ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

"Ubiquitous Computing και δυνατότητες αξιοποίησης στα έξυπνα σπίτια."

ΟΝΟΜΑΤΕΠΩΝΥΜΟ:ΘΕΟΦΡΑΣΤΟΣ ΧΑΧΑΛΑΣ

ΕΠΙΒΛΕΠΩΝ: ΤΣΑΚΑΝΙΚΑΣ ΒΑΣΙΛΕΙΟΣ

ΑΝΤΙΡΡΙΟ 2016

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

Αντίριο, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ονοματεπώνυμο, Υπογραφή

2. Ονοματεπώνυμο, Υπογραφή

3. Ονοματεπώνυμο, Υπογραφή

ΕΥΧΑΡΙΣΤΙΕΣ

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω την οικογένειά μου για τα εχέγγυα που μου προσέφερε στην ολοκλήρωση των σπουδών μου.

ΠΡΟΛΟΓΟΣ

Η συγκεκριμένη πτυχιακή εργασία εκπονήθηκε κατά κύριο λόγο για να διερευνηθεί τι είναι το λεγόμενο Ubiquitous Computing και ποιες είναι οι βασικές έννοιες που το χαρακτηρίζουν. Θα αναλύσουμε την ιστορία γύρω από την έννοια του Ubiquitous Computing, πως και από ποιόν προτάθηκε σαν ορισμός και τις εξελίξεις που συμβαίνουν στην σημερινή εποχή. Επιπλέον θα συζητήσουμε την διαδραστικότητα με ασύρματα δίκτυα και λοιπές έννοιες. Ακόμη θα αναλύσουμε το υλικό (hardware) που είναι υπεύθυνο και απαραίτητο για την υλοποίηση του Ubiquitous Computing όπως σένσορες (sensors) και υπόλοιπους αισθητήρες και μικρο-ελεγκτές. Θα αναλυθούν προβλήματα ασφαλείας, τρόποι αντιμετώπισης και αποτροπής. Τέλος κάνοντας χρήση λογισμικού τρισδιάστατης σχεδίασης θα δημιουργηθεί μοντέλο έξυπνου σπιτιού.

ΠΕΡΙΛΗΨΗ

Οι κύριοι στόχοι της παρούσας πτυχιακής εργασίας είναι να αναλύσουμε τις δυνατότητες αξιοποίησης του Ubiquitous Computing αλλά και τους κινδύνους και περιορισμούς που υπάρχουν από τη χρήση τους. Επιπλέον θα αναζητήσουμε με ποιον τρόπο και σε ποιον βαθμό έχει συμβεί η εξέλιξη του Ubiquitous Computing και επιπλέον ποιες είναι οι περαιτέρω δυνατότητες αλλά και κίνδυνοι σε ένα τέτοιο εγχείρημα.

Η εργασία μας απαρτίζεται από μια σειρά κεφαλαίων που καλύπτουν ένα συνολικό φάσμα της εν λόγω τεχνολογίας. Αρχικά δίνεται μια εισαγωγική περίληψη της τεχνολογίας και της θέσης που θα κατέχει στο μέλλον της κοινωνίας μας.

Στο δεύτερο κεφάλαιο, αυτής της πτυχιακής εργασίας, γίνεται αναφορά στο Ubiquitous Computing και στον τρόπο που λειτουργεί. Αναλύουμε τι είναι Ubiquitous Computing τον ορισμό του, τις δυνατότητες και λειτουργίες χρήσεως και την διάδοση στην σημερινή κοινωνία. Συζητάμε την ιστορία του και πως προέκυψε σαν έννοια, την συνάφεια του με τα ασύρματα δίκτυα και τις βασικές έννοιες.

Στο τρίτο κεφάλαιο αναλύεται το υλικό που απαιτείται για την υλοποίηση του Ubiquitous Computing. Συζητάμε την αρχιτεκτονική που χρησιμοποιείται καθώς και διαφόρους τύπους αισθητήρων. Επιπλέον αναφερόμαστε σε είδη μικρο– ελεγκτών, τις δυνατότητές τους και την χρήση τους σε συστήματα Ubiquitous Computing.

