπορεί να τροφοδοτήσει έναν παθητικό στόχο. Αυτό επιτρέπει στους στόχους NFC να παίρνουν πολύ απλούς παράγοντες μορφής όπως ετικέτες, αυτοκόλλητα, κλειδιά ή κάρτες που δεν απαιτούν μπαταρίες. Είναι δυνατή η επικοινωνία μεταξύ ομότιμων φορέων NFC, με την προϋπόθεση ότι και οι δύο συσκευές τροφοδοτούνται.

Συχνότητα: 13.56 MHz

Εύρος: : < 0.2 m

Παραδείγματα: Smart Πορτοφόλια / Κάρτες, Έλεγχος Πρόσβασης

4. **Bluetooth**: Το Bluetooth είναι ένα πρότυπο ασύρματης τεχνολογίας για την ανταλλαγή δεδομένων σε μικρές αποστάσεις (χρησιμοποιώντας ραδιοφωνικές εκπομπές μικρού μήκους κύματος στη ζώνη ISM από 2400-2480 MHz) από σταθερές και κινητές συσκευές, δημιουργώντας δίκτυα προσωπικής περιοχής (PANs) με υψηλά επίπεδα ασφάλειας.

   Συχνότητα: 2.4GHz

   Εύρος: : 1-100m

   Παραδείγματα: Ακουστικά Hands-free, κλειδιά, fitness trackers

5. **WiFi**: Το Wi-Fi είναι μια τεχνολογία που επιτρέπει σε μια ηλεκτρονική συσκευή να ανταλλάσσει δεδομένα ασύρματα (χρησιμοποιώντας ραδιοκύματα) μέσω ενός δικτύου υπολογιστών, συμπεριλαμβανομένων των συνδέσεων Internet υψηλής ταχύτητας. Το Wi-Fi Alliance ορίζει το Wi-Fi ως οποιοδήποτε προϊόν "ασύρματου τοπικού δικτύου

(WLAN) που βασίζεται στα πρότυπα 802.11 του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE).

Πρότυπο: 802.11 a/b/g/n/af, WiFi Direct, WPS

Συχνότητα: 2.4 GHz, 3.6 GHz και 4.9/5.0 GHz.

Εύρος: Η κοινή εμβέλεια είναι έως και 100 μέτρα, αλλά μπορεί να επεκταθεί.

Παραδείγματα: Routers, Tablets, etc

6. **Weightless**: Το Weightless είναι ένα προτεινόμενο ιδιόκτητο πρότυπο ασύρματης τεχνολογίας για την ανταλλαγή δεδομένων μεταξύ ενός σταθμού βάσης και χιλιάδων μηχανημάτων γύρω από αυτό, χρησιμοποιώντας το White space - Λευκό Διάστημα (εκπομπές ραδιοκυμάτων μήκους κύματος σε μη χρησιμοποιούμενα τηλεοπτικά κανάλια) με υψηλά επίπεδα ασφάλειας.

   Συχνότητα: Διαφέρει ανάλογα με τη νομοθεσία (470 - 790MHz).

   Εύρος: ως 10km.

   Ταχύτητες: 1kbits/s ως 10Mbits/s

   Παραδείγματα: Έξυπνοι μετρητές, αισθητήρες κυκλοφορίας, βιομηχανική παρακολούθηση.

7. **Cellular**: Κάθε εφαρμογή Διαδικτύου Πραγμάτων που απαιτεί λειτουργία σε μεγαλύτερες αποστάσεις μπορεί να επωφεληθεί από τις δυνατότητες κυψελοειδούς επικοινωνίας GSM / 3G / 4G. Ενώ η κινητή τηλεφωνία είναι σαφώς ικανή να αποστείλει μεγάλες ποσότητες δεδομένων, ειδικά το 4G, η δαπάνη και επίσης η κατανάλωση ενέργειας είναι υπερβολικά υψηλή, αλλά όμως μπορεί να είναι και ιδανική για projects που βασίζονται σε αισθητήρες χαμηλού εύρους ζώνης που αποστέλλουν πολύ μικρά ποσά δεδομένων μέσω του Διαδικτύου.

Πρότυπο: GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)
Συχνότητα: 900/1800/1900/2100MHz
Εύρος: 35km max για το GSM; 200km max για το HSPA, 100km max για το LTE
Ταχύτητες: 35 - 170 kps (GPRS), 120 – 384 kbps (EDGE), 384 Kbps – 42 Mbps (UMTS), 3 – 500 Mbps (LTE)
Παραδείγματα: κινητά τηλέφωνα, M2M, έξυπνος μετρητής.

8. **Z-Wave:** Το Z-Wave είναι μια τεχνολογία επικοινωνιών RF χαμηλής ισχύος που έχει σχεδιαστεί κυρίως για οικιακό αυτοματισμό για προϊόντα όπως ελεγκτές λαμπτήρων και αισθητήρες μεταξύ πολλών άλλων. Βελτιστοποιημένη για αξιόπιστη και με χαμηλό latency επικοινωνία στέλνοντας μικρά πακέτα δεδομένων με ταχύτητες δεδομένων έως 100kbit/s, λειτουργεί στη ζώνη κάτω των 1GHz και είναι αδιαπέραστη από παρεμβολές από WiFi ή άλλες ασύρματες τεχνολογίες στην περιοχή 2,4GHz όπως το Bluetooth ή το ZigBee. Υποστηρίζει πλήρη mesh δίκτυα χωρίς την ανάγκη για έναν κόμβο συντονιστή και είναι πολύ κλιμακωτή, επιτρέποντας τον έλεγχο έως και 232 συσκευών. Το Z-Wave χρησιμοποιεί απλούστερο πρωτόκολλο από κάποια άλλα, και έτσι επιτρέπει ταχύτερη και απλούστερη ανάπτυξη, αλλά ο μοναδικός κατασκευαστής των τσιπς είναι η Sigma Designs σε σύγκριση με τις άλλες ασύρματες τεχνολογίες όπως η ZigBee και άλλες που έχουν πολλούς κατασκευαστές.
   Πρότυπο: Z-Wave Alliance ZAD12837 / ITU-T G.9959
   Συχνότητα: 900MHz (ISM)
   Εύρος: 30m
   Ταχύτητες: 9.6/40/100kbit/s

9. **Zigbee**: Το ZigBee, όπως το Bluetooth, έχει μια μεγάλη εγκατεστημένη βάση λειτουργίας, αν και ίσως περισσότερο σε βιομηχανικά περιβάλλοντα. Το ZigBee PRO και το ZigBee Remote Control (RF4CE), μεταξύ των άλλων διαθέσιμων προφίλ ZigBee, βασίζονται στο πρωτόκολλο IEEE802.15.4, το οποίο είναι μια τεχνολογία ασύρματης δικτύωσης τυποποιημένης βιομηχανίας που λειτουργεί για εφαρμογές στα 2.4GHz που απαιτούν σχετικά σπάνιες ανταλλαγές δεδομένων σε χαμηλές ταχύτητες σε μια περιορισμένη περιοχή εύρους το πολύ 100 μέτρων, όπως σε ένα σπίτι ή ένα κτίριο. Το ZigBee/RF4CE έχει μερικά σημαντικά πλεονεκτήματα σε σύνθετα συστήματα και προσφέρει λειτουργία χαμηλής ισχύος, υψηλή ασφάλεια, ευρωστία και υψηλή δυνατότητα κλιμάκωσης με υψηλό αριθμό κόμβων και είναι σε θέση να επωφεληθεί

από ασύρματα δίκτυα ελέγχου και αισθητήρων σε εφαρμογές M2M και Διαδικτύου Πραγμάτων.

Πρότυπο: ZigBee 3.0 based on IEEE802.15.4

Συχνότητα: 2.4GHz

Εύρος: 10-100m

Ταχύτητες: 250kbps

Features	ZigBee	Bluetooth	Wi-Fi	LTE/ LTE-A
Πρότυπο	IEEE 802.15.4	IEEE 802.15.1	IEEE 802.11	LTE: 3GPP Rel. 9, LTE-A: 3GPP Rel. 10
Συχνότητα	2.4 GHz	2.4 GHz	2.4 και 5 GHz	Εξαρτάται από διαφορετικό # μπάντων
Εύρος	10-300 m	200 m BLE, 100 m (class 1), 10 m (class 2), 1 m (class 3)	10-100 m (cf. Footnote 3)	Εξαρτάται από διαφορετικό # μπάντων
Κατανάλωση Ενέργειας	Χαμηλή	Χαμηλή	Υψηλή	Υψηλή
Κατάταξη Κόστους	1 (lowest)	2	4	5 (Highest)
Ρυθμός Δεδομένων	20,40 και 250 Kbs	1Mbs	11 και 54 Mbs	LTE: 300 Mbs (DL) 75 Mbs (UL), LTE-A: 3 Gbs (DL) 1.5 Gbs(UL)
Τοπολογία Δικτύου	Ad hoc, mesh, peer-to-peer, αστέρας	Ad hoc piconents	Point-to-point	κυψελωτό δίκτυο
Υγειονομικές εφαρμογές	Τηλεπισκόπηση και έλεγχος: παρακολούθηση ασθενειών, προσωπική παρακολούθηση της ευεξίας, παρακολούθηση της οικίας, προσωπική παρακολούθηση γυμναστικής	Machine to machine (M2M):Παρέχει ασύρματη σύνδεση μεταξύ συσκευών	Πρόσβαση στο Διαδίκτυο	M2M services, παρακολούθηση ασθενών και συσκευών
παρεχόμενη ασφάλεια	128 AES κρυπτογράφηση	64/128 AES κρυπτογράφηση	WEP, WPA και WPA2 κρυπτογράφηση, έλεγχος πρόσβασης, έλεγχος ταυτότητας, εμπιστευτικότητα	Αυθεντικοποίηση, 128 AES κρυπτογράφηση
Θέματα ασφάλειας	Αξιοποίηση της διαδικασίας ανταλλαγής κλειδιών και διάρκεια ζωής της μπαταρίας	Άρνηση υπηρεσίας, ασφαλής αντιστοίχιση, κλιμάκωση, κατανάλωση ενέργειας και ενεργοποίηση / απενεργοποίηση της λειτουργίας εντοπισμού	Υποκλοπή και κακόβουλοι επιτιθέμενοι	επίθεση τύπου man-in-the middle, απειλές ταυτότητας χρήστη και συγχρονισμό αριθμού ακολουθίας

Εικόνα 2.10 Χαρακτηριστικά των επιλεγμένων ασύρματων τεχνολογιών επικοινωνιών PAN/LAN/WAN.

2.2.3. Το επίπεδο εφαρμογών του Διαδικτύου Πραγμάτων

Το επίπεδο εφαρμογών του Διαδικτύου Πραγμάτων υλοποιεί τους βασικούς τομείς δικτύωσης και δράσης μέσω διαφόρων platforms, embedded συστημάτων, partner συστημάτων καθώς και middleware. Αυτές οι εφαρμογές είναι υπεύθυνες για τη συλλογή δεδομένων, την ενσωμάτωση συσκευών, την ανάλυση σε πραγματικό χρόνο και την επέκταση εφαρμογής και διαδικασίας στο Διαδίκτυο Πραγμάτων.

Συλλογή Δεδομένων

Αυτό το λογισμικό διαχειρίζεται την ανίχνευση, τις μετρήσεις, το φιλτράρισμα των δεδομένων, την ασφάλεια δεδομένων και τη συγκέντρωση δεδομένων. Χρησιμοποιεί ορισμένα πρωτόκολλα για να βοηθήσει τους αισθητήρες στη σύνδεση με δίκτυα M2M σε πραγματικό χρόνο. Στη συνέχεια συλλέγει δεδομένα από πολλαπλές συσκευές και τα διανέμει σύμφωνα με τις ρυθμίσεις. Λειτουργεί επίσης αντίστροφα με τη διανομή δεδομένων σε συσκευές. Το σύστημα μεταδίδει τελικά όλα τα δεδομένα που έχουν συλλεχθεί σε έναν κεντρικό server.

Ανάλυση σε Πραγματικό Χρόνο

Αυτές οι εφαρμογές λαμβάνουν δεδομένα ή εισροές από διάφορες συσκευές και τη μετατρέπουν σε βιώσιμες δράσεις ή σαφή μοτίβα για ανθρώπινη ανάλυση. Αναλύουν πληροφορίες βασισμένες σε διάφορες ρυθμίσεις και σχέδια, προκειμένου να εκτελέσουν συγκεκριμένες εργασίες.

Θα πρέπει να αναπτυχθούν νέοι αλγόριθμοι «σύμπτυξης» για την επεξεργασία των συλλεγόμενων δεδομένων. Διάφορες μέθοδοι machine learning που στηρίζονται σε εξελικτικούς και γενετικούς αλγόριθμους, νευρωνικά δίκτυα και σε άλλες τεχνικές τεχνητής νοημοσύνης είναι απαραίτητα για να επιτευχθεί η αυτοματοποιημένη λήψη αποφάσεων. Αυτά τα συστήματα διαθέτουν διαρθρωμένη αρχιτεκτονική τόσο σε επίπεδο υλικού όσο και λογισμικού και είναι ιδανικά για την ανάπτυξη εφαρμογών του Διαδίκτυο Πραγμάτων.

Γενικά μία κεντρική υποδομή απαιτείται για την υποστήριξη της αποθήκευσης και της ανάλυσης των δεδομένων. Οι λύσεις που στηρίζονται στις τεχνολογίες Cloud έχουν αρχίσει να γίνονται ολοένα και πιο δημοφιλείς ενώ περαιτέρω ανάπτυξη αναμένεται για τις πλατφόρμες ανάλυσης και οπτικοποίησης πληροφορίας που στηρίζονται στην τεχνολογία του Cloud (AWS IoT service).

Ενσωμάτωση Συσκευών

Το λογισμικό που υποστηρίζει την ολοκλήρωση δεσμεύει (εξαρτώμενες σχέσεις) όλες τις συσκευές του συστήματος για τη δημιουργία του σώματος του συστήματος Διαδικτύου Πραγμάτων. Εξασφαλίζει την απαραίτητη συνεργασία και σταθερή δικτύωση μεταξύ των συσκευών. Αυτές οι εφαρμογές είναι η καθοριστική τεχνολογία λογισμικού του δικτύου Διαδικτύου Πραγμάτων, διότι χωρίς αυτές, δεν θα είχαμε ένα σύστημα Διαδικτύου Πραγμάτων. Διαχειρίζονται τις διάφορες εφαρμογές, τα πρωτόκολλα και τους περιορισμούς κάθε συσκευής για να επιτρέπεται η επικοινωνία.

Επέκταση Εφαρμογής και Διαδικασίας

Αυτές οι εφαρμογές επεκτείνουν την εμβέλεια των υπαρχόντων συστημάτων και λογισμικού για να επιτρέψουν ένα ευρύτερο, πιο αποτελεσματικό σύστημα. Ενσωματώνουν προκαθορισμένες συσκευές για ειδικούς σκοπούς, όπως η πρόσβαση σε ορισμένες κινητές συσκευές ή μηχανικά μέσα. Υποστηρίζει βελτιωμένη παραγωγικότητα και ακριβέστερη συλλογή δεδομένων.

Οπτικοποίηση: Είναι απαραίτητη για μια εφαρμογή Διαδικτύου Πραγμάτων καθώς επιτρέπει την αλληλεπίδραση του χρήστη με το περιβάλλον. Με την ανάπτυξη των συσκευών με τεχνολογία αφής η χρήση των tablets και smartphones έχει γίνει πλέον κομμάτι της καθημερινότητας. Προκειμένου να μπορέσουν οι απλοί καταναλωτές να επωφεληθούν από τη χρήση της τεχνολογίας του Διαδικτύου Πραγμάτων θα πρέπει να δημιουργηθούν προσιτές και εύκολες στην κατανόηση απεικονίσεις, οι οποίες θα μπορούν να παρέχονται με πιο ουσιώδη τρόπο. Αυτό θα επιτρέψει την μετατροπή των απλών δεδομένων σε γνώση, κάτι που είναι απαραίτητο για την γρήγορη λήψη αποφάσεων. Η εξαγωγή χρήσιμων πληροφοριών από πακέτα δεδομένων δεν είναι κάτι απλό. Κάτι τέτοιο περιλαμβάνει τόσο τον εντοπισμό κάποιου συμβάντος όσο και την οπτικοποίηση των δεδομένων που λαμβάνονται για την ευκολότερη και επιθυμητή χρήση από τον εκάστοτε χρήστη.

Οι πλατφόρμες είναι η κόλλα που συγκρατεί το Διαδίκτυο Πραγμάτων μαζί, επιτρέποντας στους χρήστες να επωφεληθούν πλήρως από τις δυνατότητες των συνδεδεμένων συσκευών. Αυτές οι πλατφόρμες επιτρέπουν στο Διαδίκτυο Πραγμάτων να επιτύχει το μετασχηματιστικό δυναμικό του, επιτρέποντας στις επιχειρήσεις να διαχειρίζονται συσκευές, να αναλύουν δεδομένα και να αυτοματοποιούν τη ροή εργασιών.

Ανάπτυξη εφαρμογών: Παρά την πρόοδο στην έρευνα του Διαδικτύου Πραγμάτων, εξακολουθεί να λείπει μια γενική προσέγγιση της μηχανικής λογισμικού για τη συστηματική ανάπτυξη των συστημάτων και των εφαρμογών Διαδικτύου Πραγμάτων. Μια σύνθεση της τελευταίας τεχνολογίας στην περιοχή μπορεί να βοηθήσει στην πλαισίωση των βασικών προσεγγίσεων που σχετίζονται με αυτή την ανάπτυξη. Ένα τέτοιο πλαίσιο θα μπορούσε να αποτελέσει τη βάση για κατευθυντήριες γραμμές για την τεχνολογία λογισμικού με γνώμονα το Διαδίκτυο.

Δεν έχει υπάρξει καθόλου ενοποιημένο σύνολο βέλτιστων πρακτικών για την τεχνολογία λογισμικού για το διαδίκτυο. Πολύ συχνά, οι απροετοίμαστοι προγραμματιστές τοποθετούν τα συστήματα Διαδικτύου Πραγμάτων σε ad hoc τρόπο και να τα ρίχνουν στην αγορά, συχνά δοκιμασμένα ελάχιστα. Επίσης, ο ακαδημαϊκός τομέας κινδυνεύει να κατακερματιστεί σε εξειδικευμένους, συχνά άσχετους ερευνητικούς τομείς.

Ο κλάδος χρειάζεται καθοδήγηση για να σχεδιάσει τη νέα γενιά συστημάτων λογισμικού που είναι κλιμακούμενα, εξαιρετικά αντιδραστικά, συχνά περιορισμένα σε πόρους, τα οποία είναι χαρακτηριστικά για το Διαδίκτυο Πραγμάτων. Πολλά από αυτά τα συστήματα βρίσκονται σε τομείς κρίσιμους για την αποστολή, όπως η ιατρική, η βιομηχανική αυτοματοποίηση και η διαχείριση ενέργειας.

Διαλειτουργικότητα / Πρότυπα:

Το κατακερματισμένο περιβάλλον των αποκλειστικών τεχνικών που προσφέρει το Διαδίκτυο Πραγμάτων πιθανόν να προβληματίσει τους χρήστες αλλά και τη βιομηχανία. Καθώς η πλήρης διαλειτουργικότητα μεταξύ προϊόντων και υπηρεσιών δεν είναι πάντα εφικτή και αναγκαία, οι αγοραστές μπορούν να διστάσουν να αγοράσουν έξυπνες συσκευές, προϊόντα και υπηρεσίες, λόγω αυτού μπορεί να υπάρξει υψηλή κυριότητα πολυπλοκότητας αλλά και ανησυχία για τον προμηθευτή. Επιπλέον, οι ελλιπώς σχεδιασμένες έξυπνες συσκευές μπορεί να έχουν αρνητικές συνέπειες για τη δικτύωση των πόρων όταν συνδεθούν και αποκτήσουν ευρύτερη πρόσβαση. Τα κατάλληλα πρότυπα, μοντέλα αναφοράς και οι βέλτιστες πρακτικές θα πρέπει να συμβάλλουν στην αναχαίτιση της εξάπλωσης των συσκευών που μπορούν να προκαλέσουν αναστάτωση μέσα στο Internet και να στηρίξουν την μεγαλύτερη ωφελιμότητα του χρήστη, την καινοτομία και την οικονομική ευκαιρία.

2.3. Πεδία όπου έχει εφαρμογή το Διαδίκτυο Πραγμάτων

Ο συνδυασμός της τεχνολογίας IoT με το Cloud Computing, 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.