Στο τέταρτο κεφάλαιο δίνουμε ιδιαίτερη έμφαση στην ασφάλεια της τεχνολογίας καθώς και στην ιδιωτικότητα και στην προστασία των προσωπικών δεδομένων. Προτείνουμε λύσεις στα πολλαπλά προβλήματα ασφαλείας που προκύπτουν για το Ubiquitous Computing. Επιπλέον δίνονται μια σειρά από ενέργειες που θα μπορούσε να κάνει ο ίδιος ο χρήστης.

Τέλος, διαμορφώνουμε και σχεδιάζουμε με το εργαλείο Google Sketch-Up μια σειρά από σενάρια όπου η τεχνολογία μπορεί να χρησιμοποιηθεί στα έξυπνα σπίτια του μέλλοντος, όπως για παράδειγμα η αποτροπή κάποιου εισβολέα στο χώρο που φυλάσσεται από συστήματα παρακολούθησης.

ABSTRACT

The main objectives of this thesis are to analyze the possibilities of utilization of Ubiquitous Computing and the risks and limitations of using them. We will also seek how and to what extent the development of Ubiquitous Computing and moreover what has happened further opportunities and risks in such a venture. Our work consists of a series of chapters that cover a whole spectrum of this technology.

Initially an introductory summary is given to the technology and the meaning that it will play in the future of our modern society. The second chapter of this thesis refers to the Ubiquitous Computing and how it works.

We analyze what is Ubiquitous Computing definition of the possibilities and use functions and the dissemination in today's society. We discuss the story and how it arose as a concept, the link with the wireless networks and basic concepts.

The third chapter analyzes the material required for the realization of Ubiquitous Computing. We discuss the architecture used and various types of sensors. Furthermore we refer to species of micro-controllers, their features and their use in Ubiquitous Computing systems.

In the fourth chapter we emphasize the safety technology and the privacy and protection of personal data. We recommend solutions to its many security problems arising for Ubiquitous Computing. Furthermore they are given a series of actions that the user could do to protect the smart home himself.

Finally, using the Google Sketch-Up tool a number of scenarios in which technology can be used in smart homes of the future, for example to prevent an intruder in the smart home that is guarded by surveillance systems.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1:ΕΙΣΑΓΩΓΗ

Η παγκόσμια κοινωνία των πληροφοριών αποτελεί σήμερα μια απτή πραγματικότητα, η οποία μας ανήκει και στην οποία ανήκουμε κατά τρόπο αδιαμφισβήτητο, μας περιβάλλει από παντού, γεμίζοντάς μας με υποσχέσεις και δυνατότητες που δεν είχαμε σκεφτεί στο παρελθόν αλλά και τρομάζοντάς μας με τις εκπλήξεις της. Το Δίκτυο ανοίγει μια ουσιαστική συζήτηση με ολόκληρη την κοινωνία. Οι συνέπειες της επιταχυνόμενης εφαρμογής των ηλεκτρονικών υπολογιστών γίνονται αισθητές σε όλα της τα πεδία: στις οικογενειακές σχέσεις, στην ψυχολογική συμπεριφορά των ανθρώπων, στην πολιτική οργάνωση, στον κόσμο των επιχειρήσεων και του εμπορίου, στην εκπαίδευση, στον τρόπο που δουλεύουμε και διασκεδάζουμε. Πως μπορούμε να χρησιμοποιήσουμε αυτή την τεχνολογική εξέλιξη και να κάνουμε το επόμενο τεχνολογικό βήμα;

Σίγουρα το μέλλον προμηνύεται ευοίωνο για τις τεχνολογίες του διαδικτύου και των υπολογιστικών συστημάτων καθώς όλο και περισσότεροι χρήστες θα τις ενσωματώσουν στην ζωή τους. Σκοπός μας είναι να χρησιμοποιηθούν με τον βέλτιστο δυνατό τρόπο για να αποτελέσουν ένα σημαντικό μέσο για την επικοινωνία και την απλούστευση των αναγκών μας.

Στην πτυχιακή μας θα αναλύσουμε και θα εξετάσουμε το Ubiquitous Computing από την αρχή της γέννησής του, τις οποιεσδήποτε δυνατότητες αξιοποίησης του για και τις μέχρι τώρα εξελίξεις και αλλαγές. Στην σημερινή εποχή του διαδικτύου οι ευκαιρίες για μεγαλύτερη πρόσβαση και ευκολότερες υπηρεσίες για τους πολίτες είναι περισσότερες κάτι που μπορεί να γίνει πραγματικότητα με το Ubiquitous Computing. Επιπλέον θα αναλύσουμε εάν μια τέτοια μορφή επικοινωνίας και αλληλεπίδρασης θα γίνει αποδεκτή και πως θα προσφέρει οφέλη σε όλο το κοινωνικό σύνολο.

Η διάρθρωση της πτυχιακής θα γίνει αρχικά με το θεωρητικό κομμάτι όπου θα μελετήσουμε το Ubiquitous Computing από την γέννηση του, την ιστορία του, τον τρόπο που χρησιμοποιείται και τις εφαρμογές και στην υλοποίηση που έχει συμβεί

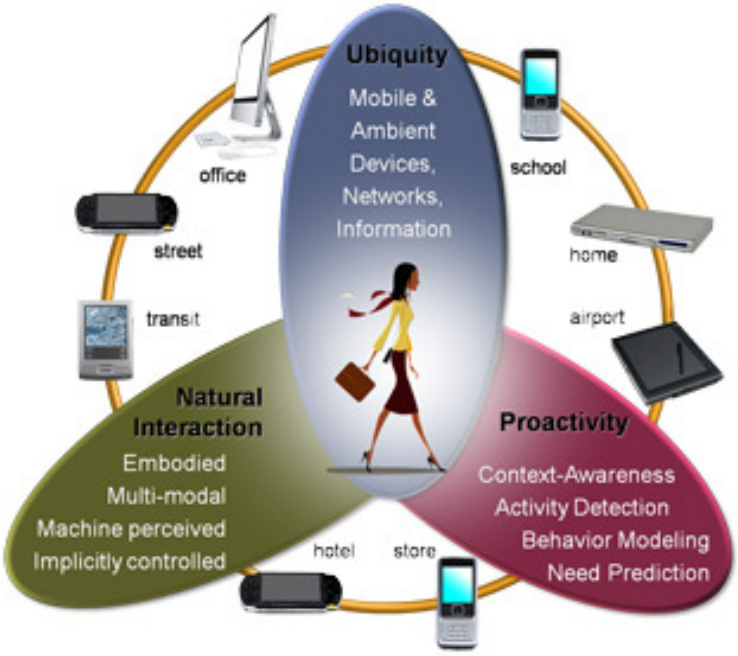
μέχρι στιγμής. Επιπλέον θα αναφερθούν ανάλογες έρευνες και μελέτες που έχουν γίνει πάνω στο αντικείμενο από την διεθνή και ελληνική βιβλιογραφία.

,

ΚΕΦΑΛΑΙΟ 2: Ubiquitous Computing (Διάχυτη Υπολογιστική)