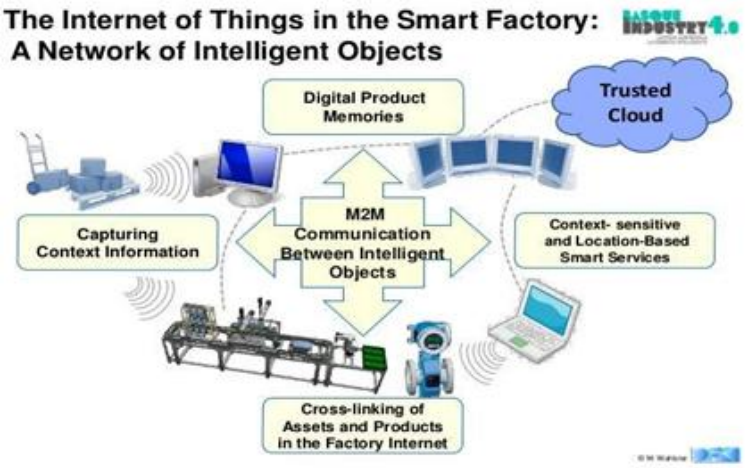
Ερευνώντας την εφαρμογή του IoT διαπιστώνουμε ότι υπάρχουν τέσσερις μεγάλοι τομείς εφαρμογής:

- Προσωπική και Οικιακή
- Επιχειρησιακή
- Δημόσιο Τομέα
- Μεταφορές

Παρακάτω παραθέτουμε μερικές εφαρμογές.

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.



Εικόνα 2.11 Το IoT στην Έξυπνη Βιομηχανία.

ΑΛΥΣΙΔΕΣ ΕΦΟΔΙΑΣΜΟΥ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΤΩΝ ΠΡΟΪΟΝΤΩΝ/ ΜΕΤΑΦΟΡΕΣ

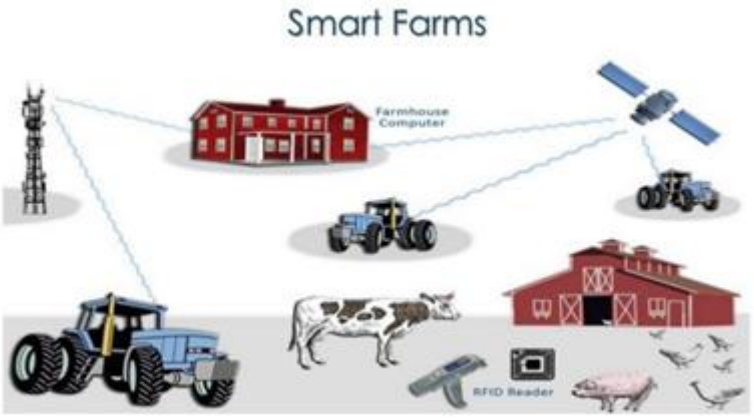
Κύριες δραστηριότητες των έξυπνων μεταφορών αποτελούν :

- 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

ΓΕΩΡΓΙΑ

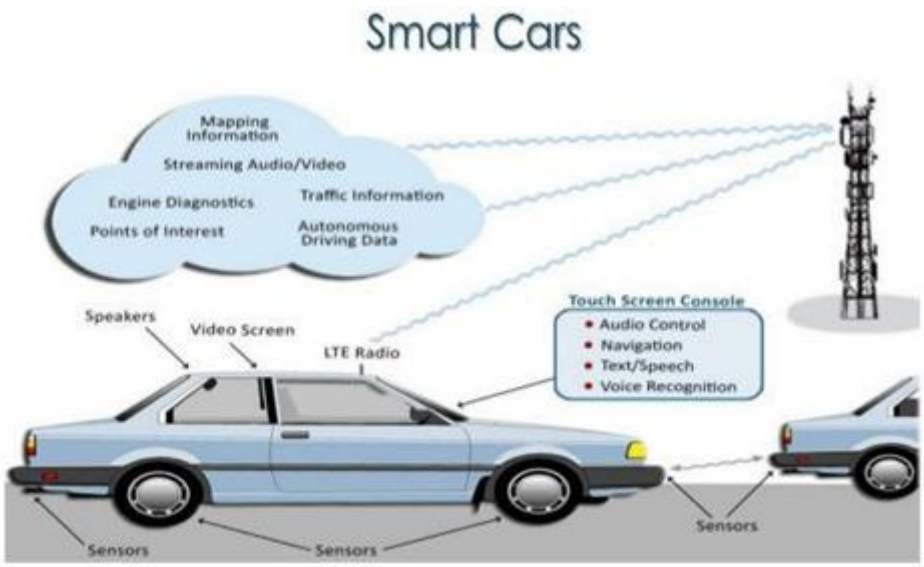
Στο τομέα της κτηνοτροφίας το IoT χρησιμεύει στην παρακολούθηση της αλυσίδας προσφοράς τροφίμων, στην παρακολούθηση των ζώων, στην φυτοπροστασία με σκοπό τον έλεγχο των συνθηκών των φυτών προκειμένου να παρθεί η μέγιστη απόδοση καλλιεργειών καθώς και την παρακολούθηση της φάρμας των ζώων για να διασφαλιστεί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



Εικόνα 2.12 Έξυπνη φάρμα

ΑΥΤΟΚΙΝΗΤΟΒΙΟΜΗΧΑΝΙΑ

Ο στόχος του έξυπνου αυτοκινήτου είναι η σύνδεση του αυτοκινήτου στο σύστημα Διαδίκτυο Πραγμάτων, 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. Σημαντική διευκόλυνση κάθε οδηγού και κυρίως στις μεγάλες πόλεις αποτελεί ο αισθητήρας στάθμευσης. Επίσης οδικές υπηρεσίες πληροφοριών μπορούν να παρέχονται. Τέλος, ο οδηγός μπορεί να ενημερώνεται εν κινήσει 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.



Εικόνα 2.13 Έξυπνο αυτοκίνητο.

Ο ΤΟΜΕΑΣ ΤΗΣ ΕΞΥΠΝΗΣ ΕΝΕΡΓΕΙΑΣ (SMARTGRIDS)

Περιλαμβάνει τα έξυπνα δίκτυα, τους έξυπνους μετρητές, το έξυπνο νερό, αλλά και την έξυπνη διαχείριση σκουπιδιών. Τα ευφυή συστήματα μέτρησης συλλέγουν και μεταφέρουν δεδομένα μέσω επικοινωνίας μεταξύ του μετρητή και των προμηθευτών ενέργειας, των διαχειριστών δικτύων και τρίτων.

Η ΣΥΜΒΟΛΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΠΡΑΓΜΑΤΩΝ 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.

ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΠΡΑΓΜΑΤΩΝ 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.

Εικόνα 2.14 Εφαρμογή IoT στην υγεία.

ΕΞΥΠΝΕΣ 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.

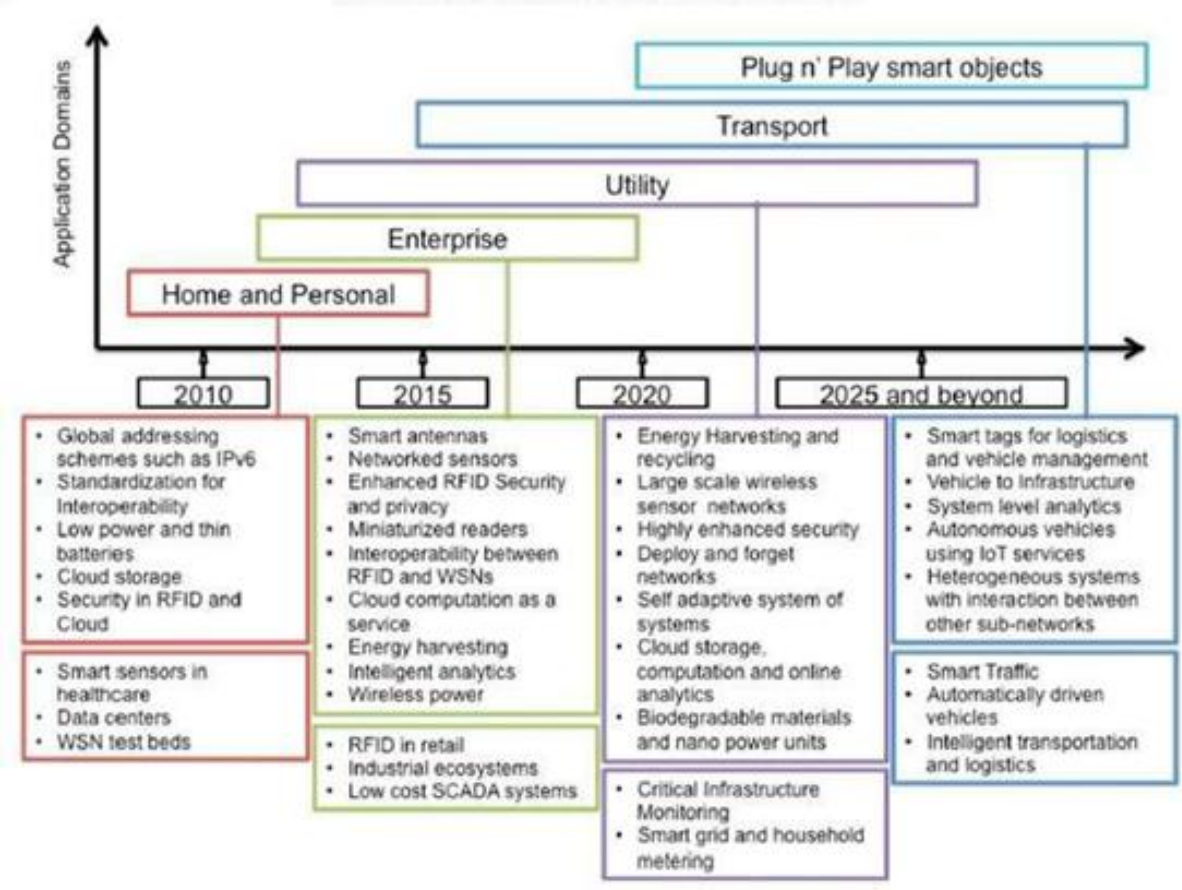
ΟΙΚΙΑΚΟΙ ΑΥΤΟΜΑΤΙΣΜΟΙ/ΕΞΥΠΝΟ ΣΠΙΤΙ

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.

Εικόνα 2.15 Έξυπνο σπίτι.

Στην ακόλουθη Εικόνα φαίνεται η αναμενόμενη ανάπτυξη των ήδη υπαρχόντων, αλλά και η δημιουργία νέων, καινοτόμων εφαρμογών του Διαδικτύου Πραγμάτων μέσα στα πλαίσια της επόμενης δεκαετίας για τους διαφορετικούς τομείς εφαρμογής .



Εικόνα 2.16 Αναμενόμενη ανάπτυξη IoT

3. Ιδιωτικότητα και ασφάλεια

Τα χαρακτηριστικά του Διαδικτύου Πραγμάτων δημιουργούν νέες και μοναδικές προκλήσεις στον τομέα της ιδιωτικότητας και της ασφαλείας. Η αντιμετώπιση αυτών των προκλήσεων και η εξασφάλιση της ιδιωτικότητας και της ασφάλειας των έξυπνων προϊόντων και υπηρεσιών, οφείλουν να αποτελέσουν θεμελιώδη προτεραιότητα. Οι χρήστες χρειάζεται να εμπιστευτούν πως οι έξυπνες συσκευές και οι συναφείς υπηρεσίες δεδομένων δεν έχουν τρωτά σημεία, καθώς η τεχνολογία του Διαδικτύου Πραγμάτων σκοπεύει να διεισδύσει και να ενσωματωθεί στην καθημερινή μας ζωή.

Εικόνα 3.1 Πεδία Ασφάλειας στο IoT

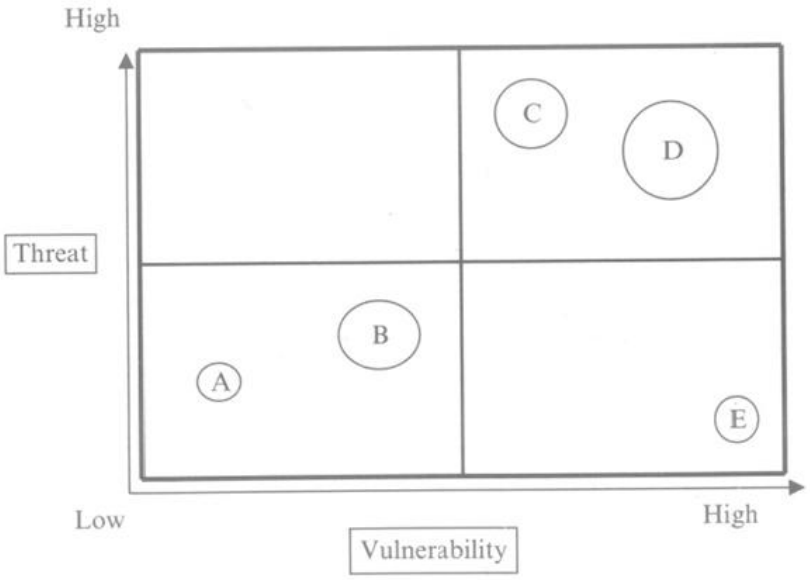
Για την καλύτερη κατανόηση της ανάλυσης απειλών και επιπτώσεων στην ιδιωτικότητα και την ασφάλεια κατά τη χρήστη του Διαδικτύου Πραγμάτων, αρχικά δίνονται οι βασικοί ορισμοί που χρησιμοποιούνται ευρέως στην ανάλυση κινδύνων:

Απειλή: Ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, τυχαία ή με πρόθεση μετατροπή των δεδομένων, καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών.

Ευπάθεια: Είναι η αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, στην εφαρμογή ή στην υποδομή που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος. Η ευπάθεια μπορεί να οριστεί και με την εξής συνάρτηση:

Ευπάθεια = Πιθανότητα να συμβεί μια απειλή x Πιθανότητα να είναι επιτυχής

Κίνδυνος: Η πιθανότητα μια συγκεκριμένη απειλή να εκμεταλλευτεί μια συγκεκριμένη ευπάθεια. Ο κίνδυνος εκφράζει το ενδεχόμενο για απώλεια.



Εικόνα 3.2 Μέθοδος αξιολόγησης κινδύνου.

Κίνδυνος = **Απειλή** x **Ευπάθεια** x **Επίδραση** (αξία ενεργητικού)
Risk = **Threat** x **Vulnerability** x **Impact** (Asset value)

Αντίμετρο: Μέτρο που λαμβάνεται για την προστασία του πληροφοριακού συστήματος και την αντιμετώπιση των απειλών. Το μέτρο μπορεί να ενεργεί ανιχνεύοντας, προλαμβάνοντας ή μειώνοντας την απώλεια που σχετίζεται με την εμφάνιση μιας απειλής ή κατηγορίας απειλών.

3.1. Ανάλυση Απειλών – Επιπτώσεων Ιδιωτικότητας σε εφαρμογές του Διαδικτύου Πραγμάτων

Η υλοποίηση των πλήρων προοπτικών του Διαδικτύου Πραγμάτων εξαρτάται και τις ατομικές επιλογές απορρήτου. Οι ροές δεδομένων του χρήστη και η εξειδίκευση που του παρέχουν οι έξυπνες συσκευές μπορούν να βελτιώσουν την ζωή του, όμως οι ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής αλλά και των πιθανών ζημιών αποτελούν εμπόδιο για την πλήρη αξιοποίηση του Διαδικτύου Πραγμάτων. Η ιδιωτικότητα είναι μία από τα βασικά και νομικά θεμελιωμένα δικαιώματα του κάθε ανθρώπου. Εξαιτίας αυτού του δικαιώματος οποιαδήποτε μη ασφαλής παροχή υπηρεσιών μπορεί να οδηγήσει σε εμπόδια στην ανάπτυξη του διαδικτύου των αντικειμένων. Αντίθετα ο σεβασμός προς τα

δεδομένα του χρήστη πρέπει να αποτελεί δεδομένο ώστε να κερδίσει την εμπιστοσύνη του χρήστη αλλά και την εμπιστοσύνη του στο Διαδίκτυο, τις συνδεδεμένες συσκευές και τις συναφείς υπηρεσίες.

Συνεπώς το Διαδίκτυο Πραγμάτων επαναπροσδιορίζει τη συζήτηση σχετικά με τα θέματα απορρήτου και του τρόπου περισυλλογής, ανάλυσης, χρησιμοποίησης και προστασίας των προσωπικών δεδομένων.

3.1.1. Κίνδυνοι έκθεσης του ιδιωτικού απορρήτου των χρηστών

Η παγκόσμια κοινωνία της πληροφορίας εξελίσσεται τόσο γρήγορα που συνεχώς αναπτύσσονται πολλοί νέοι δρόμοι και εφαρμογές του Διαδικτύου Πραγμάτων σε ό,τι αφορά τον τομέα της υγείας, της δημόσιας διοίκησης, της έρευνας, του ηλεκτρονικού εμπορίου και της ιδιωτικής ζωής. Για τις εφαρμογές αυτές, υπάρχει ένας συνεχώς αυξανόμενος όγκος προσωπικών δεδομένων, όπως τα ευαίσθητα ιατρικά, επιχειρησιακά και προσωπικά δεδομένα που συλλέγονται, επεξεργάζονται και επικοινωνούνται μέσω δικτύων κατά μήκος των κρατικών συνόρων, διασχίζοντας και χώρες οι οποίες ίσως να μην έχουν το κατάλληλο επίπεδο ιδιωτικότητας..

Για παράδειγμα έστω, ότι έχουμε ένα δίκτυο στο οποίο συνδέονται, χρήστες, δάσκαλοι, κοινωνικά κέντρα και άτομα με ειδικές ανάγκες σε ευρωπαϊκή κλίμακα. Το δίκτυο αυτό συλλέγει δεδομένα για τη συμπεριφορά των συμμετεχόντων σε μία ποικιλία ειδικά σχεδιασμένων σεναρίων. Τα εν λόγω δεδομένα μπορούν να χρησιμοποιηθούν από ειδικούς επιστήμονες στην ανάλυση συμπεριφοράς.

Ωστόσο, τα αρχεία των χρηστών, αποτελούν ευαίσθητες πληροφορίες και η ιδιωτικότητα και η εμπιστευτικότητα τους θα πρέπει να προστατευθούν ιδιαίτερα σε αυτή την περίπτωση, επειδή πιθανή πρόσβαση σε αυτές τις πληροφορίες, μπορεί να προκαλέσει κοινωνική αμηχανία. Η έλλειψη ευρείας εμπιστοσύνης στην ιδιωτικότητα, μπορεί να οδηγήσει τους συμμετέχοντες να εγκαταλείψουν το δίκτυο, και να αποτρέψει πιθανούς νέους συμμετέχοντες.

Συμπληρωματικά, δεδομένου ότι οι βάσεις δεδομένων προσώπου (παραδείγματος χάριν από το Facebook) είναι διαθέσιμες και σε μη κυβερνητικά κόμματα όπως πλατφόρμες μάρκετινγκ, η αυτόματη ταυτοποίηση των ατόμων από τις εικόνες κάμερας είναι ήδη πραγματικότητα. Επίσης, η αυξανόμενη (ασύρματη) διασύνδεση και η κάθετη επικοινωνία των καθημερινών πραγμάτων, ανοίγουν δυνατότητες ταυτοποίησης συσκευών μέσω δακτυλικών αποτυπωμάτων. Τέλος, η αναγνώριση ομιλίας χρησιμοποιείται ευρέως σε κινητές εφαρμογές και ήδη κατασκευάζονται τεράστιες βάσεις δεδομένων για δείγματα

ομιλίας. Αυτά θα μπορούσαν ενδεχομένως να χρησιμοποιηθούν για την αναγνώριση και τον εντοπισμό ατόμων, π.χ. από τις κυβερνήσεις που ζητούν πρόσβαση στα δεδομένα αυτά.

Συμπερασματικά, λόγω της ανάπτυξης αντίστοιχων δικτύων σε εθνικό και παγκόσμιο επίπεδο, όλο και περισσότερα ευαίσθητα δεδομένα θα συλλέγονται, θα αποθηκεύονται ηλεκτρονικά, θα διαμοιράζονται μεταξύ διαφόρων επαγγελματιών και θα μεταφέρονται σε διάφορους τόπους στον κόσμο. Θα πρέπει να εξασφαλιστεί ότι μόνο εξουσιοδοτημένο προσωπικό θα μπορεί να έχει πρόσβαση στις πληροφορίες. Ειδικότερα, οι χρήστες θα πρέπει να μπορούν να έχουν πρόσβαση και να επεξεργαστούν τα δεδομένα μόνο αν αυτό είναι απαραίτητο για το εξουσιοδοτημένο έργο τους (αρχή της αναγκαιότητας συλλογής και επεξεργασίας δεδομένων) και εάν ο σκοπός της επεξεργασίας δεδομένων είναι συμβατός με τους σκοπούς για τους οποίους το στοιχείο λήφθηκε (αρχή της αντιστοίχησης σκοπού). Εκτός αυτού, απαραίτητη προσοχή πρέπει να δοθεί στην αρχή ιδιωτικότητας για τη διαφάνεια, έτσι ώστε οι συμμετέχοντες να ξέρουν ποιος έχει πρόσβαση στα δεδομένα τους και για ποιους λόγους.

3.1.2. Απειλές κατά της ταυτότητας των χρηστών

Οι επιθέσεις στον κυβερνοχώρο, μπορούν να εισάγουν ψευδή δεδομένα σε ένα σύστημα, προκαλώντας κρίσιμες ζημίες στις εφαρμογές του Διαδικτύου και αλλοιώνοντας ταυτόχρονα την πραγματική αποθηκευμένη ταυτότητα των χρηστών. Οι κυβερνοεπιθέσεις είναι μία κρίσιμη απειλή σε όλα τα επίπεδα του Διαδικτύου πραγμάτων, και για αυτόν τον λόγο θα επανέλθουμε παρακάτω σε αυτό το θέμα. Εν συντομία, είναι θεμελιώδες να παρέχεται το κατάλληλο επίπεδο προστασίας από επιθέσεις στον κυβερνοχώρο σε εφαρμογές έξυπνων συσκευών, ωστόσο, η περιορισμένη από τους πόρους φύση πολλών τέτοιων δεν επιτρέπει την εφαρμογή των τυποποιημένων λύσεων ασφάλειας.

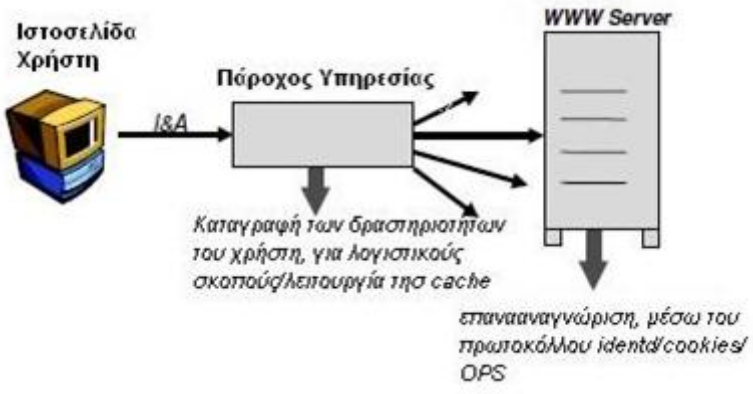
3.1.3. Παρακολούθηση δεδομένων

Ένα σημαντικό μειονέκτημα της παγκόσμιας επικοινωνίας είναι, ότι τα δεδομένα της σύνδεσης είναι διαθέσιμα σε διάφορους τόπους σε όλο τον κόσμο, αποκαλύπτοντας λεπτομέρειες για τους παρτενέρ επικοινωνίας, το χρόνο της επικοινωνίας, τις υπηρεσίες που χρησιμοποιήθηκαν, τις διάφορες συνδέσεις, κ.ο.κ. Αυτά τα δεδομένα των συναλλαγών, μπορούν να αποκαλύψουν το ποιος επικοινώνησε με ποιον, πότε, για πόση ώρα, και ποιος αγόρασε τι και σε ποια τιμή. Οι χρήστες αφήνουν ηλεκτρονικά ίχνη, τα

οποία μπορούν να χρησιμοποιηθούν για τη δημιουργία προφίλ καταναλωτών ή επικοινωνίας.

Κάθε ηλεκτρονικό μήνυμα περιέχει μια επικεφαλίδα με πληροφορίες για τον αποστολέα και τον παραλήπτη, καθώς επίσης και για τη δρομολόγηση και το θέμα του μηνύματος. Αυτές οι πληροφορίες θα μπορούσαν να διαβαστούν ή να τροποποιηθούν από κάθε τόπο από τον οποίο πέρασαν και να χρησιμοποιηθούν για την ανάλυση της κίνησης στο δίκτυο. αντίστοιχη υποκλοπή μπορεί να πραγματοποιηθεί και κατά τη σύνδεση του χρήστη σε ασύρματα δίκτυα.

Αν ένας χρήστης συνδεθεί στο Διαδίκτυο, τα στοιχεία της επικοινωνίας θα έχουν ήδη ληφθεί από την αντίστοιχη εταιρεία τηλεπικοινωνιών ή ακόμα και από τους παρόχους ηλεκτρονικού ταχυδρομείου. Οι πάροχοι υπηρεσιών αποθηκεύουν τα προσωπικά δεδομένα των συνδρομητών τους και οι επικοινωνιακές τους συνήθειες θα μπορούσαν να ανιχνευτούν εύκολα και να επιτηρηθούν από τους παρόχους. Επίσης, τα προσωπικά δεδομένα των χρηστών μπορούν να καταγραφούν και από απομακρυσμένους εξυπηρετητές (remote servers).



Εικόνα 3.3 Συλλογή των Δεδομένων Επικοινωνίας.

Τα δεδομένα που συναλλάσσονται, μπορούν γενικά να αποκαλύψουν ευαίσθητες πληροφορίες για τη συμπεριφορά και τα ενδιαφέροντα επικοινωνίας του χρήστη. Ισχυρό ενδιαφέρον σε τέτοιου είδους δεδομένα που αποκαλύπτουν τις προτιμήσεις των χρηστών, συνήθως έχουν οι διαφημιστικές εταιρείες. Οι χρήστες έχουν τους λόγους τους να ανησυχούν για τη διανομή των συναλλακτικών δεδομένων τους για οικονομικά οφέλη και την πιθανή χρήση τους για λόγους πέρα από αυτούς για τους οποίους συλλέχθηκαν.

3.1.4. Ιδιωτικότητα αποθηκευμένων δεδομένων

Τα ιδιωτικά δεδομένα των χρηστών που έχουν συλλεχθεί, συνήθως καταχωρούνται και διατηρούνται για μελλοντική χρήση, πολλά χρόνια αργότερα. Οι μακροπρόθεσμες βάσεις δεδομένων και οι ισχυρές μηχανές αναζήτησης καθιστούν πολύ εύκολο το χτίσιμο ενός περιεκτικού προφίλ των χρηστών και να συμβάλουν έτσι στη “επίδραση του φακελώματος”. Θα πρέπει να εξασφαλιστεί ότι μόνο το ελάχιστο εξουσιοδοτημένο προσωπικό θα μπορεί να έχει πρόσβαση πάνω στις αποθηκευμένες πληροφορίες (παραδείγματος χάριν σε μία βάση δεδομένων), για διαχειριστικούς σκοπούς και όχι για την άντληση, εκμετάλλευση ή άμεση τροποποίηση τους.

3.1.5. Απόρρητο τοποθεσίας χρηστών

Ο εντοπισμός και η παρακολούθηση είναι η απειλή προσδιορισμού και καταγραφής της τοποθεσίας ενός ατόμου μέσω του χρόνου και του χώρου. Η παρακολούθηση της τοποθεσίας απαιτεί την προηγούμενη αναγνώριση του χρήστη, ώστε να συνδέονται συνεχόμενες τοποθεσίες σε ένα άτομο. Σήμερα, η παρακολούθηση είναι δυνατή με διαφορετικά μέσα, όπως GPS, πλοήγηση στο διαδίκτυο ή τοποθεσία κινητού τηλεφώνου.

Ο εντοπισμός και η παρακολούθηση ατόμων είναι μια σημαντική λειτουργία σε πολλά συστήματα Διαδικτύου Πραγμάτων. Οι χρήστες την αντιλαμβάνονται ως παραβίαση όταν δεν έχουν τον έλεγχο των πληροφοριών θέσης τους, δεν γνωρίζουν την αποκάλυψή τους ή εάν οι πληροφορίες χρησιμοποιούνται και συνδυάζονται σε ακατάλληλο περιβάλλον. Αυτό συμπίπτει με τον ορισμό της ιδιωτικής ζωής. Τα δεδομένα τοποθεσίας εμφανίζονται ως απειλή κατά κύριο λόγο στη φάση της επεξεργασίας των πληροφοριών, έξω από τον έλεγχο του χρήστη.

Ωστόσο, η εξέλιξη του Διαδικτύου θα αλλάξει και θα επιδεινώσει την απειλή αυτή με τρεις τρόπους: Πρώτον, παρατηρούμε την αυξανόμενη χρήση των υπηρεσιών τοποθεσίας. Οι τεχνολογίες του Διαδικτύου Πραγμάτων όχι μόνο θα υποστηρίξουν την ανάπτυξη τους και θα βελτιώσουν την ακρίβειά τους, αλλά θα επεκτείνουν και αυτές τις υπηρεσίες. Δεύτερον, καθώς η συλλογή δεδομένων γίνεται πιο παθητική, πιο διαδεδομένη και λιγότερο επεμβατική, οι χρήστες έχουν λιγότερη επίγνωση για την παρακολούθηση και τους σχετικούς κινδύνους. Τρίτον, η αυξανόμενη αλληλεπίδραση με έξυπνα πράγματα και συστήματα αφήνει ίχνη δεδομένων που όχι μόνο θέτουν τον χρήστη σε κίνδυνο αναγνώρισης αλλά επιτρέπουν επίσης την παρακολούθηση της θέσης και της δραστηριότητάς του, για παράδειγμα, μεταφέροντας ένα έξυπνο τηλέφωνο με δυνατότητα NFC για να πάρετε ένα εισιτήριο λεωφορείου ή χρησιμοποιώντας το έξυπνο σύστημα στάθμευσης των πόλεων. Με αυτές τις εξελίξεις, η απειλή εντοπισμού της τοποθεσίας θα

υπάρχει και σε καταστάσεις όπου ο χρήστης μπορεί ψευδώς να αντιληφθεί ότι βρίσκεται σε κατάσταση ιδιωτικότητας, δηλαδή σε απομονωμένο από τους άλλους χώρο, όπως ένα δωμάτιο.

Οι κύριες προκλήσεις που εντοπίζουμε είναι (i) η ευαισθητοποίηση σχετικά με την παρακολούθηση ενόψει της συλλογής παθητικών δεδομένων, (ii) ο έλεγχος των δεδομένων κοινόχρηστης τοποθεσίας σε εσωτερικά περιβάλλοντα και (iii) τα πρωτόκολλα διατήρησης της ιδιωτικής ζωής για αλληλεπίδραση με τα συστήματα του Διαδικτύου Πραγμάτων.

	Technology	Size	Intercon-nection	Data collection	Thing Interac-tion	System Interaction	Lifecycle	Vertical vs. horizontal
Identification	Cameras, face recognition		Fingerprint-ing			Speech, cloud interfaces		
Tracking	Indoor LBS			Decreasing awareness		Data trails		
Profiling		Explosion of data sources		Qualitatively new sets of data				
Interaction & Presentation					*Presenta-tion media*	Pervasive interaction with users		
Lifecycle transitions				Product history log			Exchange-ability	Sensitive data on devices
Inventory attacks	*Diversifi-cation*		Wireless communica-tion					
Linkage				Decreasing transparency				*Drives linkage locally*

Εικόνα 3.4 Περίληψη των επιπτώσεων των εξελισσόμενων χαρακτηριστικών στις επτά κατηγορίες απειλών για την προστασία της ιδιωτικής ζωής. Οι δηλώσεις με πλάγιους χαρακτήρες δείχνουν ότι ο αντίκτυπος είναι ενδεχομένως διφορούμενος.

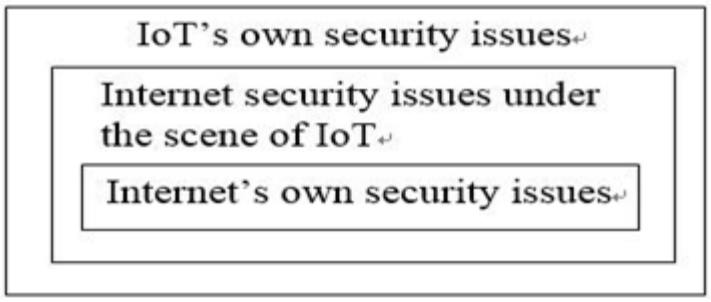
3.2. Ανάλυση Απειλών – Επιπτώσεων Ασφάλειας σε εφαρμογές του Διαδικτύου Πραγμάτων

Παρόλο που ο τομέας της ασφάλειας δεν είναι κάτι καινούριο για τον τομέα της πληροφορικής, τα χαρακτηριστικά του Διαδικτύου Πραγμάτων δημιουργούν νέες και μοναδικές προκλήσεις στον τομέα της ασφαλείας.

3.2.1. Θέματα Ασφάλειας στο Διαδίκτυο Πραγμάτων σε συσχέτιση με το παραδοσιακό Διαδίκτυο

Δεδομένου ότι το Διαδίκτυο Πραγμάτων συγχώνευσε το παραδοσιακό Διαδίκτυο, τα ασύρματα δίκτυα επικοινωνιών, το WSN και άλλα δίκτυα, οι υπάρχουσες τεχνολογίες ασφάλειας στο Διαδίκτυο μπορούν να του παράσχουν κάποια ασφάλεια. Ωστόσο, η υπάρχουσα αρχιτεκτονική ασφάλειας και η τεχνολογία ασφάλειας δεν μπορούν να

καλύψουν όλα τα ζητήματα ασφάλειας και των τριών στρωμάτων του. Έτσι, η αρχιτεκτονική ασφάλειας του Διαδικτύου Πραγμάτων δεν μπορεί απλώς να αντιγράψει την παραδοσιακή αρχιτεκτονική ασφάλειας του Internet ούτε να επανασχεδιάσει πλήρως τις νέες αρχιτεκτονικές ασφαλείας. Με αυτή τη λογική, τα ζητήματα ασφαλείας μπορούν να διαχωριστούν σε τρεις κατηγορίες.



Εικόνα 3.5 Κατηγορίες των θεμάτων ασφάλειας του Διαδικτύου Πραγμάτων.

- **Θέματα ασφάλειας του Διαδικτύου**

Αυτά τα ζητήματα ασφάλειας υπάρχουν αρχικά στο παραδοσιακό περιβάλλον του Διαδικτύου καθώς και στο περιβάλλον του Διαδικτύου. Μπορούν ακόμα να επιλυθούν συνεχίζοντας τη χρήση της παραδοσιακής αρχιτεκτονικής ασφαλείας του Διαδικτύου.

Για παράδειγμα: παρακολούθηση δεδομένων, παραβίαση, πλαστογράφηση, επιθέσεις άρνησης υπηρεσίας, επιθέσεις man in the middle και άλλες κοινές επιθέσεις στο διαδίκτυο.

- **Ζητήματα ασφάλειας του Διαδικτύου υπό το πρίσμα του Διαδικτύου Πραγμάτων**

Αυτά τα ζητήματα ασφάλειας επιλύονται ήδη από ορισμένες τεχνολογίες ασφαλείας στο περιβάλλον του Διαδικτύου. Ωστόσο δεδομένης της φύσης του Διαδικτύου Πραγμάτων, δημιουργούν ορισμένα νέα ζητήματα ασφάλειας. Αυτά τα ζητήματα ασφάλειας δεν μπορούν απλά να επιλυθούν συνεχίζοντας τη χρήση της τεχνολογίας ασφαλείας για το παραδοσιακό Διαδίκτυο, αλλά πρέπει να ληφθούν υπόψη και τα ιδιαίτερα χαρακτηριστικά φύσης του Διαδικτύου Πραγμάτων.

Για παράδειγμα: Το DNS δεν πιστοποιεί τον αιτούντα. Σε περιβάλλον Διαδικτύου Πραγμάτων θα προκαλέσει διαρροή προσωπικού απορρήτου.

- **Ζητήματα ασφάλειας του Διαδικτύου Πραγμάτων**

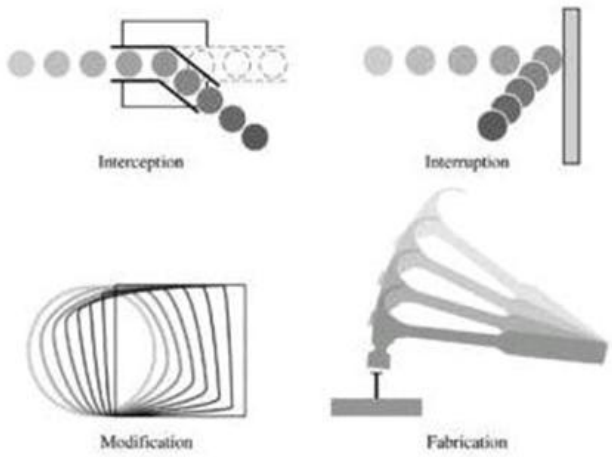
Αυτά τα ζητήματα ασφάλειας οφείλονται στη νέα δομή δικτύου, στον ειδικό εξοπλισμό και σε άλλους παράγοντες του Διαδικτύου Πραγμάτων. Δεν μπορούν να λυθούν με τις παραδοσιακές αρχιτεκτονικές ασφάλειας του Διαδικτύου, επομένως πρέπει να σχεδιαστούν νέες αρχιτεκτονικές ασφάλειας και πρωτόκολλα ασφάλειας.

Για παράδειγμα: πρωτόκολλα ελέγχου ταυτότητας, βασική συμφωνία και προστασία της ιδιωτικής ζωής των συσκευών WSN

Σε επόμενη υποπαράγραφο θα παραθέσουμε τις απειλές στην ασφάλεια, σχετικά με τα επίπεδα του του Διαδικτύου Πραγμάτων. Οι απειλές στις οποίες θα αναφερθούμε μπορεί να ανήκει σε οποιοδήποτε από τις παραπάνω προαναφερθείσες κατηγορίες.

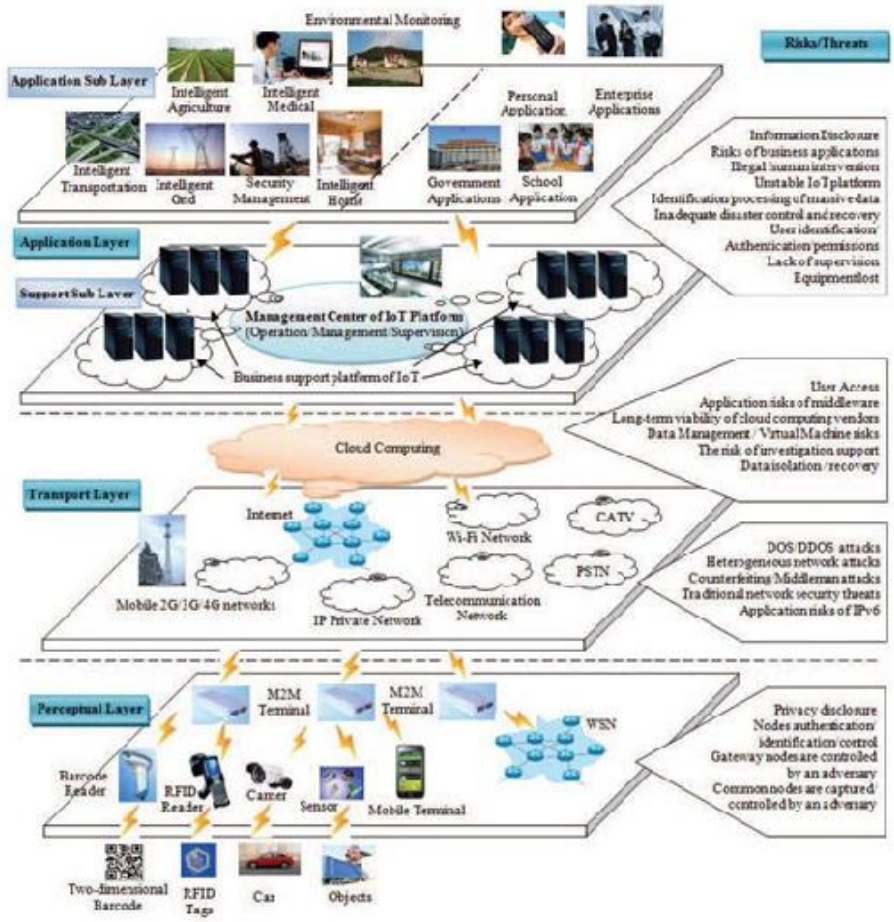
3.2.2. Ευρύτερη Κατηγοριοποίηση απειλών προς την ασφάλεια

- **Διακοπή (interruption):** Τα αντικείμενα του συστήματος χάνονται, δεν είναι διαθέσιμα ή είναι μη χρησιμοποιήσιμα.
- **Παρεμπόδιση (interception):** Σημαίνει πως μια μη εξουσιοδοτημένη ομάδα έχει κερδίσει το δικαίωμα πρόσβασης σε ένα αντικείμενο. Αυτή η εξωτερική ομάδα μπορεί να είναι είτε πρόσωπα, είτε προγράμματα ή ακόμα και παρέμβαση ενός πληροφοριακού συστήματος. Παρόλο που μια απώλεια μπορεί να αποκαλυφθεί σχετικά γρήγορα, ο υποκλοπέας μπορεί να μην αφήσει καθόλου ίχνη για την ανίχνευση της ύπαρξης του.
- **Τροποποίηση (modification)**: Εάν μια μη εξουσιοδοτημένη ομάδα όχι μόνο προσπελάσει τα δεδομένα, αλλά ανακατευτεί και με κάποια αντικείμενα, τότε μιλάμε για τροποποίηση.
- **Πλαστοποίηση (fabricate)**: Τέλος μια μη εξουσιοδοτημένη ομάδα μπορεί να κατασκευάσει πλαστά αντικείμενα σε ένα Π.Σ. Ο εισβολέας μπορεί να προσθέσει εγγραφές σε μια υπάρχουσα βάση δεδομένων. Μερικές φορές αυτές οι προσθέσεις ανιχνεύονται σαν πλαστές, αλλά εάν έχουν γίνει περίτεχνα τότε είναι αδιαχώριστες από τα πραγματικά αντικείμενα.