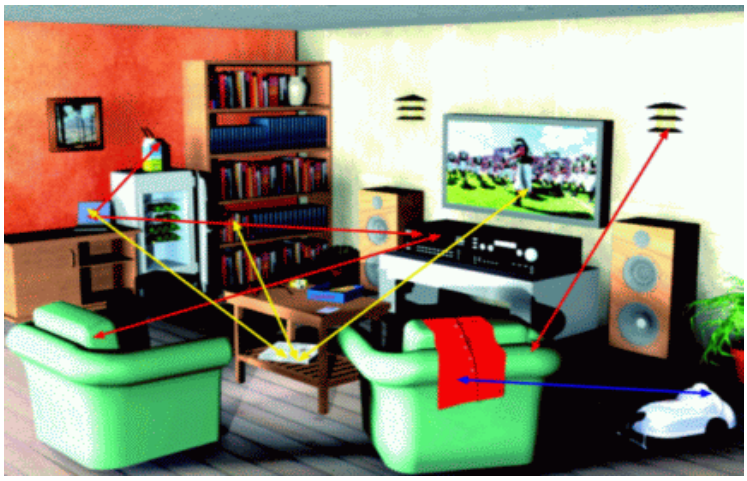
Ο όρος της διάχυτης υπολογιστικής (Ubiquitous Computing) είναι μια έννοια στην τεχνολογία λογισμικού και την επιστήμη των υπολογιστών, όπου υπολογιστικά συστήματα, εφαρμογές και υλοποιήσεις μπορούν να συμβούν οπουδήποτε. Σε αντίθεση με τους σταθερούς οικιακούς υπολογιστές (Desktops) , η διάχυτη υπολογιστική μπορεί να συμβεί χρησιμοποιώντας οποιαδήποτε συσκευή, σε οποιαδήποτε θέση, και σε κάθε μορφή. Ένας χρήστης αλληλεπιδρά με τον υπολογιστή, τον οποίο μπορεί να υπάρξει σε πολλές διαφορετικές μορφές, συμπεριλαμβανομένων των φορητών υπολογιστών, τα δισκία και τα τερματικά σε αντικείμενα καθημερινής χρήσης, όπως ένα ψυγείο ή ένα ζευγάρι γυαλιά. Οι βασικές τεχνολογίες που υποστηρίζουν την διάχυτη υπολογιστική συμπεριλαμβάνονται σε πληθώρα στοιχείων όπως το Internet, το προηγμένο υλικό, το λειτουργικό σύστημα, κάθε είδους αισθητήρες, μικροεπεξεργαστές, τα δίκτυα, και τα κινητά.

Η διάχυτη υπολογιστική είναι το αντίθετο της εικονικής πραγματικότητας. Ενώ στην εικονική πραγματικότητα τοποθετείτε ο άνθρωπος μέσα σε περιβάλλοντα δημιουργημένα από τον υπολογιστή στη διάχυτη υπολογιστική υλοποιούμε τους υπολογιστές ώστε να συνυπάρχουν με τους ανθρώπους. Συμπερασματικά η διάχυτη υπολογιστική αποτελεί μια αλληλεπίδραση μεταξύ ανθρώπου και υπολογιστή. Μέσω αυτής της αλληλεπίδρασης ο άνθρωπος θα μπορεί κατά την διάρκεια των δραστηριοτήτων του, να δεσμεύσει πολλαπλά υπολογιστικά συστήματα ακόμη και χωρίς να το γνωρίζει. Ο χρήστης δηλαδή δεν θα λειτουργεί μόνο με μια κεντρική υπολογιστική μονάδα αλλά με ένα μεγάλο σύνολο που έχουν δημιουργηθεί μέσα στο ανθρώπινο περιβάλλον. Δηλαδή το Ubiquitous Computing αποτελεί την συνέχεια και εξέλιξη της αλληλεπίδρασης των υπολογιστών με σκοπό μέσω έξυπνων συστημάτων περιβάλλοντος να βοηθούν τους ανθρώπους σε όλες τις φάσεις και προβλήματα της ζωής τους.



Εικόνα 1 – Ubiquitous Computing στην καθημερινή μας ζωή

Υπό αυτή την έννοια, της διάχυτης υπολογιστικής, τα τωρινά συστήματα και εφαρμογές θα πρέπει να προσαρμοστούν και να εξελιχθούν στην προσπάθεια να είναι άρρηκτα ενσωματωμένα στις ανάγκες και απαιτήσεις των χρηστών. Σε μία τεχνολογική κοινωνία που βασίζεται στην διάχυτη υπολογιστική οι υπηρεσίες θα πρέπει να προβλέπουν τις ανάγκες των χρηστών και να τις επιλύνουν με τέτοιο τρόπο ώστε να μην χρειάζεται η παρουσία και λειτουργία κάποιου χρήστη και αν είναι δυνατόν να μην γίνονται αντιληπτές.



Εικόνα 2 – Ubiquitous Computing και καθημερινότητα

2.1 Ιστορία του Ubiquitous Computing

Πατέρας και πρώτος εισηγητής της έννοιας του Ubiquitous Computing ήταν ο Mark Weiser το 1988. Αυτός και οι συνάδελφοι του στο εργαστήριο πληροφορικής του κέντρου Xerox Palo Alto Center (PARC) έγραψαν κάποια από τα πρώτα άρθρα σχετικά με το ζήτημα. Αναγνώρισαν το Ubiquitous Computing σαν μια αόρατη παρουσία που θα μπορούσε να απλοποιήσει και να λύσει καθημερινά προβλήματα των ανθρώπων με την βοήθεια υπολογιστικών συστημάτων και εφαρμογών.