Εικόνα 3.6 Απειλές Ασφαλείας.

3.2.3. Θέματα Ασφάλειας στο Διαδίκτυο Πραγμάτων ως προς τα τρία επίπεδά του



Εικόνα 3.7 Ρίσκα και Κίνδυνοι που αντιμετωπίζει η αρχιτεκτονική 3 επιπέδων.

3.2.3.1. Θέματα Ασφάλειας στα υλικά συστατικά του Διαδικτύου Πραγμάτων

Φυσική βλάβη ή καταστροφή συσκευών/κόμβων: Πιο αναλυτικά, με καταστροφή των κόμβων που αποτελούν μέρος της εφαρμογής του Διαδικτύου Πραγμάτων, μπορούν να υποκλαπούν, να αντιγραφούν ή να τροποποιηθούν τα αποθηκευμένα δεδομένα. Τα κρίσιμα σημεία για την υποκλοπή είναι τα σημεία διαχείρισης και συγκέντρωσης του δικτύου. Σε αυτή την κατηγορία ανήκουν και οι περιπτώσεις κλοπής, αντικατάστασης ή τροποποίησης μιας συσκευής/κόμβου. Επίσης, πιθανές βλάβες είναι και η απώλεια ισχύος ή δικτύου, οι οποίες μπορούν να οδηγήσουν σε απώλεια δεδομένων.

Χρήση για άλλους σκοπούς: Ενώ οι συνήθεις επιτραπέζιοι υπολογιστές χρησιμοποιούνται με κάπως ελεγχόμενο, τυποποιημένο τρόπο, οι συσκευές στο Διαδίκτυο των Πραγμάτων μπορούν να χρησιμοποιηθούν με τρόπους που δεν είχαν αρχικά προβλεφθεί από τον κατασκευαστή. Για να γίνουν τα προϊόντα όσο το δυνατόν πιο φιλικά προς το χρήστη, οι κατασκευαστές συχνά περιλαμβάνουν μόνο ασφάλεια κατάλληλη για την ειδική περίπτωση χρήσης τους, καθώς η δημιουργία ισχυρής κρυπτογράφησης συχνά προσθέτει κόστος για τον χρήστη.

Ένα παράδειγμα που συχνά συναντά κανείς είναι τα μπαρ και άλλοι δημόσιοι χώροι που χρησιμοποιούν οπτικοακουστικά συστήματα που προορίζονταν αρχικά για ιδιωτική χρήση. Όταν το μπαρ δώσει πρόσβαση στο ασύρματο δίκτυο για τους πελάτες του, η ασφάλεια σε όλα τα οπτικοακουστικά συστήματα είναι ανύπαρκτη. Ο χρήστης κατά συνέπεια μπορεί να αποκτήσει πρόσβαση σε αυτά και σε λογαριασμούς συνδεδεμένους με τις συσκευές, όπως το Spotify, το Google Music, κλπ.

Η πρόκληση αυτή ενισχύεται και από άλλους παράγοντες όπως η μαζική κλίμακα ανάπτυξης ομοιογενών Διαδικτύου Πραγμάτων συσκευών όπου ορισμένες από αυτές, έχουν την δυνατότητα να συνδέονται αυτόματα με άλλες συσκευές. Αυτό αυξάνει τις πιθανότητες οι συσκευές αυτές να συνδεθούν σε μη ασφαλή περιβάλλοντα.

Μη εξουσιοδοτημένη πρόσβαση/έλεγχος πρόσβασης: Ο έλεγχος πρόσβασης είναι ουσιαστικός για την αποτροπή πρόσβασης των μη εξουσιοδοτημένων οντοτήτων στους πόρους του συστήματος (δεδομένα, υπηρεσίες, υλικό κλπ.). Οι μηχανισμοί ελέγχου πρόσβασης διαδραματίζουν σημαντικό ρόλο στην πρόληψη δραστηριοτήτων που οδηγούν σε παραβίαση της ασφάλειας του Διαδικτύου Πραγμάτων και η έλλειψη ή η ελλιπής

εφαρμογή τέτοιων μηχανισμών μπορεί να προκαλέσει παραβίαση της ασφάλειας του συστήματος. Ακολουθούν οι ιδιότητες ασφαλείας του ελέγχου πρόσβασης:

I. **Ταυτοποίηση:** Οι οντότητες του Διαδικτύου Πραγμάτων αποτελούνται από διάφορα αντικείμενα όπως άτομα, κόμβους αισθητήρων, φορητούς υπολογιστές, φάρμακα κ.λπ., τα οποία πρέπει να αναγνωρίζονται μοναδικά. Υπάρχουν διαφορετικά συστήματα αναγνώρισης που προτείνονται όπως το αναγνωριστικό αντικειμένου RFID, το IPv4, το IPv6, το EPCglobal, το Near Field Communications Forum (NFC) κλπ. Επομένως, η αναγνώριση είναι το χαρακτηριστικό που προσδιορίζει μοναδικά τα αντικείμενα και διαχειρίζεται την ταυτότητά τους, λαμβάνοντας υπόψη την ασφάλεια και την υψηλή επεκτασιμότητα του Διαδικτύου Πραγμάτων.

II. **Έλεγχος ταυτότητας:** Η επιβεβαίωση ότι μια οντότητα είναι αυτή που ισχυρίζεται και τα ληφθέντα δεδομένων είναι τα αναμενόμενα. Ο έλεγχος ταυτότητας σημαίνει επαλήθευση ταυτότητας. Διαδραματίζει σημαντικό ρόλο πριν δημιουργήσει ένα κανάλι επικοινωνίας μεταξύ δύο οντοτήτων. Επίσης, επιβεβαιώνει την αμοιβαία εμπιστοσύνη μεταξύ διαφορετικών αντικειμένων ή χρηστών πιστοποιώντας την ταυτότητά τους.

3.2.3.2. Θέματα Ασφάλειας στο επίπεδο επικοινωνίας του Διαδικτύου Πραγμάτων

Γενικά τα ασύρματα δίκτυα αισθητήρων είναι ευάλωτα σε διάφορους τύπους επιθέσεων. 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. 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.

Τέτοιοι τύποι επιθέσεων παρατίθενται παρακάτω:

Μη εξουσιοδοτημένη πρόσβαση σε RFID: Μια μη εξουσιοδοτημένη πρόσβαση σε ετικέτες που περιέχουν τα δεδομένα ταυτοποίησης είναι ένα μείζον ζήτημα του Διαδικτύου 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. 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 αυτομπλοκάρεται λόγω της σύγχυσης που δημιουργείται.

Επίθεση 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. 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.

Εικόνα 3.8 Επίθεση Ενδιάμεσου Κόμβου.

Επίθεση άρνησης υπηρεσίας (DoS attack): Ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες. Υπάρχουν γενικά δύο μορφές

αυτής της επίθεσης. Η μία είναι η επίθεση κατά την οποία η υπηρεσία αναγκάζεται να καταρρεύσει και να πρέπει να επανεκκινηθεί και η άλλη είναι η αποστολή υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων για εξυπηρέτηση με αποτέλεσμα η υπηρεσία να μην μπορεί να εξυπηρετήσει αυτούς που πραγματικά θέλουν την υπηρεσία. Μια επίθεση άρνησης υπηρεσίας μπορεί να είναι καταστροφική σε ένα περιβάλλον Διαδικτύου Πραγμάτων που απαιτεί διαρκή επικοινωνία των «πραγμάτων».

Μία κατηγορία επίθεσης άρνησης υπηρεσίας είναι η Κατανεμημένη επίθεση άρνησης υπηρεσίας (distributed denial-of-service attack, DDoS attack). Η κυριότερη μορφή των επιθέσεων αυτών χρησιμοποιεί πολλαπλές επιθέσεις μέσω άλλων θυμάτων ή και θυτών.

a. **Jamming:** Παρεμποδίζει το σύνολο του δικτύου παρεμβαίνοντας στις συχνότητες των κόμβων αισθητήρων.
b. **Sybil επίθεση:** Ένας απλός κόμβος παρουσιάζει πολλαπλές ταυτότητες στους άλλους κόμβους στο δίκτυο.
c. **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 επίθεση άρνησης υπηρεσίας (denial of service).

Ο παρακάτω πίνακας συνοψίζει κάποιες επιθέσεις που δέχεται το επίπεδο επικοινωνίας :

Απειλές στο επίπεδο επικοινωνίας του Διαδικτύου Πραγμάτων				
Απειλές	**Τρωτά σημεία**	**Επιπτώσεις / Συνέπειες**	**Οι έννοιες της ασφάλειας που επηρεάζονται**	**Αντίμετρα**
- Μη εξουσιοδοτημένη πρόσβαση σε RFID - επιθέσεις άρνησης εξυπηρέτησης (DoS attack) - επίθεση Ενδιάμεσου Κόμβου (Man-in-the-middle attack) - Flooding	Ανεξέλεγκτη ή απροστάτευτη ροή δεδομένων	- σε κίνδυνο τα δεδομένα - απώλεια δεδομένων - απώλεια επικοινωνίας/σύνδεσης - αδυναμία ελέγχου της συσκευής	- διαθεσιμότητα - εμπιστευτικότητα - ακεραιότητα - ιδιωτικότητα	κρυπτογράφηση των δεδομένων
παρεμβολές (ηλεκτρομαγνητική συμβατότητα)	ασύρματη σύνδεση	απώλεια επικοινωνίας	διαθεσιμότητα	εναλλακτική σύνδεση δικτύου (wired network connection)

Εικόνα 3.9 Επιθέσεις που δέχεται το επίπεδο επικοινώνιας.

3.2.3.3. Θέματα Ασφάλειας στο επίπεδο εφαρμογών του Διαδικτύου Πραγμάτων

Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα: Κάθε εφαρμογή που εκτελείται σε μία συσκευή του Διαδικτύου πραγμάτων μπορεί να έχει μεγάλο αριθμό χρηστών. Επομένως, πρέπει να χρησιμοποιηθεί αποτελεσματική τεχνολογία ελέγχου ταυτότητας για να αποφευχθεί η παράνομη πρόσβαση των χρηστών σε δεδομένα.

Συμπληρωματικά, τα δεδομένα που βρίσκονται αποθηκευμένα σε σύννεφο είναι πιθανό να δεχτούν επίθεση, γεγονός που μπορεί να οδηγήσει σε δεδομένων και σε πιθανή αποτυχία της αντίστοιχης εφαρμογής που τα χρησιμοποιεί. Ως εκ τούτου, είναι σημαντικό να διασφαλίζεται η ασφαλής πρόσβαση στα αποθηκευμένα δεδομένα στο σύννεφο. Ένα άλλο αντίστοιχο ζήτημα είναι η κακόβουλη επίθεση εμπιστευτικών πληροφοριών που αποσκοπεί στην τροποποίηση των δεδομένων.

Ιδιαίτερη προσοχή πρέπει να δοθεί στην περίπτωση που προσωπικά δεδομένα χρηστών αποθηκεύονται σε κοινόχρηστο περιβάλλον στο σύννεφο, στο οποίο μπορεί να υπάρχει πρόσβαση και από άλλες εφαρμογές.

Τέλος, τα Big Data, τα οποία είναι ένας πολύ μεγάλος όγκος αποθηκευμένης πληροφορίας, αποτελεί μία ακόμα πρόκληση για την ασφάλεια.

Επεξεργασία πληροφοριών σε πραγματικό χρόνο: Κάποιες συσκευές (κόμβοι) του Διαδικτύου Πραγμάτων πραγματοποιούν ανάλυση δεδομένων σε πραγματικό χρόνο και προσωρινή αποθήκευση δεδομένων. Το επίπεδο εφαρμογής μπορεί να είναι ευάλωτο σε επιθέσεις με σκοπό την υποκλοπή η αλλοίωση των δεδομένων.

DoS στο επίπεδο εφαρμογής: Το επίπεδο εφαρμογής είναι το κορυφαίο στρώμα του Διαδικτύου πραγμάτων και περιέχει διεπαφή χρήστη. Ένα από τα πιο σημαντικά προβλήματα σε αυτό το επίπεδο είναι το DoS / DDoS. Υπάρχουν δύο τύποι DoS / DDoS στο επίπεδο εφαρμογής:

a. **Επίθεση επαναπρογραμματισμού:** Ένας εισβολέας μπορεί να αποκτήσει πρόσβαση, να τροποποιήσει και να ελέγξει τον πηγαίο κώδικα έτσι ώστε τα αιτήματα της εφαρμογής να μπαίνουν σε άπειρη αναμονή για πόρους δικτύου.
b. **Επίθεση DoS πάνω σε ένα μονοπάτι:** Ένας εισβολέας πλημμυρίζει ένα μονοπάτι επικοινωνίας από άκρο σε άκρο, χρησιμοποιώντας επαναλαμβανόμενα ή ψεύτικα πακέτα. Σε αυτή την περίπτωση οι κόμβοι των αισθητήρων θα συγκλονιστούν και η διάρκεια ζωής του δικτύου θα μειωθεί.

Επιθέσεις εφαρμογών: Υπάρχουν αρκετές επιθέσεις στο επίπεδο εφαρμογής μεταξύ αυτών εξηγούμε τις πιο κοινές, όπως οι επιθέσεις XSS, CSRF και SQL Injection:

a. **Επίθεση Cross-Site Scripting (XSS):** Αυτή η επίθεση λειτουργεί με τρόπο που θέτει σε κίνδυνο τη σχέση εμπιστοσύνης μεταξύ του χρήστη και του ιστότοπου εφαρμογής ιστού με την έγχυση κακόβουλου κώδικα. Οι επιτιθέμενοι μπορούν να ελέγξουν την ακεραιότητα της εφαρμογής.
b. **Επίθεση Cross-Site Request Forgery (CSRF):** Είναι επίσης γνωστή ως επίθεση με ένα κλικ. Αυτή η επίθεση στοχεύει στη μετάδοση κακόβουλων αιτημάτων, τα οποία εμπιστεύεται ο ιστότοπος ή η εφαρμογή προορισμού χωρίς τη συναίνεση του χρήστη από τον οποίον προέρχονται. Ο ιστότοπος εμπιστεύεται τον χρήστη και δε μπορεί να διακρίνει αν αυτά τα αιτήματα είναι αυθεντικά ή όχι
c. **Επίθεση SQL Injection:** Ένας εισβολέας στοχεύει στην έγχυση ενός ερωτήματος SQL από τον πελάτη στην εφαρμογή. Ως εκ τούτου, ο εισβολέας μπορεί να διαβάσει, να τροποποιήσει ή να τροποποιήσει δεδομένα από το σύστημα διαχείρισης βάσεων δεδομένων (DBMS). Επίσης, η εν λόγω

επίθεση, υπό τις κατάλληλες προυποθέσεις, μπορεί να εκτελέσει και διαχειριστικές λειτουργίες πάνω στη βάση δεδομένων, όπως ανάκτηση και τερματισμός της λειτουργίας της. Οι συνέπειες της επίθεσης SQL injection επηρεάζουν την εμπιστευτικότητα, την ακεραιότητα, την εξουσιοδότηση και τον έλεγχο ταυτότητας.

Ασταθής πλατφόρμα: Οι συσκευές του Διαδικτύου Πραγμάτων συχνά διαθέτουν ξεπερασμένη ή ασταθή πλατφόρμα λογισμικού, γεγονός το οποίο αποτελεί κίνδυνο για την ασφάλεια τους και μπορεί να διευκολύνει οποιαδήποτε από τις παραπάνω επιθέσεις.

Απειλές στα υλικά συστατικά και στο επίπεδο εφαρμογών του Διαδικτύου Πραγμάτων				
Απειλές	**Τρωτά σημεία**	**Επιπτώσεις / Συνέπειες**	**Οι έννοιες της ασφάλειας που επηρεάζονται**	**Αντίμετρα**
- εισβολή (μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, επεξεργασία πληροφοριών σε πραγματικό χρόνο) - εκμετάλλευση αδυναμιών (χρήση για άλλους σκοπούς, ασταθής -DoS στο επίπεδο εφαρμογής -Επιθέσεις εφαρμογών Web πλατφόρμα)	- Ανεπαρκής έλεγχος ταυτότητας ή εξουσιοδότησης - Ανασφαλείς διεπαφές χρήστη - Ανασφαλείς υπηρεσίες δικτύου - απροστάτευτα δεδομένα	- σε κίνδυνο τα δεδομένα - απώλεια δεδομένων - αλλοίωση δεδομένων - απώλεια επικοινωνίας - αδυναμία ελέγχου της συσκευής	- διαθεσιμότητα - εμπιστευτικότητα - ακεραιότητα - ιδιωτικότητα - αυθεντικότητα	- κρυπτογράφηση - ψηφιακή υπογραφή
- απώλεια ισχύος - απώλεια δικτύου - κλοπή -καταστροφή - τροποποίηση ή αντικατάσταση αισθητήρα/συσκευής	- φυσική πρόσβαση στη συσκευή - ανεπαρκής έλεγχο ταυτότητας	- απώλεια επικοινωνίας - απώλεια δεδομένων - αλλοίωση δεδομένων	- διαθεσιμότητα - ιδιωτικότητα - ακεραιότητα - εμπιστευτικότητα	- εναλλακτική πηγή ενέργειας - εναλλακτική σύνδεση δικτύου - πιστοποίηση - μετακίνηση συσκευής σε δυπρόσιτη περιοχή δικτύου

Εικόνα 3.10 Απειλές στα υλικά συστατικά και στο επίπεδο εφαρμογών του IoT.

3.3. Παραδείγματα ζητημάτων Ιδιωτικότητας και ασφάλειας σε συσκευές και εφαρμογές του Διαδικτύου πραγμάτων

- Συσκευές που «φέρονται»/«φοριούνται» (Παραδείγματος χάριν Google Glass)

Ζητήματα σχετικά με

- την ενημέρωση όσων βιντεοσκοπούνται
- την κεντρική αποθήκευση των δεδομένων
- την κατοχή τεχνολογίας αναγνώρισης προσώπων από την Google
- την «συνήθεια» στη χρήση τέτοιων γυαλιών αντί των συμβατικών
- τον έλεγχο στη χρήση των δεδομένων

- Body trackers (ανιχνευτές/ιχνηλάτες σώματος)

Ζητήματα:

- Ενδιαφέρον από εργοδότες για τη χρήση των δεδομένων με σκοπό την τιμολόγηση της ασφάλισης των εργαζομένων
- Περιστατικό 2011: Δεδομένα σεξουαλικής συμπεριφοράς στα αποτελέσματα μηχανής αναζήτησης του διαδικτύου. Η προεπιλεγμένη επιλογή για το προφίλ ήταν «δημόσιο».

- Ευφυή δίκτυα - ευφυή συστήματα μέτρησης

Κίνδυνοι:

- ανάλυση των χαρακτηριστικών για συμπεριφορική διαφήμιση
- διακρίσεις όσον αφορά τις τιμές
- πρόσβαση για την επιβολή του νόμου
- ασφάλεια του νοικοκυριού

Ζητήματα προσωπικών δεδομένων:

- Κίνδυνοι για ιδιωτικότητα και προστασία προσωπικών δεδομένων
- Χρήση για δευτερεύοντες σκοπούς
- Απουσία δυνατότητας συγκατάθεσης: ποιος πρέπει να την παρέχει (ιδιοκτήτης συσκευής, φέρουσα συσκευή, υποκείμενο των δεδομένων), σε ποιον και πότε.
- Δημιουργία ατομικού προφίλ
- Λεπτομερής παρακολούθηση
- Λήψη αυτοματοποιημένων αποφάσεων
- Απουσία δυνατότητας να παραμένει κανείς ανώνυμος

- Έλλειψη ασφάλειας
- Ανάγκη βελτιστοποίησης των υπολογιστικών πόρων/ενέργειας από αισθητήρες και αντικείμενα → υλοποίηση μέτρων για εξασφάλιση εμπιστευτικότητας/ακεραιότητας/διαθεσιμότητας
- Διαφορετικά επίπεδα επεξεργασίας → δυσκολία στον συντονισμό εμπλεκομένων μερών (stakeholders) → ύπαρξη τρωτών σημείων

3.4. Νόμοι και κανονισμοί

Στην παγκόσμια κοινωνία της πληροφορίας, υπάρχει σοβαρός κίνδυνος για την ιδιωτικότητα. Ένα βασικό πρόβλημα, είναι ότι η κίνηση σε ένα παγκόσμιο δίκτυο (όπως για παράδειγμα το διαδίκτυο), διασχίζει τα διεθνή όρια και δεν υπάρχει δυνατότητα κεντρικής διαχείρισης. Στο διαδίκτυο, δεν υπάρχει καμία γενική ευθύνη η οποία να ανατίθεται σε μια συγκεκριμένη οντότητα, και δεν υπάρχει κανένας διεθνής μηχανισμός επίβλεψης για να επιβάλει τις νομικές υποχρεώσεις (ειδικά νομοθεσία για την προστασία των δεδομένων).

Έτσι λοιπόν, υπάρχουν σοβαροί κίνδυνοι για την ιδιωτικότητα, επειδή τα προσωπικά δεδομένα που αφορούν τους χρήστες ή άλλα υποκείμενα είναι διαθέσιμα και μπορούν να διαβαστούν ή να ανιχνευτούν σε διαφορετικούς ιστότοπους σε όλο τον κόσμο.

Όσοι εμπλέκονται στην συλλογή και επεξεργασία προσωπικών δεδομένων θα πρέπει να συμμορφώνονται με τη νομοθεσία περί προστασίας δεδομένων στα κράτη μέλη στα οποία πραγματοποιείται η εργασία αυτή στο σύνολό της ή σε τμήματα της που ορίζει ότι τα προσωπικά δεδομένα θα πρέπει:

- να είναι σωστά και νομίμως επεξεργασμένα
- να είναι επεξεργασμένα για περιορισμένους σκοπούς
- να είναι επαρκή, σχετικά και όχι υπερβολικά
- να είναι ακριβή και ενημερωμένα
- να μην φυλάσσονται για μεγαλύτερο χρονικό διάστημα από αυτό που είναι απαραίτητο
- Να υποβάλλονται σε επεξεργασία σύμφωνα με τα δικαιώματα του υποκειμένου των δεδομένων
- Να είναι ασφαλή
- Να μην μεταφέρονται σε άλλες χώρες χωρίς επαρκή προστασία

Όσοι εμπλέκονται στην συλλογή και επεξεργασία προσωπικών δεδομένων τόσο σε ατομικό επίπεδο όσο και σε επίπεδο κοινοπραξίας, θα πρέπει να συμμορφώνονται μεταξύ

άλλων τόσο με τους κανονισμούς του Horizon 2020 (**1982/2006/ΕΚ**) όσο και με τους ξεχωριστούς κανονισμούς και οδηγίες της ΕΕ, όπως:

- Ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ.
- Η οδηγία για την προστασία των δεδομένων (**οδηγία 95/46/ΕΚ** για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών), θα αντικατασταθεί από τον κανονισμό EU General Data Protection Regulation (GDPR) 2016/679) στις 25 Μαΐου 2018. Η κυριότερη επιδίωξη της Οδηγίας ήταν, η δημοκρατία και τα ατομικά δικαιώματα και ελευθερίες, που προστατεύονται από Συντάγματα και νόμους στα διάφορα κράτη μέλη, να συνοδεύονται από τη διατύπωση της ανάγκης για συνεχή διασυνοριακή ροή προσωπικών δεδομένων, ενώ ταυτόχρονα να προστατευτούν τα δικαιώματα του ατόμου, έναντι της ολοένα εντεινόμενης επεξεργασίας και αξιοποίησης προσωπικών πληροφοριών.
- Αξίζει να σημειωθεί ότι σε αντίθεση με τη γενική Οδηγία **95/46/ΕΚ** για την προστασία δεδομένων, η Οδηγία **97/66/ΕΚ** προστάτευε και τα έννομα συμφέροντα των νομικών προσώπων. Η Οδηγία **97/66/ΕΚ** στη συνέχεια αντικαταστάθηκε από την **Οδηγία 2002/58/ΕΚ**, “για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)”. Η υιοθέτηση ιδιαίτερης οδηγίας για την προστασία δεδομένων στον τηλεπικοινωνιακό τομέα, καθώς και η δέσμευση των κοινοτικών υπηρεσιών από τις επιλογές της γενικής οδηγίας, αφενός δηλώνουν την προσήλωση της Κοινότητας στις αρχές προστασίας και αφετέρου αποτελούν υπό μία έννοια το πρώτο δείγμα ειδικών ρυθμίσεων που εξειδικεύουν ανά τομέα τους γενικούς κανόνες της Οδηγίας.
- Η τελευταία κοινοτική **Οδηγία** ήταν η **2006/24/ΕΚ**, «για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας **2002/58/ΕΚ**»
- Οδηγία **2009/136/EC** για την τροποποίηση της οδηγίας **2002/22/EC** (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)

σχετικά με την καθολική υπηρεσία και για τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών.

Ο κατάλογος των κύριων εγγράφων αναφοράς που πρέπει να πληροί κάθε έργο είναι τα εξής:

- Ηθική επισκόπηση στο FP7 - Προστασία δεδομένων και δεοντολογικές κατευθυντήριες γραμμές (Ευρωπαϊκή Επιτροπή).
- Ηθική για τους ερευνητές - Διευκόλυνση της αριστείας στην έρευνα στο FP7 (Ευρωπαϊκή Επιτροπή). Σημείωση οδηγιών για ερευνητές και αξιολογητές κοινωνικών και ανθρωπιστικών επιστημών.
- Έρευνα (Ευρωπαϊκή Επιτροπή).
- Καθοδήγηση Πώς να ολοκληρώσετε την αυτοαξιολόγηση της ηθικής σας (Ευρωπαϊκή Επιτροπή, Γενική Διεύθυνση Έρευνας και Καινοτομίας, Έκδοση 5.0, 15 Μαρτίου 2016).
- Γνωμοδότηση **05/2014** σχετικά με τις τεχνικές ανωνυμοποίησης (ομάδα εργασίας του Άρθρου 29). Γνωμοδότηση **4/2007** σχετικά με την έννοια των προσωπικών δεδομένων (ομάδα εργασίας του Άρθρου 29). Γνωμοδότηση **15/2011** σχετικά με τον ορισμό της συγκατάθεσης (ομάδα εργασίας του Άρθρου 29). Σημείωμα καθοδήγησης για την προστασία δεδομένων και την έρευνα (London School of Economics).
- Καθοδήγηση σχετικά με την προστασία δεδομένων, την εμπιστευτικότητα και τη διαχείριση αρχείων (University of Sussex).
- Λίστα ελέγχου προστασίας δεδομένων (ESOMAR).
- Εισαγωγή στην Προστασία Δεδομένων (EDRI).

Η Ελλάδα ως κράτος μέλος της Ευρωπαϊκής Ένωσης, οφείλει να εναρμονίσει τη νομοθεσία της με βάση τις κοινοτικές Οδηγίες. Έτσι το 1997 ψηφίστηκε ο νόμος **2472/1997** για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και το 2006 ο νόμος **3471/06**, για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Ο νόμος **2472/1997** ενσωματώνει στο ελληνικό δίκαιο την οδηγία **1995/46** για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ρυθμίζει την επεξεργασία δεδομένων προσωπικού χαρακτήρα (τα χαρακτηριστικά των δεδομένων προσωπικού χαρακτήρα, τις προϋποθέσεις επεξεργασίας, τις υποχρεώσεις του

υπευθύνου της επεξεργασίας κλπ) και τα δικαιώματα του υποκειμένου των δεδομένων (ενημέρωσης, πρόσβασης, αντίρρησης, προσωρινής δικαστικής προστασίας).

Ο νόμος **2472/1997** τροποποιήθηκε το 2000 και το 2001 και επιβάλλεται από την Αρχή Προστασίας Προσωπικών Δεδομένων. Συμπληρώνεται από το νόμο **2774/1999** περί προστασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα καθώς και από τον **3115/2003.**

Με το **άρθρο 1 του νόμου 3115/2003** συστάθηκε, σύμφωνα με την **παράγραφο 2 του άρθρου 19 του Συντάγματος**, η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Η ΑΔΑΕ είναι Ανεξάρτητη Αρχή που απολαύει διοικητικής αυτοτέλειας. Έδρα της είναι η Αθήνα, μπορεί όμως με απόφασή της να εγκαθιστά και να λειτουργεί γραφεία και σε άλλες πόλεις της Ελλάδας. Οι αποφάσεις της ΑΔΑΕ κοινοποιούνται με μέριμνά της στον Υπουργό Δικαιοσύνης, ενώ στο τέλος κάθε έτους υποβάλλεται Έκθεση των πεπραγμένων της στον Πρόεδρο της Βουλής, στον Υπουργό Δικαιοσύνης και στους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή και στο Ευρωπαϊκό Κοινοβούλιο.

Η ΑΔΑΕ υπόκειται σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον Κανονισμό της Βουλής.

Τέλος, οι ρυθμίσεις του νόμου **2472/97** συμπληρώθηκαν από το Νόμο **3471/06** (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών). Ο νόμος αυτός κατοχύρωσε σημαντικά δικαιώματα των συνδρομητών και χρηστών τηλεπικοινωνιακών υπηρεσιών.

Γενικός κανονισμός για την προστασία των δεδομένων της Ευρωπαικής Ένωσης – EU General Data Protection Regulation (GDPR)

Ο στόχος του GDPR είναι να προστατεύσει όλους τους πολίτες της ΕΕ από τις παραβιάσεις της ιδιωτικής ζωής και των δεδομένων σε έναν κόσμο όλο και περισσότερο καθοδηγούμενο από δεδομένα, ο οποίος είναι πολύ διαφορετικός από τότε που συστάθηκε η οδηγία του 1995. Μολονότι οι βασικές αρχές της προστασίας της ιδιωτικής ζωής εξακολουθούν να ισχύουν από την προηγούμενη οδηγία, έχουν προταθεί πολλές αλλαγές στις ρυθμιστικές πολιτικές. Τα βασικά σημεία του GDPR καθώς και πληροφορίες για τις επιπτώσεις που θα έχει στις επιχειρήσεις μπορούν να βρεθούν παρακάτω.

- **Αυξημένο εδαφικό πεδίο εφαρμογής (εξωεδαφική εφαρμογή)**

Αναμφισβήτητα η μεγαλύτερη αλλαγή στο ρυθμιστικό περιβάλλον της ιδιωτικής ζωής των δεδομένων έρχεται με την εκτεταμένη δικαιοδοσία του GDPR, καθώς ισχύει για όλες τις εταιρείες που επεξεργάζονται τα προσωπικά δεδομένα των υποκειμένων των δεδομένων που διαμένουν στην Ένωση, ανεξάρτητα από την τοποθεσία της εταιρείας. Προηγουμένως, η εδαφική εφαρμογή της οδηγίας ήταν διφορούμενη και αναφέρεται στη διαδικασία των δεδομένων «στο πλαίσιο μιας εγκατάστασης». Το θέμα αυτό έχει προκύψει σε πολλές περιπτώσεις δικαστικών διαδικασιών. Το GPDR καθίσταται σαφές στην εφαρμογή του - θα εφαρμόζεται στην επεξεργασία προσωπικών δεδομένων από ελεγκτές και μεταποιητές στην ΕΕ, ανεξάρτητα από το εάν η επεξεργασία πραγματοποιείται στην ΕΕ ή όχι. Το GDPR θα εφαρμόζεται επίσης στην επεξεργασία δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων στην ΕΕ από ελεγκτές ή μεταποιητές μη εγκατεστημένους στην ΕΕ, όπου οι δραστηριότητες αφορούν: στην προσφορά αγαθών ή υπηρεσιών σε πολίτες της ΕΕ (ανεξάρτητα από το αν απαιτείται πληρωμή) και στην παρακολούθηση της συμπεριφοράς που λαμβάνει χώρα εντός της ΕΕ. Οι επιχειρήσεις εκτός ΕΕ που επεξεργάζονται τα δεδομένα των πολιτών της ΕΕ θα πρέπει επίσης να διορίσουν έναν εκπρόσωπο στην ΕΕ.

- **Ποινικές ρήτρες**

Σύμφωνα με το GDPR οι εταιρείες / οργανισμοί που το παραβιάζουν, μπορεί να τους επιβληθεί πρόστιμο μέχρι 4% του ετήσιου συνολικού κύκλου εργασιών ή €20 εκατ. (Όποιο είναι μεγαλύτερο). Πρόκειται για το ανώτατο πρόστιμο που μπορεί να επιβληθεί για τις πιο σοβαρές παραβάσεις, π.χ. επεξεργασία δεδομένων χωρίς τη δέουσα συγκατάθεση του πελάτη ή παραβίαση του πυρήνα των εννοιών της Ιδιωτικότητας και Ασφάλειας. Υπάρχει μια κλιμακωτή προσέγγιση για τα πρόστιμα, π.χ. σε μια εταιρεία μπορεί να επιβληθεί πρόστιμο ύψους 2% για μη σωστή τήρηση των αρχείων της (άρθρο 28), για τη μη ενημέρωση της εποπτεύουσας αρχής και το υποκείμενο των δεδομένων για παραβίαση ή μη διενέργεια εκτίμησης αντικτύπου. Είναι σημαντικό να σημειώσουμε ότι αυτοί οι κανόνες ισχύουν τόσο για τους ελεγκτές όσο και για τους μεταποιητές - που σημαίνει ότι το cloud δεν θα εξαιρεθεί από την επιβολή του GDPR.

- **Συγκατάθεση**

Οι όροι για τη συγκατάθεση έχουν ενισχυθεί και οι εταιρείες δεν θα μπορούν πλέον να χρησιμοποιούν μακρούς δυσανάγνωστους όρους και ακατανόητες προϋποθέσεις,

καθώς η αίτηση συναίνεσης πρέπει να παρέχεται με κατανοητή και εύκολα προσπελάσιμη μορφή, με τον σκοπό της επεξεργασίας δεδομένων να επισυνάπτεται με αυτή τη συγκατάθεση. Η συγκατάθεση πρέπει να είναι σαφής και διακριτή από άλλα θέματα και να παρέχεται με κατανοητή και εύκολα προσιτή μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα. Πρέπει να είναι τόσο εύκολο να αποσύρετε τη συγκατάθεση, όσο και να την δώσετε.

Δικαιώματα υποκειμένων δεδομένων

- **Ειδοποίηση παραβίασης**

Σύμφωνα με το GDPR, η κοινοποίηση παραβίασης θα καταστεί υποχρεωτική σε όλα τα κράτη μέλη όπου μια παραβίαση δεδομένων ενδέχεται να "οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων". Αυτό πρέπει να γίνει εντός 72 ωρών από την πρώτη στιγμή της συνειδητοποίησης της παραβίασης. Οι επεξεργαστές δεδομένων θα υποχρεούνται επίσης να ειδοποιούν τους πελάτες τους, τους ελεγκτές, "χωρίς αδικαιολόγητη καθυστέρηση", αφού πρώτα καταλάβουν την παραβίαση δεδομένων.

- **Δικαίωμα πρόσβασης**

Μέρος των διευρυμένων δικαιωμάτων των προσώπων στα οποία αναφέρονται τα στοιχεία του GDPR είναι το δικαίωμα των υποκειμένων των δεδομένων να λαμβάνουν από τον υπεύθυνο επεξεργασίας δεδομένων την επιβεβαίωση του κατά πόσον τα προσωπικά δεδομένα που τους αφορούν υποβάλλονται σε επεξεργασία, πού και για ποιο σκοπό. Επιπλέον, ο ελεγκτής παρέχει δωρεάν αντίγραφο των προσωπικών δεδομένων σε ηλεκτρονική μορφή. Η αλλαγή αυτή είναι μια δραματική αλλαγή στη διαφάνεια των δεδομένων και την ενδυνάμωση των υποκειμένων των δεδομένων.

- **Δικαίωμα στη λήθη**

Επίσης γνωστό ως Διαγραφή Δεδομένων, το δικαίωμα στη λήθη παρέχει στο υποκείμενο των δεδομένων τη δυνατότητα να διαγράψει τα προσωπικά του δεδομένα ο ελεγκτής δεδομένων, να παύσει την περαιτέρω διάδοση των δεδομένων και ενδεχομένως να σταματήσει την επεξεργασία των δεδομένων από τρίτους. Οι όροι για τη διαγραφή, όπως περιγράφονται στο άρθρο 17, περιλαμβάνουν τα δεδομένα που δεν έχουν πλέον σχέση με τους αρχικούς σκοπούς επεξεργασίας ή τα υποκείμενα των δεδομένων που αποσύρουν τη συναίνεση. Πρέπει επίσης να σημειωθεί ότι αυτό το δικαίωμα απαιτεί από τους ελεγκτές να συγκρίνουν τα δικαιώματα των υποκειμένων με το "δημόσιο συμφέρον για τη διαθεσιμότητα των δεδομένων" κατά την εξέταση αυτών των αιτημάτων.

- **Φορητότητα δεδομένων**

Το GDPR εισάγει τη φορητότητα δεδομένων - το δικαίωμα για ένα υποκείμενο των δεδομένων να λαμβάνει τα προσωπικά δεδομένα που το αφορούν, τα οποία είχαν δοθεί στο παρελθόν σε μορφή "κοινής χρήσης και αναγνώσιμη από μηχανή" και έχουν το δικαίωμα να διαβιβάζουν τα δεδομένα αυτά σε άλλον ελεγκτή.

- **Προστασία δεδομένων βάση του σχεδιασμού**

Η προστασία της ιδιωτικής ζωής βάση του σχεδιασμού ως έννοια έχει υπάρξει εδώ και χρόνια, αλλά τώρα γίνεται μέρος της νομικής απαίτησης με το GDPR. Στον πυρήνα της, η προστασία της ιδιωτικής ζωής βάση του σχεδιασμού απαιτεί την ενσωμάτωση της προστασίας των δεδομένων από την εμφάνιση του σχεδιασμού των συστημάτων, από ότι την προσθήκη. Ειδικότερα: «Ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα με αποτελεσματικό τρόπο ώστε να ανταποκρίνεται στις απαιτήσεις του παρόντος κανονισμού και να προστατεύει τα δικαιώματα των υποκειμένων των δεδομένων». Το άρθρο 23 ζητεί από τους ελεγκτές να διατηρούν και να επεξεργάζονται μόνο τα δεδομένα που είναι απολύτως απαραίτητα για την εκπλήρωση των καθηκόντων τους (ελαχιστοποίηση των δεδομένων), καθώς και τον περιορισμό της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε όσους χρειάζονται τη διεξαγωγή της επεξεργασίας.

- **Υπεύθυνοι προστασίας δεδομένων**

Επί του παρόντος, οι υπεύθυνοι επεξεργασίας υποχρεούνται να κοινοποιούν τις δραστηριότητές τους επεξεργασίας δεδομένων σε τοπικές αρχές προστασίας δεδομένων, οι οποίες, για τις πολυεθνικές, μπορεί να είναι ένας γραφειοκρατικός εφιάλτης με τα περισσότερα κράτη μέλη να έχουν διαφορετικές απαιτήσεις κοινοποίησης. Σύμφωνα με το GDPR, δεν θα είναι απαραίτητο να υποβάλλονται ειδοποιήσεις / καταχωρήσεις σε κάθε τοπική αρχή προστασίας επεξεργασίας των δεδομένων, ούτε θα απαιτείται η κοινοποίηση / έγκριση για μεταφορές βάσει των Πρότυπων Ρητρών Σύμβασης (MCC). Αντ 'αυτού, θα υπάρχουν εσωτερικές απαιτήσεις τήρησης αρχείων, και ο διορισμός των DPO θα είναι υποχρεωτικός μόνο για τους ελεγκτές και τους μεταποιητές των οποίων οι κύριες δραστηριότητες συνίστανται σε επεξεργασίες που απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ή ειδικών κατηγοριών δεδομένων ή δεδομένων σχετικά με ποινικές καταδίκες και αξιόποινες πράξεις.