Ο Weiser ανέπτυξε περαιτέρω τις ιδέες του στο άρθρο “The computer for the Twenty-First Century” το 1991.Το όραμα του Weiser ήταν :

- Υπολογιστικά συστήματα παντού, που να είναι αόρατα και να αλληλεπιδρούν με το περιβάλλον και με τους ανθρώπους.
- Οι υπολογιστές να μην βρίσκονται απομονωμένοι αλλά και ταυτόχρονα να μην χρειάζεται η διαρκής επιτήρηση από χρήστες.
- Η επίδραση του Ubiquitous Computing να είναι τέτοια ώστε να εμφανίζεται και να περιβάλλει κάθε δραστηριότητα μας.
- Το Ubiquitous Computing να είναι παρόμοιο με τον ηλεκτρισμό. Ενώ μπορούμε να το χρησιμοποιήσουμε σε κάθε μας εργασία αυτό παραμένει αόρατο πίσω από τοίχους.

Σε μία από τις διαλέξεις του ο Weiser ανέφερε το Ubiquitous Computing σαν σιωπηλός και ήσυχος υπηρέτης. Δηλαδή μία μορφή εφαρμογής και υλοποίησης που θα μας βοηθάει χωρίς την συνεχή επιτήρησή μας.

Το κέντρο ερευνών PARC συνέχισε την έρευνα του στον τομέα του Ubiquitous Computing από το 1991 μέχρι το 2000 με 41 άτομα στην ομάδα τους. Δημιούργησε συσκευές όπως notepads, ηλεκτρικούς πίνακες και έγγραφα που αποθήκευαν αυτόματα τι γραφόταν πάνω σε αυτά. Άρα η διαφορά ήταν ότι τώρα ο χρήστης έμενε απερίσπαστος στην διαδικασία και δεν ανησυχούσε για το πώς να λειτουργήσει τον υπολογιστή.

Επιπλέον ένας ακόμη από τους πρωτοπόρους του Ubiquitous Computing ήταν το Active Badge το 1988, ένα έξυπνο δίκτυο τηλεφωνικό δικτύων που προσπαθούσε να επιλύσει το πρόβλημα της αυτόματης ανάθεσης κλήσεων στο σωστό μέρος και διεύθυνση.

2.2 Ubiquitous Computing και ασύρματες ζεύξεις

Ως ασύρματο δίκτυο ονομάζεται το είδος του δικτυού που για να μεταφέρει την πληροφορία χρησιμοποιεί ραδιοκύματα. Τα δεδομένα αυτά μεταφέρονται μέσω του υλικού (αέρας) με την βοήθεια ηλεκτρομαγνητικών κυμάτων και σε αντίθεση με τηα ενσύρματα δίκτυα δεν χρησιμοποιούν κάποιο είδος καλωδίου. Στα ασύρματα δίκτυα εντάσσονται τα δίκτυα κινητής τηλεφωνίας, οι δορυφορικές επικοινωνίες, τα ασύρματα δίκτυα, τα ασύρματα τοπικά δίκτυ WLAN και κάθε είδους δίκτυο που δεν περιέχει καλώδια.

Δεδομένης της τρέχουσας τεχνολογικής κοινωνίας και εξέλιξης που διανύουμε μπορούμε να πούμε ότι το Ubiquitous Computing είναι πιο κοντά από κάθε άλλη φορά. Παρόλο που ο Weiser είδε το Ubiquitous Computing από μια πιο ακαδημαϊκή σκοπιά η σημερινή τεχνολογική κατάσταση μας επιτρέπει να συζητάμε για κάτι που παλιότερα ήταν όνειρο. Στην πραγματικότητα μια πληθώρα από συσκευές που χρησιμοποιούν ασύρματες επικοινωνίες και πρωτόκολλα έχουν κατακλείσει την ζωή μας. Από κινητά, pda’s ,έξυπνα ρολόγια και τηλεοράσεις μέχρι κάθε είδους μικρό-αισθητήρα.