4. Απαιτήσεις Ιδιωτικότητας και Ασφάλειας στο Διαδίκτυο Πραγμάτων

4.1. Απαιτήσεις Ιδιωτικότητας

Για την μετατροπή της ιδιωτικότητας από μία γενική έννοια σε τεχνική απαίτηση έχουν ορισθεί οι επιμέρους απαιτήσεις ιδιωτικότητας από τους (Fischer-Hübner, 2001), (Cannon, 2004), (Καλλονιάτης, 2011) και περιλαμβάνουν τις παρακάτω διαδικασίες:

- **Αυθεντικοποίηση (Authentication):** η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μιας οντότητας. Αποτελεί κυρίως απαίτηση ασφάλειας, παρά ιδιωτικότητας, ωστόσο έχει σημαντική συνεισφορά και στην ικανοποίηση απαιτήσεων ιδιωτικότητας.
- **Εξουσιοδότηση (Authorization)**: η διαδικασία μέσω της οποίας μία οντότητα αποκτά δικαιώματα - πρόσβαση σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος.
- **Αναγνώριση (Identification)**: η διαδικασία μέσω της οποία ελέγχεται αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι.
- **Προστασία Δεδομένων (Data Protection)**: η διαδικασία μέσω της οποίας διασφαλίζονται, σύμφωνα και με την Ευρωπαϊκή Οδηγία 1995/46/ΕΚ, οι κάτωθι αρχές:
  - ✓ Αρχή της νομιμότητας και της δικαιοσύνης.
  - ✓ Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν.
  - ✓ Αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων.
  - ✓ Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων.
  - ✓ Αρχή της ασφάλειας και της ακεραιότητας.
  - ✓ Εποπτεία και Επικύρωση.

- **Ανωνυμία (Anonymity):** η διαδικασία μέσω της οποίας διασφαλίζεται ότι μία οντότητα μπορεί να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει με μια άλλη οντότητα χωρίς να αποκαλύψει την ταυτότητά του.

- **Ψευδωνυμία (Pseydonymity):** η διαδικασία μέσω της οποίας προστατεύεται η αναγνώριση (Identification) μιας οντότητας από μη εξουσιοδοτημένες τρίτες οντότητες.
- **Μη-συνδεσιμότητα (Unlinkability):** η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα μιας οντότητας από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, οδηγώντας έτσι στην αποκάλυψη της ταυτότητάς της.
- **Μη-παρατηρησιμότητα (Unobservability):** η διαδικασία μέσω της οποία προστατεύεται η ιδιωτικότητα μιας οντότητας από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να παρατηρήσουν ή να εντοπίσουν ίχνη της πρώτης.

4.2. Απαιτήσεις Ασφάλειας

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 του Διαδικτύου Πραγμάτων. 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.

Η ασφάλεια των πληροφοριακών συστημάτων στηρίζεται σε **τρεις βασικές ιδέες** οι οποίες είναι απαραίτητες για την ορθή λειτουργία ενός Πληροφοριακού Συστήματος, και είναι οι εξής:

Ακεραιότητα (Integrity): Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια. Για παράδειγμα, μια εφημερίδα που δημοσιεύει τα άρθρα της και στο Διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα.

Διαθεσιμότητα (Availability): Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα

θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. Για παράδειγμα: το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με συνέπεια εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας, προκαλεί το ίδιο αποτέλεσμα.

Εμπιστευτικότητα (Confidentiality): Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή. Για παράδειγμα: με την κλοπή φορητών υπολογιστών από το κατάλληλο τμήμα μιας εταιρίας. Το 2006 μια μελέτη με τη συνεργασία 480 εταιριών έδειχνε ότι 80% των εταιριών είχε πρόβλημα με διαρροή πληροφοριών λόγο κλοπής φορητού.

Εικόνα 4.1 Βασικές Αρχές Ασφάλειας.

Οι θεμελιώδης αρχές χρήσης και λειτουργίας των πληροφοριακών συστημάτων θα πρέπει να ικανοποιούν τις ακόλουθες **απαιτήσεις ασφάλειας** αλλά και να **πληρούν** κάποιες βασικές **ιδιότητες**:

- Οι πληροφορίες που συσχετίζονται με προσωπικά δεδομένα θα πρέπει να **διαχειρίζονται από το συνολικό σύστημα** με σκοπό τη βελτίωση των παρεχομένων υπηρεσιών προς τους πολίτες.
- Η διαχείριση των πληροφοριών θα πρέπει να γίνεται αποκλειστικά από κατάλληλο **εξουσιοδοτημένο προσωπικό**.

- Τα δικαιώματα πρόσβασης στο σύστημα θα πρέπει να έχουν προσδιοριστεί με διαδικασίες ανεξάρτητες της φάσης υλοποίησης του πληροφοριακού συστήματος. Ο καθορισμός των διαδικασιών αυτών γίνεται σε επίπεδο **νομοθετικό** (νόμοι, διατάγματα), **οργανωτικό** (κανόνες λειτουργίας οργανισμού, καθηκοντολόγιο) και **δομικό** (κατάλληλη στελέχωση, υπεύθυνη επιτροπή ασφάλειας).
- Η **παροχή εμπιστευτικών πληροφοριών** προς τρίτους θα επιτρέπεται κατόπιν έγγραφης άδειας του άμεσα ενδιαφερόμενου.
- Οι **μηχανισμοί ασφάλειας**, δε θα πρέπει να μειώνουν τη συνολική αποτελεσματικότητα του συστήματος. Στη περίπτωση που δεν είναι δυνατή η εφαρμογή του προηγούμενου αξιώματος, θα πρέπει να υπάρχει ικανοποιητική ισορροπία μεταξύ απόδοσης και ασφάλειας του συστήματος.
- Η σωστή ανάπτυξη και η αποδοτική λειτουργία πληροφοριακών συστημάτων είναι μια διαδικασία, που εμπεριέχει αναπόσπαστα τη ταυτόχρονη δόμηση ενός **πλαισίου ασφάλειας**, το οποίο να εξασφαλίζει τις απαιτήσεις ορθότητας, διαθεσιμότητας και μυστικότητας των περιεχομένων πληροφοριών.
- **Ευχρηστία (Usability).** Το σύστημα πρέπει να είναι σχεδιασμένο με στόχο την διευκόλυνση του χρήστη.
- **Γενικότητα (Generality).** Το σύστημα πρέπει να μπορεί να εκτελέσει ποικίλες διαδικασίες, σύμφωνα με τις ανάγκες του χρήστη.
- **Αποδοτικότητα (Effeciency).** Το σύστημα πρέπει να λειτουργεί γρήγορα και ορθά, χρησιμοποιώντας κατά βέλτιστο τρόπο τους διατιθέμενους πόρους.
- **Ευελιξία (Flexibility).** Το σύστημα πρέπει να μπορεί να προσαρμόζεται σε διαρκώς μεταβαλλόμενες καταστάσεις
- **Αδιαφάνεια (Opacity).** Ο χρήστης πρέπει να γνωρίζει μόνο ότι είναι απαραίτητο για να διεκπεραιώσει την εργασία του .
- **Ασφάλεια (Security).** Το σύστημα πρέπει να διαφυλάσσει τα δεδομένα ενός χρήστη από μη εξουσιοδοτημένη χρήση τους από άλλους.
- **Ακεραιότητα (Integrity).** Οι χρήστες και τα δεδομένα τους πρέπει να διαφυλάσσονται από απρόβλεπτες μετατροπές από μη εξουσιοδοτημένους χρήστες.
- **Ευκινησία (Capacity).** Οι χρήστες δεν πρέπει να υφίστανται άσκοπους περιορισμούς στις ενέργειές τους.

5. Μέτρα επίτευξης Ιδιωτικότητας και Ασφάλειας στο Διαδίκτυο Πραγμάτων και ελαχιστοποίησης απειλών-κινδύνων

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.

Τα μέτρα ελαχιστοποίησης των απειλών και κινδύνων που θα παρουσιαστούν σε αυτό το κεφάλαιο, δε θα διαχωριστούν σε μέτρα για την Ιδιωτικότητα και μέσα για την Ασφάλεια, διότι τα περισσότερα προτεινόμενα μέσα συμβάλουν στην βελτίωση και των δύο.

Αυθεντικοποίηση (Authentication)

Η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα του χρήστη. Επίσης, επιβεβαιώνει την αμοιβαία εμπιστοσύνη μεταξύ διαφορετικών αντικειμένων ή χρηστών πιστοποιώντας την ταυτότητά τους. Υπάρχουν διάφορες διαδικασίες αυθεντικοποίησης που μπορούν να χρησιμοποιηθούν για την επιβεβαίωση της ταυτότητας ενός χρήστη. Τα συνθηματικά είναι ο πλέον συνηθισμένος τρόπος, ο οποίος βασίζεται στη χρήση ενός μυστικού, γνωστού μόνο στο χρήστη. Άλλοι μηχανισμοί αυθεντικοποίησης περιλαμβάνουν συνδυασμούς κρυπτογραφίας και πρωτοκόλλων εξακρίβωσης της ταυτότητας του χρήστη.

Διάφορα αντικείμενα, όπως έξυπνες κάρτες, τα οποία έχει στην κατοχή του ο χρήστης, μπορούν επίσης να χρησιμοποιηθούν για αυθεντικοποίηση στο σύστημα. Ένας άλλος τρόπος εξακρίβωσης της ταυτότητας, περιλαμβάνει την εξέταση διάφορων βιομετρικών χαρακτηριστικών του χρήστη, όπως είναι τα δακτυλικά αποτυπώματα. Ο συνδυασμός πολλαπλών τεχνολογιών εξακρίβωσης της ταυτότητας, έχει ως αποτέλεσμα ισχυρότερη αυθεντικοποίηση.

Εξουσιοδότηση (Authorization)

Η διαδικασία μέσω της οποίας ο χρήστης αποκτά δικαιώματα-πρόσβαση σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός συστήματος. Αν σε ένα σύστημα υπάρχουν πολλοί χρήστες, τότε ο διαχειριστής του συστήματος φροντίζει να εξουσιοδοτεί τον καθένα από αυτούς με τα αντίστοιχα δικαιώματα, ανάλογα με το ρόλο τους και τις υποχρεώσεις τους στο σύστημα.

Από τη στιγμή που έχει διακριβωθεί η ταυτότητα ενός χρήστη μέσω της αυθεντικοποίησης, το σύστημα θα πρέπει να φροντίζει έτσι ώστε ο χρήστης αυτός να μπορεί να ενεργήσει μόνο στα πλαίσια των κανόνων που καθορίζονται από την πολιτική ασφάλειας. Αυτό επιτυγχάνεται εφαρμόζοντας ελέγχους προσπέλασης. Σχετικά με τους ελέγχους προσπέλασης ισχύουν οι ακόλουθες έννοιες:

- **Υποκείμενα.** Πρόκειται για τις ενεργές οντότητες στο σύστημα (χρήστες, διεργασίες, υπηρεσίες)
- **Αντικείμενα.** Με τον όρο αυτό περιγράφονται οι πόροι ή οι παθητικές οντότητες στο σύστημα (αρχεία, συσκευές, προγράμματα)
- **Τρόπος προσπέλασης.** Ο όρος αυτός αναφέρεται στην ενέργεια που πραγματοποιεί ένα υποκείμενο σε ένα αντικείμενο π.χ. ανάγνωση, εγγραφή, εκτέλεση, αναφορά ιδιοχαρακτηριστικών.

Η εξουσιοδότηση συνίσταται στην εξέταση αν το υποκείμενο έχει δικαίωμα για τον συγκεκριμένο τρόπο προσπέλασης στο αντικείμενο, και στην απαγόρευση της ενέργειας, αν τελικά δεν υπάρχει το σχετικό δικαίωμα.

Αναγνώριση και ταυτοποίηση (Identification)

Η διαδικασία μέσω της οποίας ελέγχεται αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι.

Οι οντότητες του Διαδίκτυου Πραγμάτων αποτελούνται από διάφορα αντικείμενα όπως άτομα, κόμβους αισθητήρων, φορητούς υπολογιστές, φάρμακα κ.λπ., τα οποία πρέπει να αναγνωρίζονται μοναδικά. Η αναγνώριση είναι το χαρακτηριστικό που προσδιορίζει μοναδικά τα αντικείμενα και διαχειρίζεται την ταυτότητά τους, λαμβάνοντας υπόψη την ασφάλεια και την υψηλή επεκτασιμότητα του Διαδικτύου Πραγμάτων.

Όλοι οι χρήστες του συστήματος (τεχνικό προσωπικό, διαχειριστές, προγραμματιστές, κοινοί χρήστες κλπ.), θα πρέπει να έχουν ένα μοναδικό αναγνωριστικό (user ID), για καθαρά προσωπική τους χρήση. Τα user IDs δεν πρέπει να φανερώνουν τα δικαιώματα του χρήστη στο σύστημα. Μια ομάδα μπορεί να μοιράζεται το ίδιο user ID για την εκτέλεση συγκεκριμένων εργασιών, μόνο σε εξαιρετικές περιπτώσεις, και εφόσον κάτι τέτοιο είναι απαραίτητο για το σύστημα/εφαρμογή. Σε μια τέτοια περίπτωση θα πρέπει να υπάρχει ειδική έγκριση, όπως επίσης και να χρησιμοποιηθεί κάποιος μηχανισμός που θα καθορίζει τις ευθύνες των μελών της ομάδας. Υπάρχει και ο μηχανισμός της Διαχείριση ταυτότητας, όπου η ταυτότητα ενός χρήστη μπορεί να διαχειριστεί διαιρώντας την ταυτότητα ενός ατόμου σε υπο-ταυτότητες, όπου κάθε υπο-ταυτότητα είναι ψευδώνυμο που έχει επιλέξει ο χρήστης. Ένας χρήστης μπορεί να εκχωρήσει οποιαδήποτε υπο-

ταυτότητα για οποιοδήποτε υποσύστημα /υποεφαρμογή. Αυτό επιτρέπει την απόκρυψη ευαίσθητων δεδομένων.

Στην περίπτωση των συσκευών του Διαδικτύου Πραγμάτων, η ταυτοποίηση είναι μία δύσκολη διαδικασία καθώς απαιτεί τη δημιουργία κατάλληλης υποδομής με εξυπηρετητές ώστε να διασφαλίζεται ότι το εκάστοτε αντικείμενο ή η συσκευή ανάγνωσης είναι πραγματική. Με δεδομένο ότι οι παθητικές ετικέτες δεν μπορούν να ανταλλάξουν πολλά μηνύματα με τους εξυπηρετητές ταυτοποίησης, καθίσταται πολλή δύσκολη η διαδικασία της ταυτοποίησης στο Διαδίκτυο των Αντικειμένων. Ωστόσο υπάρχουν προτάσεις για την υλοποίηση της συγκεκριμένης λειτουργίας.

Υπάρχουν διαφορετικά συστήματα αναγνώρισης που προτείνονται όπως το αναγνωριστικό αντικειμένου RFID, το IPv4, το IPv6, το EPCglobal, το Near Field Communications Forum (NFC). Ένας τρόπος ταυτοποίησης είναι το πρωτόκολλο yoking, το οποίο παρέχει κρυπτογραφημένες πληροφορίες ότι δύο ετικέτες δεν έχουν διαβαστεί ταυτόχρονα και στοιχεία ότι δεν έχουν διαβαστεί σε απόσταση μεταξύ τους. Επίσης υπάρχει το κλιμακωτό σύστημα ονομασίας φυσικών αντικειμένων (PONS) που επαναχρησιμοποιεί τις υπάρχουσες οντολογίες και εκχωρεί σημασιολογικά αναγνωριστικά με βάση τη διεύθυνση URL. Μια άλλη προσέγγιση είναι ένα σύστημα διαχείρισης ταυτότητας αντικειμένου (IdM). Τα υπάρχοντα συστήματα IdM αποτελούνται από δύο τύπους οντοτήτων, οι οποίοι είναι πάροχοι ταυτότητας (IdP) και πάροχος υπηρεσιών (SP), για τη διαχείριση της εξουσιοδότησης και για την παροχή υπηρεσιών πρόσβασης και διαχείρισης ταυτότητας αντίστοιχα.

Προστασία Δεδομένων (Data Protection)

Η διαδικασία μέσω της οποίας διασφαλίζονται σύμφωνα και με την Ευρωπαϊκή Οδηγία 1995/46/ΕΚ, οι κάτωθι αρχές:

- Αρχή της νομιμότητας και της δικαιοσύνης
- Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν
- Αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων
- Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων
- Αρχή της ασφάλειας και της ακεραιότητας
- Εποπτεία και Επικύρωση

Ανωνυμία (Anonymity)

Η διαδικασία μέσω της οποίας διασφαλίζεται ότι ένας χρήστης μπορεί να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει με έναν άλλο χρήστη, χωρίς να αποκαλύψει την ταυτότητά του. Σύμφωνα με τους Pfitzmann και Hansen (2007), ανωνυμία μιας οντότητας σημαίνει ότι αυτή δεν είναι αναγνωρίσιμη μέσα σε ένα σύνολο οντοτήτων. Το σύνολο αυτό περιλαμβάνει όλες τις οντότητες που μετέχουν σε μια επικοινωνία και που πιθανόν θα μπορούσαν να αναγνωρισθούν από διάφορους επιτιθέμενους. Ανάλογα με το ρόλο που έχει ο χρήστης στην επικοινωνία, έχουν καθοριστεί δύο μορφές ανωνυμίας: η ανωνυμία του αποστολέα (sender anonymity) και η ανωνυμία του παραλήπτη (receiver anonymity). Η ανωνυμία του αποστολέα σημαίνει ότι σε μια επικοινωνία ο χρήστης που έχει το ρόλο του αποστολέα παραμένει ανώνυμος ενώ ο παραλήπτης όχι. Το αντίστοιχο συμβαίνει στην ανωνυμία του παραλήπτη.

Ψευδωνυμία (Pseydonymity)

Ψευδωνυμία είναι η διαδικασία μέσω της οποίας προστατεύεται η αναγνώριση του χρήστη από μη εξουσιοδοτημένους τρίτους χρήστες. Η Fischer-Hubner (2001) ορίζει την ψευδωνυμία ως την απαίτηση που διασφαλίζει την απόκρυψη της ταυτότητας του χρήστη όταν αυτός ενεργεί στα πλαίσια μίας επικοινωνίας χρησιμοποιώντας ένα ή περισσότερα ψευδώνυμα. Η ψευδωνυμία υλοποιείται όταν δεν μπορεί να υλοποιηθεί η ανωνυμία.

Μη συνδεσιμότητα (Unlinkability)

Η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα του χρήστη από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, οδηγώντας έτσι στην αποκάλυψη της ταυτότητάς του χρήστη. Στην ουσία, μη συνδεσιμότητα σημαίνει πως ο επιτιθέμενος δεν είναι σε θέση να διακρίνει αν τα στοιχεία που τον ενδιαφέρουν μέσα σε ένα σύστημα (χρήστες, μηνύματα που εστάλησαν κτλ), σχετίζονται μεταξύ τους ή όχι.

Μη παρατηρησιμότητα (Unobservability)

Η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα του χρήστη από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να παρατηρήσουν ή να εντοπίσουν ίχνη του πρώτου. Σύμφωνα με τους Pfitzmann και Hansen (2007), μία οντότητα (π.χ. χρήστης, μήνυμα, ενέργεια) είναι μη-παρατηρήσιμη σε ένα σύνολο οντοτήτων όταν: α) ο επιτιθέμενος δεν μπορεί να εντοπίσει την οντότητα αυτή και β) ο

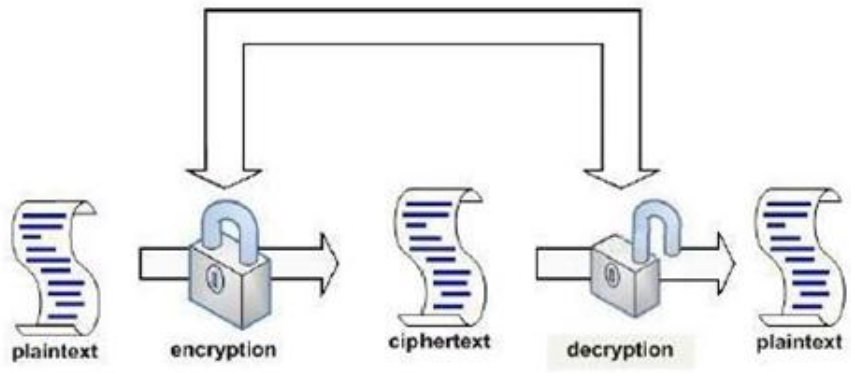
κάτοχος της οντότητας αυτής παραμένει ανώνυμος σε σχέση με τους άλλους κατόχους των υπόλοιπων οντοτήτων.

Κρυπτογραφία

Η κρυπτογραφία (Encryption) είναι μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Η κρυπτογράφηση στο διαδίκτυο έχει σκοπό την διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της μη αποποίησης ευθύνης στις συναλλαγές προστατεύοντας έτσι την ιδιωτικότητα του χρήστη. Στόχος της κρυπτογραφίας είναι να επικοινωνούν δύο άνθρωποι από ένα μη ασφαλές κανάλι χωρίς να υποκλαπεί το μήνυμά τους. Υπάρχουν διεθνή πρότυπα, και η ΑΔΑΕ οφείλει να εκδίδει τεχνικές οδηγίες και συστάσεις που θα καθορίζουν το μήκος του κλειδιού ανά πεδίο κρυπτογράφησης. Το επίπεδο της κρυπτογράφησης πρέπει να είναι τέτοιο ώστε η παραβίαση να μην είναι δυνατή σε λογικό χρόνο και με λογικούς υπολογιστικούς πόρους.