Πλέον οι μικροεπεξεργαστές έχουν γίνει τόσο μικροί και φθηνοί που μπορούν να ενσωματωθούν σε οποιοδήποτε προϊόν. Όχι μόνο ηλεκτρικές συσκευές και αυτοκίνητα άλλα σε παιχνίδια, εργαλεία ακόμη και σε ρούχα. Στην πραγματικότητα η τεχνολογία αυτή θα προβεί σε περαιτέρω εξελίξεις και βελτιώσεις που σημαίνει ότι δισεκατομμύρια μικροσκοπικοί επεξεργαστές θα έχουν ενσωματωθεί στον φυσικό μας κόσμο. Και αυτές οι συσκευές θα είναι συνδεδεμένες μεταξύ τους με ασύρματα δίκτυα. Η ραγδαία ανάπτυξη στα ασύρματα δίκτυα μπορεί να φανεί από την

ανάπτυξη που είχαν τα κινητά τηλέφωνα μέσα σε σύντομο χρονικό διάστημα. Από την εποχή που το κινητό τηλέφωνο αποτελούσε ένα αντικείμενο κύρους πλέον είναι απαραίτητο στην ζωή μας.

Εικόνα 3 – Ubiquitous Computing και ασύρματα δίκτυα

Τα κινητά τηλέφωνα και ένα πλήθος συσκευών που μας επιτρέπουν την ασύρματη διεπαφή με διάφορες τεχνικές όπως wireless networks WLAN, Bluetooth, ZigBee. Φυσικά δεν πρέπει να ξεχνάμε και την χρήση δορυφορικών συστημάτων GPS όπου ο προσδιορισμός θέσης μπορεί να γίνει με μεγάλη ακρίβεια.

Τα πλεονεκτήματα των ασύρματων δικτύων είναι :

- Ευκολία. Πρόσβαση σε πόρους του δικτύου σας από οποιαδήποτε θέση εντός της περιοχής κάλυψης του ασύρματου δικτύου ή από οποιοδήποτε hotspot WiFi.
- Κινητικότητα. Διασύνδεση στο διαδίκτυο από όπου και αν βρισκόμαστε.
- Παραγωγικότητα. Η ασύρματη πρόσβαση στο Internet και σε βασικές εφαρμογές αυξάνει την παραγωγικότητα.
- Εύκολη εγκατάσταση. Δεν χρειάζεται η εγκατάσταση καλωδίων, έτσι η εγκατάσταση μπορεί να είναι γρήγορη και αποδοτική.
- Επεκτάσιμη. Μπορείτε εύκολα να επεκτείνετε ασύρματα δίκτυα με τον υπάρχοντα εξοπλισμό, ενώ ένα ενσύρματο δίκτυο ενδέχεται να απαιτεί επιπλέον καλωδίωση.
- Ασφάλεια. Προϋποθέσεις και πρωτόκολλα σε ασύρματα δίκτυα παρέχουν ισχυρή προστασία της ασφάλειας.
- Κόστος. Επειδή τα ασύρματα δίκτυα δεν απαιτούν καλωδίωση το κόστος τους είναι μικρότερο.

2.3 Bluetooth

Στη μικρότερη τάξη μεγέθους ασύρματων δικτύων συναντώνται τα WPAN, τοπικά δίκτυα πολύ μικρής εμβέλειας με σκοπό την ασύρματη και ad hoc δικτύωση ετερογενών φορητών συσκευών. Το σπουδαιότερο πρότυπο στον χώρο αυτόν είναι η οικογένεια πρωτοκόλλων Bluetooth που σχεδιάστηκε από μία ομάδα εταιρειών και υιοθετήθηκε στη συνέχεια από την IEEE ως το πρότυπο 802.15 για WPAN. Οι βασικότερες προδιαγραφές αφορούν το φυσικό επίπεδο και το υποεπίπεδο MAC, όπου έχουν δημιουργηθεί διαφορετικά πρωτόκολλα για διαφορετικές εφαρμογές και τα οποία ονομάζονται προφίλ (π.χ. προφίλ ασύρματου τηλεφώνου, προφίλ πρόσβασης σε LAN κλπ). Κάθε προφίλ περιλαμβάνει πρότυπα για όλα τα επίπεδα και προσφέρει λύσεις για τη διασύνδεση με διαφορετικά δίκτυα μεγαλύτερης κλίμακας.