Ένα κρυπτοσύστημα αποτελείται από τις εξής πέντε παραμέτρους:

- Τα plaintexts
- Τα cipher texts
- Τα κλειδιά
- Την κρυπτογραφική μετατροπή ή κρυπτογραφική συνάρτηση
- Την αντίθετη συνάρτηση ή αποκρυπτογραφική μετατροπή



Εικόνα 5.1 Κρυπτογράφηση και αποκρυπτογράφηση.

Ενδεικτικοί αλγόριθμοι είναι οι εξής: RSA, Diffie Helman και El Gamal για ασύμμετρη κρυπτογραφία, 3DES(Data Encryption Standard), AES (Advanced Encryption Algorithm), Blowfish, CAST για συμμετρική κρυπτογραφία.

Τυπικά οι αλγόριθμοι κρυπτογράφησης χρειάζονται ένα μεγάλο μέρος από τους πόρους του συστήματος, δηλαδή σε ισχύ και εύρος ζώνης, και στη πηγή αλλά και στο προορισμό. Τέτοιου είδους λύσεις όμως συχνά δεν μπορούν να εφαρμοστούν στο Διαδίκτυο των αντικειμένων με δεδομένο τις περιορισμένες δυνατότητες σε ισχύ και υπολογιστική ικανότητα των ετικετών ή κάποιων αισθητήρων. Συνεπώς πρέπει να βρεθούν λύσεις ασφαλείας που να παρέχουν την επιθυμητή ποιότητα ασφαλείας με την ελάχιστη χρήση πόρων. Ένας τρόπος κρυπτογραφίας είναι η χρήση ελαφριού τύπου συμμετρικών κλειδιών. Μία άλλη λύση που έχει προταθεί είναι η επανετικετοποίηση (Relabeling), η οποία προτείνει την εξάλειψη των μοναδικών αναγνωριστικών και την αντικατάστασή τους με ένα μηχανισμό δημιουργίας καινούριων ετικετών, Ενώ όμως οι συσκευές με δυνατότητες υψηλής ισχύς όπως οι συσκευές ανάγνωσης μπορούν να επανετικετοποιούν, οι ετικέτες συνήθως παθητικές ετικέτες RFID δε μπορούν. Για αυτό το λόγο προτείνεται η χρήση ενός μινιμαλιστικού τρόπου κρυπτογράφησης, όπου κάθε ετικέτα μπορεί να περιέχει μία συλλογή από ψευδώνυμα. Με περιστροφή των ψευδωνύμων δίνεται σε κάθε αναζήτηση από τη συσκευή ανάγνωσης και διαφορετικό.

Ασύμμετρη Κρυπτογραφία ή Κρυπτογραφία Δημοσίου-Ιδιωτικού κλειδιού

Η ασύμμετρη κρυπτογραφία (Public Key Cryptography) είναι ένα από τα βασικότερα είδη κρυπτογράφησης η οποία εγγυάται την αυθεντικοποίηση των χρηστών ενός συστήματος. Αυτό το είδος κρυπτογράφησης απαιτεί την ύπαρξη δύο κλειδιών, ενός δημοσίου (public key) και ενός ιδιωτικού (private key). Το δημόσιο κλειδί δημοσιοποιείται, ενώ το ιδιωτικό κρατείται πάντοτε μυστικό. Το ιδιωτικό κλειδί δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στο δημόσιο κλειδί. Η ανάγκη να μοιράζεται ο αποστολέας με τον παραλήπτη το ίδιο κλειδί εξαφανίζεται. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η διαπιστευμένη και επιβεβαιωμένη συσχέτιση των δημόσιων κλειδιών με τους κατόχους τους, ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστογραφία. Το ιδιωτικό κλειδί είναι μαθηματικά συνδεδεμένο με το δημόσιο κλειδί. Τυπικά, λοιπόν, είναι δυνατόν να «σπάσει» ένα τέτοιο κρυπτοσύστημα ανακτώντας το ιδιωτικό κλειδί από το δημόσιο.

Συμμετρική Κρυπτογραφία

Στη συμμετρική κρυπτογραφία (Symmetric Cryptography ή Secret-Key Cryptography) ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να το αποκρυπτογραφήσει. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση αλλά και για πιστοποίηση ταυτότητας.

Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη τη διακινούμενη πληροφορία, χωρίς κάποιον άλλον να λάβει γνώση αυτού. Σε γενικές γραμμές, οι αλγόριθμοι ασύμμετρου κλειδιού είναι πιο αργοί από τους αλγόριθμους συμμετρικού κλειδιού. Για το λόγο αυτό, χρησιμοποιούνται κυρίως για ασφαλή μετάδοση συμμετρικών κλειδιών και για κρυπτογράφηση δεδομένων μικρού μεγέθους (PINs και αριθμούς πιστωτικών καρτών). Τέλος, λόγω των πλεονεκτημάτων που παρουσιάζουν, χρησιμοποιούνται ευρέως και σε πρωτόκολλα όπως TLS (Transport Layer Security), IPSec (IP Security) και SSH (Secure Shell).

Ψηφιακές υπογραφές

Ο σκοπός της τεχνικής των ψηφιακών υπογραφών είναι να συνδυάσει μοναδικά την πληροφορία με την ταυτότητα του κατόχου της. Πρόκειται για ένα εργαλείο που παρέχει ακεραιότητα των δεδομένων και πιστοποίηση ταυτότητας. Η έννοια πιστοποίηση ταυτότητας περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων και την ταυτοποίηση ενός υπολογιστή. Οι ψηφιακές υπογραφές επιτυγχάνουν την πιστοποίηση ταυτότητας, παράγοντας ένα σύνολο πληροφοριών που βασίζεται στο έγγραφο και σε ιδιωτικά στοιχεία το αποστολέα. Το σύνολο αυτό δημιουργείται μέσω μιας συνάρτησης κατακερματισμού και του ιδιωτικού κλειδιού του αποστολέα.

Η σωστή εφαρμογή της ψηφιακής υπογραφής σε ένα κρυπτογραφημένο σύστημα διασφαλίζει θεμελιώδεις απαιτήσεις ασφαλείας όπως την αυθεντικότητα των δεδομένων και της πηγής (data origin authentication, data source authentication), την ακεραιότητα της πληροφορίας (data integrity) την εξουσιοδότηση του υπογράφοντα (authorization) και την αποφυγή άρνησης αποστολής της από αυτόν (non-repudiation). Η απαίτηση για non-repudiation προσθέτει ένα επιπλέον επίπεδο ασφαλείας σε ένα κρυπτογραφημένο σύστημα καθώς, εάν ο δημιουργός μιας υπογραφής την αποστείλει και στη συνέχεια το αρνηθεί, αυτό σημαίνει ότι ψεύδεται διότι η υπογραφή θα επικυρώνεται

με τη χρήση του δημοσίου κλειδιού. Παραδείγματα εφαρμογών είναι η ασφάλεια οικονομικών συναλλαγών, η προστασία του λογισμικού (διασφαλίζεται η αυθεντικότητα και η ακεραιότητα του) και η ασφάλεια της ηλεκτρονικής αρχειοθέτησης (Electronic Filing)

Πρωτόκολλα επικοινωνίας

Έρευνες σε πρωτόκολλα δίνουν λύσεις στην ακεραιότητα, την αυθεντικότητα και το απόρρητο των συσκευών, καθώς αναπτύσσεται η ανθεκτικότητα του δικτύου. Τέτοια πρωτόκολλα είναι το TLS ή το DTLS καθώς και το IPv6 με το IPsec.

- **Πρωτόκολλο 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.

Εικόνα 5.2 Πρωτόκολλο 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:

  - προστασία από την αλλοίωση των δεδομένων
  - προστασία εναντίον των επιθέσεων
  - κωδικοποίηση δεδομένων

Επικοινωνία κόμβων

Για την προστασία από τις επιθέσεις που πραγματοποιούνται κατά τη διάρκεια της επικοινωνίας των συσκευών-κόμβων του Διαδικτύου Πραγμάτων, 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 ενδιάμεσοι κόμβοι 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.

Συμπληρωματικά, με τη χρήση κατάλληλων πρωτοκόλλων επικοινωνίας ανάμεσα στους κόμβους, μπορεί να επιτευχθεί το απόρρητο τοποθεσίας του αποστολέα των δεδομένων. Τέτοιο πρωτόκολλο είναι η δρομολόγηση σε έναν τυχαία επιλεγμένο ενδιάμεσο κόμβο (routing to a randomly selected intermediate node -**RRIN**). Η καταγραφή και ο εντοπισμός των πακέτων μπορεί να προληφθεί από το πρωτόκολλο δρομολόγησης απορρήτου τοποθεσίας (Location Privacy Routing - **LPR),** το οποίο κατανέμει ομοιόμορφα τις κατευθύνσεις εισερχόμενης και εξερχόμενης κίνησης σε κόμβους αισθητήρων. Η δρομολόγηση - φάντασμα μιας διαδρομής (**Phantom single-path routing**) διασφαλίζει ότι τα πακέτα φτάνουν στον σταθμό-βάση (**Base Station**) ακολουθώντας διαφορετικές διαδρομές με τέτοιο τρόπο ώστε κάθε πακέτο που δημιουργείται από μια πηγή να ακολουθεί μια διαφορετική τυχαία πορεία προς το σταθμό-βάση.

Μηχανισμοί Ασφαλείας Συσκευών

Οι συσκευές του Διαδικτύου Πραγμάτων θα πρέπει να εφαρμόζουν μηχανισμούς φυσικής ασφάλειας και κρυπτογραφικούς μηχανισμούς ασφαλείας. Οι μηχανισμοί φυσικής ασφάλειας περιλαμβάνουν: μηχανισμό εντολής kill, ηλεκτροστατικό μηχανισμό θωράκισης, ενεργό ετικέτα παρεμβολής και αποκλεισμού. Αυτοί οι μηχανισμοί αυξάνουν το κόστος του υλικού και είναι δύσκολο να ενοποιηθούν.

Τείχος Προστασίας (Firewall)

Η χρήση του τείχους προστασίας στα επίπεδα του Διαδικτύου Πραγμάτων όπου είναι εφικτό (π.χ. στις βάσεις δεδομένων μιας υποδομής) μπορεί να συνεισφέρει στην αποτροπή/ανίχνευση εισβολών και στην αποτροπή SQL injections.

Ενημέρωση/εκπαίδευση χρηστών

Είναι απαραίτητο όλοι οι χρήστες να είναι ενημερωμένοι για τους μηχανισμούς ασφαλείας που τους προσφέρονται και για το πώς μπορούν οι ίδιοι να συμβάλουν στην εφαρμογή και ενδυνάμωση τους. Ενέργειες που μπορούν να πραγματοποιηθούν από τους χρήστες περιλαμβάνουν την επιλογή ισχυρού κωδικού προσβάσεως και τη συχνή αλλαγή του, την τακτική ενημέρωση όσων συσκευών χρησιμοποιούν στο Διαδίκτυο Πραγμάτων, την εγκατάλειψη παλιών συσκευών που πιθανώς να μην έχουν επαρκείς μηχανισμούς

ασφάλειας, την χρήση των συσκευών μόνο για τον ενδεδειγμένο σκοπό τους, την αποφυγή σύνδεσης σε άγνωστα δίκτυα, αλλά και ενέργειες που πραγματοποιούν και για την ασφάλεια τους στο διαδίκτυο, όπως την προσοχή κατά το άνοιγμα ύποπτης ηλεκτρονικής αλληλογραφίας.

Για να μην αφήνεται έρμαιο στα χέρια των συσκευών ανάγνωσης και σε αυτούς που τις διαχειρίζονται, ο χρήστης θα πρέπει να μπορεί να προστατεύει τα προσωπικά του δεδομένα, επιλέγοντας ποια δεδομένα του θα ανταλλάσσονται σε περίπτωση ερώτησης από κάποια συσκευής ανάγνωσης, ποιος θα συλλέγει τα δεδομένα αυτά, όπως επίσης και το χρόνο της συλλογής τους. Επιπλέον θα πρέπει να γνωρίζει το χρόνο παραμονής των δεδομένων του στις συσκευές ανάγνωσης, ο οποίος δε πρέπει να υπερβαίνει τον απαιτούμενο. Αυτό φυσικά προϋποθέτει και τη συμμόρφωση των εφαρμογών στα αντίστοιχα θέματα αλλά και την δυνατότητα ρύθμισης των παραπάνω ρυθμίσεων από τον χρήστη.

Νόμοι και κανονισμοί

Είναι απαραίτητο να δημιουργηθούν νέοι νόμοι και κανονισμοί και να ενημερωθούν οι εν ισχύ σχετικά με τα θέματα που έχουν προκύψει τα τελευταία χρόνια από το Διαδίκτυο των Πραγμάτων. Επίσης, οι σχετικοί νόμοι και οι κανονισμοί θα πρέπει να ενημερώνονται συχνά, εφόσον η τεχνολογία και οι εξελίξεις προχωρούν με ταχύ ρυθμό.

Δημιουργία αντιγράφων ασφαλείας και ανάκτηση (Backup and recovery)

Τα δεδομένα που αποθηκεύονται είτε τοπικά στις συσκευές του Διαδικτύου Πραγμάτων είτε σε Βάσεις Δεδομένων είτε στο σύννεφο, είναι πιθανοί στόχοι επιθέσεων. Γι΄αυτό το λόγο είναι απαραίτητο να υπάρχουν μηχανισμοί δημιουργίας αντιγράφων ασφαλείας, έτσι ώστε σε περίπτωση απώλειας ή κλοπής τους, να είναι εφικτή η ανάκτηση τους.

Επίσης είναι σημαντικό σε περίπτωση επίθεσης σε ένα οποιοδήποτε μηχανισμό του Διαδικτύου Πραγμάτων, έχουν δημιουργηθεί οι αντίστοιχοι μηχανισμοί ανάκτησης λειτουργίας, και να υπάρχει ένα πλάνο ενεργειών ώστε να είναι όσο το δυνατόν πιο άμεση η επαναφορά του συστήματος και η επαναφορά στην φυσιολογική κατάσταση λειτουργίας.

Ασφάλεια κατά τον κύκλο ζωής συσκευών

Η ασφάλεια των συσκευών στο Διαδίκτυο των πραγμάτων με τους παραπάνω αναφερόμενους τόπους θα πρέπει να παρέχεται σε όλη τη διάρκεια του κύκλου ζωής της συσκευής και αφορά σε γενικές γραμμές τα εξής:

a. **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.
b. **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.
c. **Ταυτότητας συσκευής**: Όταν η συσκευή είναι συνδεδεμένη στο δίκτυο, θα πρέπει να πιστοποιείται πριν από τη λήψη ή τη μετάδοση δεδομένων.
d. **Firewalls και IPS**: Η συσκευή χρειάζεται επίσης ένα τείχος προστασίας και το δικό του πρωτόκολλο επικοινωνίας με άλλες συσκευές.
e. **Ενημερώσεις:** οι συσκευές θα πρέπει να είναι σε θέση να κάνουν ενημερώσεις.

Θέματα ιδιωτικότητας	**Λύσεις του Διαδικτύου Πραγμάτων**
Έκθεση δεδομένων	κρυπτογράφηση, τη διαίρεση δεδομένων σε τομείς, την ανάλυση ευαίσθητων δεδομένων ως ιδιωτικών ή μη
Επιθέσεις στον κυβερνοχώρο	Μεθόδων ανίχνευσης και ανάκτησης του συστήματος
Υποκλοπή και εμπιστευτικότητα των δεδομένων	απόκρυψη δεδομένων και κρυπτογραφικές τεχνικές
Απειλές ταυτότητας και ιδιωτικότητα αποθηκευμένων δεδομένων	Ψευδονοποίηση δεδομένων, διαχείριση ταυτότητας, ανωνυμία
Ιδιωτικότητα της τοποθεσίας	Πρωτόκολλα Ασφάλειας

Εικόνα 5.3 Κύρια Θέματα Προστασίας Προσωπικών Δεδομένων και οι αντίστοιχες λύσεις που βασίζονται στο IoT.

6. Συμπεράσματα και προτάσεις για το έργο σε εξέλιξη

Κατά την περίοδο συγγραφής της παρούσης Διπλωματικής εργασίας, βρίσκεται σε εξέλιξη η υλοποίηση ενός ευρωπαϊκού έργου στο Διαδίκτυο των Πραγμάτων. Το έργο έχει ως σκοπό τη δημιουργία ενός ανοιχτού development framework, το οποίο θα διευκολύνει τη μεταφορά της τεχνολογίας παιχνιδιών σε περιβάλλοντα τα οποία δε θα έχουν ως σκοπό την αναψυχή (για παράδειγμα για εκπαιδευτικούς σκοπούς). Στο πλαίσιο αυτό, επικεντρώνεται στην ανάπτυξη λύσεων λογισμικού που βελτιώνουν τη διαδραστική αλληλεπίδραση όλων των συμμετεχόντων σχετικά με τον κύκλο ζωής ενός Σοβαρού Παιχνιδιού (Serious Game – SG) και διευκολύνουν την ομαλή ενσωμάτωση της δραστηριότητας των παικτών στον φυσικό χώρο που ορίζεται ως το Διαδίκτυο των πραγμάτων.

Η πλατφόρμα, η οποία θα υλοποιηθεί πάνω στο εν λόγω framework, περιλαμβάνει τεχνολογίες λογισμικού και υλικού που ενσωματώνονται μαζί για να παρέχουν υπηρεσίες σε όλους τους ενδιαφερόμενους φορείς και αποτελείται από δύο κύρια επίπεδα. Το επίπεδο της Παιχνιδοποίησης (Gamification) που είναι υπεύθυνο για την ενσωμάτωση των καλύτερων τεχνικών και ψυχολογικών πρακτικών και αρχών στο σχεδιασμό Σοβαρού Παιχνιδιού (SG) και το επίπεδο πλατφόρμας του Διαδικτύου Πραγμάτων (IoT) που είναι υπεύθυνο για την αλληλεπίδραση με τον φυσικό κόσμο. Επίσης θα αναπτυχθούν δύο Σοβαρά Παιχνίδια (SGs), εφαρμόζοντας τα παραπάνω στο πλαίσιο της περιβαλλοντικής συνείδησης (για παιδιά και νέους ενήλικες) και των κοινωνικών δεσμών (για αυτιστικά παιδιά).

Σε αυτό το έργο συνεργάζονται επαγγελματίες από όλους τους συναφείς τομείς των επιχειρήσεων, συμπεριλαμβανομένης της βιομηχανίας Σοβαρού Παιχνιδιού (SG), ερευνητικών ιδρυμάτων, επιστημόνων συμπεριφοράς, προγραμματιστών λογισμικού, εμπειρογνωμόνων συστημάτων προσομοίωσης και εμπειρογνωμόνων δικτύων ασύρματων αισθητήρων. Αυτή η κοινοπραξία υπό την ηγεσία του κλάδου πληροί τις ανάγκες ενός σχεδίου σύμπραξης δημόσιου και ιδιωτικού τομέα για την υλοποίηση των αποτελεσμάτων στην πραγματική ζωή.

Τα ζητήματα που προκύπτουν σε αυτή την περίπτωση, σχετικά με την Ασφάλεια και την Ιδιωτικότητα των χρηστών, δεν περιορίζονται μόνο στα θέματα που έχουμε αναφέρει προηγούμενα σε αυτή την εργασία, αλλά επεκτείνονται λόγω της φύσης του έργου. Πιο συγκεκριμένα, οι εφαρμογές που θα υλοποιηθούν απευθύνονται εκτός των άλλων σε παιδιά (και σε μια ομάδα αυτιστικών παιδιών), τα οποία είναι δύσκολο να τηρήσουν κάποιος οδηγίες για την ασφάλεια τους που είναι πιθανό να εφάρμοζε ένας

ενήλικας. Επίσης, η εφαρμογή και δοκιμή της πλατφόρμας θα πραγματοποιηθεί σε διαφορετικά ευρωπαϊκά Κράτη, όπου θα είναι πιο δύσκολη η επίβλεψη του φυσικού κόσμου του Διαδικτύου των πραγμάτων (χρήστες και συσκευές) και με διαφορετικούς κανόνες και νομοθεσία. Ιδιαίτερη προσοχή θα πρέπει να δοθεί και στο γεγονός ότι οι χώροι διεξαγωγής των δοκιμών, θα είναι κοινόχρηστοι και όχι ιδιωτικοί. Τέλος, η ομάδα ανάπτυξης του έργου είναι πολυσύνθετη και αποτελείται από επαγγελματίες διαφόρων ειδικοτήτων και περιοχών, συνεπώς θα πρέπει να υπάρξει σαφής διαχωρισμός των ρόλων, των ιδιοτήτων και των δικαιωμάτων που θα αποδοθούν σε κάθε έναν, στο επίπεδο του έργου, των συστατικών και των δεδομένων τους.