Από φυσικής άποψης το Bluetooth λειτουργεί περίπου στα 2,4 GHz, κάνει χρήση της μεθόδου διασποράς φάσματος FHSS με την τακτική εναλλαγή της συχνότητας να καθορίζεται τυχαία από έναν κεντρικό κόμβο, τον κόμβο Master, και προδιαγράφει τρία επίπεδα ισχύος της εκπομπής από τα οποία εξαρτάται και η εμβέλεια επικοινωνίας (πάντα μικρότερη των 10 μέτρων σε PAN). Ένα πρόβλημα των προδιαγραφών του Bluetooth είναι ότι, λόγω της μετάδοσης στην ελεύθερη ζώνη συχνοτήτων των 2,4 GHz, οι συσκευές που το υποστηρίζουν αδυνατούν να χρησιμοποιήσουν ταυτόχρονα τα περισσότερα πρωτόκολλα της οικογένειας IEEE 802.11, καθώς τότε θα εμφανιζόταν σοβαρά προβλήματα παρεμβολών.

Η οικογένεια πρωτοκόλλων IEEE 802.11 αποτελεί το καθιερωμένο πρότυπο της βιομηχανίας στο χώρο των ασύρματων τοπικών δικτύων. Όλα τα πρωτόκολλα 802.11x έχουν κοινό υποεπίπεδο MAC και διαφέρουν στο φυσικό μέσο. Το υποεπίπεδο LLC, που αναλαμβάνει τον έλεγχο ροής, τον έλεγχο σφαλμάτων και τη διασύνδεση προς το επίπεδο δικτύου, ταυτίζεται με το καθιερωμένο κοινό πρωτόκολλο 802.2 που χρησιμοποιείται και στο Ethernet και στα περισσότερα ενσύρματα τοπικά δίκτυα με αποτέλεσμα την άμεση και χωρίς ανάγκη μετατροπής συνδεσιμότητας ενός 802.11 WLAN με το Internet ή άλλα WAN/διαδίκτυα που χρησιμοποιούν το IP ως πρωτόκολλο δικτύου. Το βασικό πρωτόκολλο MAC του 802.11 είναι το DCF, το οποίο βασίζεται στη μέθοδο CSMA/CA, ενώ στα δομημένα WLAN πάνω από το DCF τρέχει επιπλέον το πρωτόκολλο PCF το οποίο,