Οι υπεύθυνοι του έργου έχουν ήδη διατυπώσει τις ενέργειες που θα πραγματοποιηθούν και τις οδηγίες που θα τηρηθούν για την επίτευξη της Ασφάλειας και τις Ιδιωτικότητας, οι οποίες είναι πράγματι στα πλαίσια των προτάσεων που διατυπώθηκαν στο Κεφάλαιο 5 και παρουσιάζονται παρακάτω.

1. **Οδηγίες για την χρήση των προσωπικών δεδομένων**

- Δεν απαιτούνται σημαντικά προσωπικά δεδομένα από το έργο και όλα τα δεδομένα μπορούν να συλλέγονται σε ανώνυμη μορφή. Τα πολύ συγκεκριμένα δεδομένα που απαιτούνται για το παιχνίδι και η χρήση τους δικαιολογούνται από την τεκμηρίωση του έργου.
- Τα προσωπικά δεδομένα θα επεξεργάζονται με δίκαιο και νόμιμο τρόπο για τον συγκεκριμένο, ρητό και νόμιμο σκοπό της διεξαγωγής ερευνητικών δραστηριοτήτων στο πλαίσιο του προγράμματος.
- Τα συλλεγόμενα προσωπικά δεδομένα θα είναι επαρκή, συναφή και όχι υπερβολικά σε σχέση με τους σκοπούς του έργου.
- Τα συλλεχθέντα προσωπικά δεδομένα θα είναι ακριβή και ενημερωμένα, ενώ ανακριβή ή ελλιπή δεδομένα θα διαγραφούν ή θα διορθωθούν.
- Όλα τα υποκείμενα των δεδομένων (ή οι νόμιμοι εκπρόσωποί τους) πρέπει να συναινέσουν ρητά στη συλλογή δεδομένων προκειμένου να συμμετάσχουν σε πιλότους του έργου.
- Τα προσωπικά δεδομένα δεν θα φυλάσσονται για περισσότερο από ό, τι είναι απαραίτητο για τους σκοπούς για τους οποίους συλλέχθηκαν τα δεδομένα (συγκεκριμένα, θα καταστραφούν στο τέλος του έργου).
- Τα προσωπικά δεδομένα δεν θα μοιράζονται μεταξύ της εφαρμογής για διαφορετικούς σκοπούς.

- Τα προσωπικά δεδομένα δεν θα μεταφερθούν σε άλλες χώρες χωρίς επαρκή προστασία.
- Όλα τα προσωπικά δεδομένα θα διασφαλίζονται χρησιμοποιώντας τις τεχνικές που περιγράφονται παρακάτω.

2. Προαπαιτούμενα για την ασφαλή επεξεργασία και αποθήκευση των δεδομένων

- Η λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων για την αποτροπή μη εξουσιοδοτημένων ενεργειών σε σχέση με τα δεδομένα.
- Η εξασφάλιση ότι κανείς δεν θα μπορεί να προσπελάσει, να διαβάσει, να αντιγράψει, να τροποποιήσει, να χρησιμοποιήσει με οποιονδήποτε τρόπο ή επεξεργαστεί τα δεδομένα, εκτός αν είναι εξουσιοδοτημένος να το κάνει σύμφωνα με σαφείς κανόνες πρόσβασης (access rights).
- Οργάνωση της επεξεργασίας με τρόπο που προσφέρει πλήρη έλεγχο και παρακολούθηση των ακολουθούμενων διαδικασιών.
- Σε περίπτωση επεξεργασίας δεδομένων από τρίτους, θα πρέπει να επιλέγεται κάποιος που μπορεί να εγγυηθεί την ασφαλή επεξεργασία.
- Πολιτικές εμπιστευτικότητας και προστασίας της ιδιωτικής ζωής.
- Προσδιορισμός της φύσης των δεδομένων που είναι διαθέσιμα στο κοινό.

3. Μέτρα Ασφάλειας

- **Αποθήκευση δεδομένων**. Τα δεδομένα θα αποθηκεύονται σε περιβάλλοντα ασφαλούς σύννεφου (cloud). Θα χρησιμοποιηθούν μόνο πάροχοι υποδομών / υπηρεσιών που συμμορφώνονται με τους κανόνες Προστασίας Δεδομένων της ΕΕ και διαθέτουν πιστοποιημένους ελέγχους ασφαλείας. Επιπλέον, τα κέντρα δεδομένων θα βρίσκονται μόνο στις περιφέρειες της ΕΕ.
- **Ασφάλεια αποθήκευσης**. Τα δεδομένα θα αποθηκεύονται σε ψηφιακές βάσεις δεδομένων, κατά προτίμηση σε ξεχωριστά εικονικά ή φυσικά συστήματα από τις υπόλοιπες υπηρεσίες λογισμικού. Πρέπει να χρησιμοποιούνται μόνο αναγνωρισμένα συστήματα διαχείρισης βάσεων δεδομένων. Τα δεδομένα προτείνεται να κρυπτογραφούνται ή τουλάχιστον τα προσωπικά δεδομένα όπως πληροφορίες ηλικίας, φύλου και τοποθεσίας.
- **Πρόσβαση στα δεδομένα**. Τα δεδομένα δεν πρέπει να είναι προσβάσιμα σε κανένα μη εξουσιοδοτημένο άτομο. Η άμεση πρόσβαση στα δεδομένα που διατηρούνται σε βάσεις δεδομένων πρέπει να αποφεύγεται. Ο έλεγχος πρόσβασης

πρέπει να επιβάλλεται με βάση το ακόλουθο ελάχιστο σύνολο ρόλων και δικαιωμάτων:

(i) Οι παίκτες έχουν πρόσβαση μόνο στα δικά τους δεδομένα.

(ii) Οι εκπαιδευτικοί μπορούν να έχουν πρόσβαση μόνο σε δεδομένα των παικτών με τους οποίους συνδέονται

(iii) Οι προγραμματιστές παιχνιδιών μπορούν να έχουν πρόσβαση μόνο σε συγκεντρωτικά στατιστικά στοιχεία για το δικό τους Σοβαρό Παιχνίδι και όχι μεμονωμένα δεδομένα παικτών.

(iv) Διαχειριστές πλατφόρμας - Μόνο άτομα που έχουν εγκριθεί από την επιτροπή συντονισμού του προγράμματος μπορούν να έχουν πρόσβαση στην πλατφόρμα και στις βάσεις δεδομένων της. Η πρόσβαση αυτή πρέπει επίσης να περιορίζεται στο ελάχιστο δυνατό σύνολο προσώπων και στο ελάχιστο σύνολο αλληλεπιδράσεων που απαιτούνται για την εκτέλεση των διοικητικών καθηκόντων.

Σε όλες τις περιπτώσεις, η πρόσβαση σε δεδομένα πρέπει να είναι δυνατή μόνο μετά από έλεγχο ταυτότητας χρήστη και οι προσπάθειες πρόσβασης πρέπει να καταγράφονται για σκοπούς λογοδοσίας.

- **Έλεγχος ταυτότητας χρήστη και εξουσιοδότηση.** Επιτυγχάνεται μέσω συνδυασμών ονόματος χρήστη / ισχυρών κωδικών πρόσβασης, οι οποίοι αλλάζουν συχνά. Επιτρέπονται λύσεις one-factor single-sign-on
- **Έλεγχος πρόσβασης χρήστη:** Ο έλεγχος πρόσβασης χρήστη (User Access Control - UAC) είναι υπεύθυνος για τον έλεγχο του προφίλ κάθε παίκτη προκειμένου να του δοθεί πρόσβαση στο παιχνίδι και την πλατφόρμα σύμφωνα με τον προκαθορισμένο ρόλο του. Αποτελείται από τέσσερα βασικά υποσυστήματα: τη διαχείριση χρηστών, τη διαχείριση ρόλων, τον έλεγχο συνεδρίας και το υποσύστημα δικαιωμάτων.
- **Διάρκεια αποθήκευσης.** Τα δεδομένα προσωπικού χαρακτήρα δεν φυλάσσονται για περισσότερο από όσο είναι αναγκαίο:

  (i) Τα συλλεγμένα δεδομένα θα διαγραφούν στο τέλος του έργου.

  (ii) Τα συλλεγμένα δεδομένα που σχετίζονται με ένα χρήστη θα διαγραφούν εάν υπάρχει περίοδος αδράνειας του χρήστη μεγαλύτερης των τριών μηνών.

  (iii) Οι χρήστες μπορούν ρητά να ζητήσουν να καταστραφούν τα δεδομένα τους επιλέγοντας την αντίστοιχη επιλογή μέσα από το μενού του Σοβαρού Παιχνιδιού.

- **Ασφάλεια επικοινωνίας.** Οποιαδήποτε ανταλλαγή πληροφοριών μεταξύ της πλατφόρμας, των βάσεων δεδομένων και των πελατών της πρέπει να είναι ασφαλής, μέσω της χρήσης SSL / TLS. Η χρήση τείχους προστασίας και λιστών ελέγχου πρόσβασης επίσης συνίσταται.
- **Ανωνυμοποίηση.** Τα δεδομένα είναι ανώνυμα.
- **Άλλοι έλεγχοι IT.** Τα αντίγραφα ασφαλείας στις βάσεις δεδομένων πρέπει να γίνονται τακτικά, ανάλογα με τη χρήση. Οι εφεδρικές βάσεις δεδομένων πρέπει να προστατεύονται με κωδικό πρόσβασης και να αποθηκεύονται σε τοποθεσίες που προστατεύονται από περιοριστικές λίστες ελέγχου πρόσβασης. Η χρήση της κρυπτογράφησης συνιστάται. Οι διακομιστές που χρησιμοποιούνται από την πλατφόρμα (συμπεριλαμβανομένων των διακομιστών cloud) πρέπει να έχουν ασφαλείς διαμορφώσεις, σύμφωνα με τις συνήθεις βέλτιστες πρακτικές όσον αφορά την εγκατάσταση ενημερώσεων ασφαλείας, προστασία από ιούς / προστασία από κακόβουλο λογισμικό, τοπικά αντίγραφα ασφαλείας, αποκλεισμό ορισμένων υπηρεσιών ή εγκαταστάσεων λογισμικού, Κωδικοί πρόσβασης διαχειριστή κλπ.
- **Διαχείριση παραβίασης.** Σε περίπτωση παραβίασης των δεδομένων, η ομάδα του έργου πρέπει να συγκεντρώσει λεπτομέρειες σχετικά με το περιστατικό ασφαλείας και να ενημερώσει την Επιτροπή Συντονισμού του Έργου, η οποία πρέπει να συγκαλέσει το συντομότερο δυνατόν και να συμβουλευτεί
  (i) τον Υπεύθυνο Προστασίας Δεδομένων της
  (ii) τον σύμβουλο δεοντολογίας
  (iii) τις νομικές υπηρεσίες των οργανώσεων-εταίρων
  (iv) την Ευρωπαϊκή Επιτροπή
  για να αποφασίσει σχετικά με τα μέτρα και τις επόμενες ενέργειες που πρέπει να εφαρμόσουν για τον περιορισμό τυχόν ζημιών και την ενημέρωση των υποκειμένων των δεδομένων.

Πρέπει να επισημανθεί ότι η υλοποίηση ενός ολικού πλάνου διαχείρισης και αντιμετώπισης κινδύνων είναι μια σημαντική διαδικασία για κάθε έργο. Σκοπός του πλάνου είναι η αποφυγή προβλέψιμων κινδύνων, η προστασία από λάθος αποφάσεις και η ελαχιστοποίηση των απωλειών και ζημιών από απρόβλεπτα γεγονότα. Συνεπώς και για το ευρωπαϊκό έργο σε εξέλιξη, είναι απαραίτητο να σχεδιαστεί ένα αντίστοιχο πλάνο.

Πιο συγκεκριμένα το πλάνο διαχείρισης και αντιμετώπισης κινδύνων προϋποθέτει όλα τα παρακάτω:

1. Την αναγνώριση των απειλών κατά του συστήματος που θα υλοποιηθεί

2. Την αναγνώριση των επιμέρους ευπαθειών
3. Την αναγνώριση των πιθανών κατηγοριών απωλειών.
4. Την εκτίμηση της πιθανότητας να συμβεί μια απώλεια
5. Τον προσδιορισμό των απαραίτητων προφυλάξεων / αντίμετρων για την αντιμετώπιση των κινδύνων
6. Την διαμόρφωση και υλοποίηση του πλέον αποτελεσματικού και ενδεδειγμένου από άποψη κόστους συστήματος ασφαλείας.

Πρέπει να γίνει ανάλυση όλων των κινδύνων και να αναγνωριστούν όλες οι απειλές και οι ευπάθειες, τόσο σε φυσικό όσο και σε λογικό επίπεδο, καθώς και οι πιθανότητες εμφάνισης τους. Ακόμα πρέπει να γίνει καταγραφή όλων των πιθανών απωλειών που αυτά μπορεί να επιφέρουν, και να προσδιοριστούν και οι απαραίτητες προφυλάξεις που πρέπει να ληφθούν. Το επόμενο βήμα είναι η διαμόρφωση ενός αποδοτικού συστήματος ασφαλείας που θα εξασφαλίζει και θα εγγυάται την ακεραιότητα, την εμπιστευτικότητα αλλά και την διαθεσιμότητα των δεδομένων, με το ελάχιστο δυνατό κόστος στο έργο.

Το πλάνο διαχείρισης ενός τέτοιου συστήματος εφαρμόζεται σε τέσσερις φάσεις:

- *Σχεδιασμός (Plan):* Σε αυτήν την φάση σχεδιάζεται το όλο σύστημα, καταγράφονται όλα τα αγαθά και περιουσιακά στοιχειά, αναλύεται η επικινδυνότητα αυτών και επιλέγονται οι απαραίτητοι έλεγχοι.
- *Εκτέλεση (Do):* Εδώ συντελείται η εφαρμογή του συστήματος και των ελέγχων λειτουργίας
- *Έλεγχος (Check):* Φάση στην οποία έχουμε την αντικειμενική αξιολόγηση του πλάνου που έχει εκτελεστεί αλλά και η αξιολόγηση των επιδόσεων αυτού (αποδοτικότητα και αποτελεσματικότητα)
- *Ενεργοποίηση (Act):* Σε αυτήν την φάση γίνονται αλλαγές όπου χρειάζονται, ώστε να βελτιστοποιηθεί το σύστημα.

Τα οφέλη που το έργο θα αποκομίσει με την εφαρμογή των παραπάνω, είναι ότι εκτός του ότι θα κερδίζει την εμπιστοσύνη του χρήστη, θα μειώσει τα συμβάντα σχετικά με την ασφάλεια και επομένως θα αυξήσει την αξιοπιστία του, εξασφαλίζοντας τα υλικά στοιχεία και τα δεδομένα του από υποβάθμιση, απώλεια, ζημιά ή και κλοπή. Θα συμμορφώνεται επίσης με την σχετική νομοθεσία και τέλος θα έχει εξασφαλίσει την άμεση επαναφορά και λειτουργία των συστημάτων του σε περίπτωση καταστροφής μεγάλης κλίμακας.

ΑΝΑΦΟΡΕΣ

[1] COETZEE, Louis και EKSTEEN, Johan: “The Internet of Things – Promise for the Future? An Introduction.” s.l. IIMC International Information Management Corporation, 2011.

[2] Vermesan, Ovidiu και Friess, Peter: “Internet of Things – From Research and Innovation to Market Deployment.” s.l. : River Publishers, 2014. 978-8793102941.

[3] L. T. Y. L. W. a. A. V. Feng Xia, «Internet of Things».

[4] R. B. S. M. M. P. Jayavardhana Gubbia:“Internet of Things (IoT): A vision, architectural elements, and future directions” Future Generation Computer Systems, 2013.

[5] Weimin Wang: “The research and development of the Internet of Things technology. Information network security”, 2011, 03, pp.53-56.

[6] Geng Yang. “The characteristic and key technology of the Internet of Things.” The academic journal of Nanjing University. 2010, 30(4), pp.20-29.

[7] Mi Weng. “The Internet of Things key management based on wireless sensor network.” The academic journal of Shanghai University. 2011, 27(1), pp.66-69.

[8] “SRI Consulting Business Intelligence/National Intelligence Council”. Appendix F of Disruptive Technologies Global Trends 2025, 2008.

[9] Zhang, Baoquan. “Evaluation on Security System of Internet of Things Based on Fuzzy-AHP Method.” E -Business and E -Government (ICEE), 2011 International Conference. 2011

[10] Dong Chen. “A Novel Secure Architecture for the Internet of Things.” 2011 Fifth International Conference on Genetic and Evolutionary Computing, 2011.

[11] China Telecom. China Telecom Ineternet of Things Report. 2009

[12] Juels A, Rivest R L, Szydlo M. “The blocker tag: Selective blocking of RFID tags for consumer Privacy.” In Proceedings of 10th ACM Conference on Computer and Communication Security (CCS2003), Washington, DC, USA, 2003, 103-111.

[13] Sarma S E, Weis S A, Engels D W. “Radio frequency identification: Secure risks and challenges.” RSA Laboratories Cryptobytes, 2003, 6(1): 2-9.

[14] Weis S A, Sarma S E, Rivest R L, et al. “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems.” First International Conference on Security in Pervasive Computing, 2003.

[15] Lee S M, Hwang Y J, Lee D H. “Efficient authentication for low-cost RFID system[C].” International Conference on Computational Science and Its Applications (ICCSA2005). Berlin, 2005: 619-627.

[16] Rhee K, Kwak J, Kim S, Won D. “Challenge-Response Based RFID Authentication Protocol for Distributed Database Environment.” In Proceeding of the 2nd International Conference on Security in Pervasive Computing (SPC 2005), 2005, 70-84.

[17] Vanstone, S. “Responses to NIST's proposal”. Communications of the ACM 35 (1992), 50-52.

[18] Ning Kong. “The Internet of things addressing key technology research.” Master Thesis. Chinese Academy of Sciences, 2008

[19] Παναγοπούλου Γ. “Διαδίκτυο των πραγμάτων (Internet Of Things) Ζητήματα προσωπικών δεδομένων”, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

[20] Μάγκος Εμμανουήλ: “Ασφάλεια Π.Σ. Ενότητα Α: Εισαγωγικές Έννοιες” , Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

[21] Μάγκος Εμμανουήλ: “Ασφάλεια Υπολογιστών και Προστασία Δεδομένων Σημειώσεις Μαθήματος Δ’ Εξαμήνου” ,Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

[22] Xabier Larrucea ; Annie Combelles ; John Favaro ; Kunal Taneja: “Software Engineering for the Internet of Things”, IEEE Software, Volume: 34, Issue: 1, Jan.-Feb. 2017

[23] A. Tajer, S. Kar, H.V. Poor, and S. Cui, “Distributed Joint Cyber Attack Detection and State Recovery in Smart Grids”, IEEE Int. Conf. on Smart Grid Communications, Brussels, Belgium, Oct. 2011, pp.202-207.

[24] H.D. Nguyen, S. Gutta, and Q. Cheng, “An Active Distributed Approach for Cyber Attack Detection,” IEEE Conf. on Signals, Systems and Computers, Pacific Grove, CA, Nov. 2010, pp. 1540-1544

[25] D. Slamanig, and C. Stingle, “Privacy Aspects of eHealth”, IEEE 3rd Int. Conf. on Availability, Reliability and Security, Barcelona, Mar. 2008, pp. 1226-1233

[26] R. Hall, A. Rinaldo, and L. Wasserman, “Differential Privacy for Functions and Functional Data”, J. of Machine Learning Research, 2013, pp.703-727.

[27] J. Ren, Y. Li, and T. Li , “Routing-Based Source-Location Privacy in Wireless Sensor Networks”, IEEE Int. Conf. on Communications, June 2009, pp.1-5.

[28] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, “Protecting Recevier-Location Privacy in Wireless Sensor Networks”, IEEE 26th Int. Conf. on Computer Communications, Anchorage, AK, May 2007, pp.1955-1963.

[29] K. Mehta, D. Liu, and M. Wright, “Location Privacy in Sensor Networks Against a Global Eavesdropper”, IEEE Int. Conf. on Network Protocols, Beijing, Oct. 2007, pp. 314-323.

[30] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle, “Privacy in the Internet of Things:Threats and Challenges”, 10 June 2013

[31] European Commission, “FUTURE NETWORKS, The way ahead!”, Information Society and Media

[32] L. Atzori, A. Iera, G. Morabito, “The Internet of Things: A survey”, Computer Networks, 31 May 2010

[33] A. Juels, “RFID Security and Privacy: A Research Survey”, IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, FEBRUARY 2006

[34] https://www.postscapes.com/internet-of-things-technologies/

[35] https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

[36] https://www.tutorialspoint.com/internet_of_things/internet_of_things_hardware.htm

[37] http://www.eugdpr.org/key-changes.html

[38] http://www.adae.gr

[39] http://www.gartner.com/newsroom/id/3412017