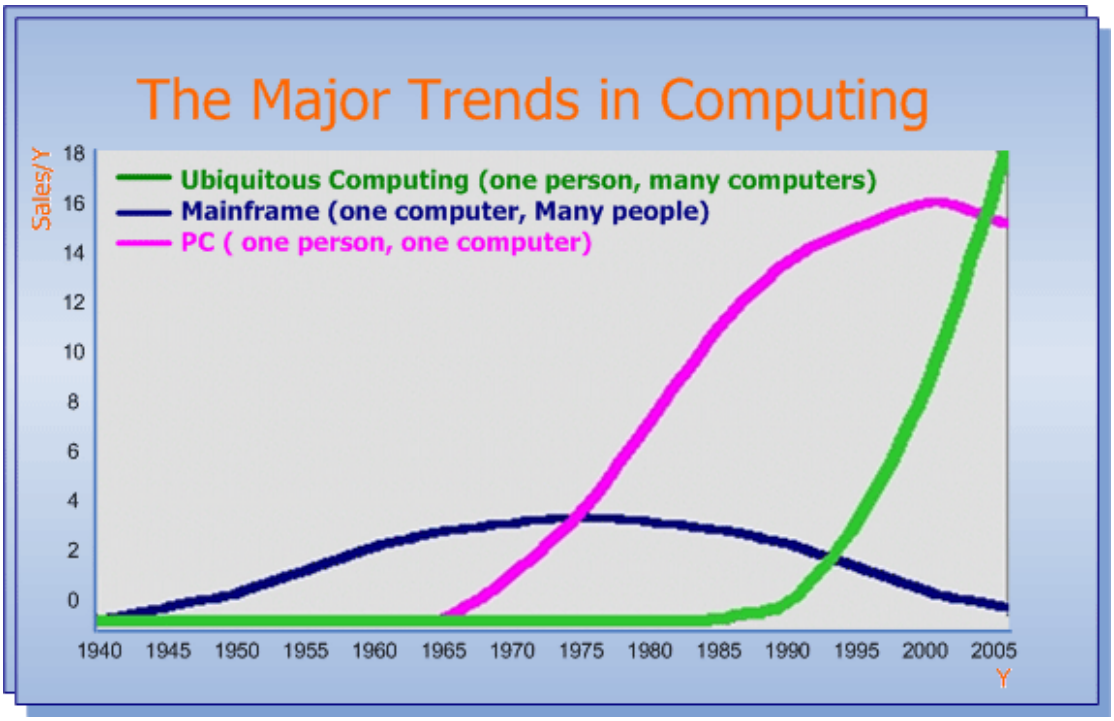
αξιοποιώντας το AP, προσφέρει στα τερματικά, όταν χρειάζεται, πρόσβαση στο κοινό μέσο χωρίς ανταγωνισμό και συγκρούσεις. Το DCF δίνει λύση στα, έμφυτα στις ασύρματες επικοινωνίες, προβλήματα του κρυμμένου τερματικού και του εκτεθειμένου τερματικού, τα οποία είναι και ο λόγος για τον οποίον δεν μπορεί να εφαρμοστεί η μέθοδος CSMA/CD του Ethernet σε WLAN. Το πρόβλημα του κρυμμένου τερματικού έγκειται στο ότι αν ένα τερματικό Γ εκπέμπει σε ένα τερματικό Β, ένα άλλο τερματικό Α που θέλει να αποστείλει δεδομένα στο Β αλλά είναι εκτός εμβέλειας του Γ δεν θα ανιχνεύσει ότι το κανάλι είναι απασχολημένο και θα εκπέμψει. Το αντίστροφο πρόβλημα του εκτεθειμένου τερματικού αφορά το ότι ένα τερματικό Α μπορεί να μη μεταδώσει πλαίσιο σε ένα άλλο τερματικό Β, νομίζοντας ότι το κανάλι είναι κατειλημμένο γιατί ανιχνεύει εκπομπή από ένα τερματικό Γ προς ένα τερματικό Δ. Τα Γ και Δ όμως είναι εκτός εμβέλειας του Β άρα στην πραγματικότητα δεν επρόκειτο να γίνει σύγκρουση.

Εικόνα 4 - Δίκτυο Bluetooth

2.4 Βασικές έννοιες του Ubiquitous Computing

Στην ιστορία των υπολογιστών έχουμε περάσει σε τρία στάδια εξέλιξης.

- Το πρώτο, mainframe, ήταν η εποχή που έναν υπολογιστή τον χειριζόμασταν πολλοί άνθρωποι διότι στην αρχή της γέννησης των υπολογιστών ήταν πολύ δύσκολο στο να έχει κάποιος το προσωπικό του υπολογιστή.
- Το δεύτερο είναι το στάδιο όπου ο καθένας μπορούσε να έχει τον δικό του προσωπικό υπολογιστή Personal Computer (PC).
- Και το τρίτο στάδιο που βρισκόμαστε τώρα είναι το στάδιο του Ubiquitous Computing όπου το κάθε άτομο μπορεί να χειρίζεται πολλούς υπολογιστές.



Εικόνα 5 - Τα στάδια των υπολογιστικών συστημάτων

Παραδείγματα του Ubiquitous Computing αποτελούν τα :

- Κινητά και ασύρματα δίκτυα.
- Hands Free διεπαφές χρήστη.
- Υπηρεσίες καθορισμού θέσεις και τοποθεσίας.

- Αόρατη υπολογιστική.
- Υπολογιστική σε ρούχα.

Δηλαδή το Ubiquitous Computing αλληλεπιδρά με το περιβάλλον και με εμάς σε μια αρμονική συνύπαρξη με σκοπό την απλοποίηση της ζωής των ανθρώπων.

Εικόνα 6 - Αλληλεπίδραση μεταξύ των στοιχείων του UbiquitousComputing

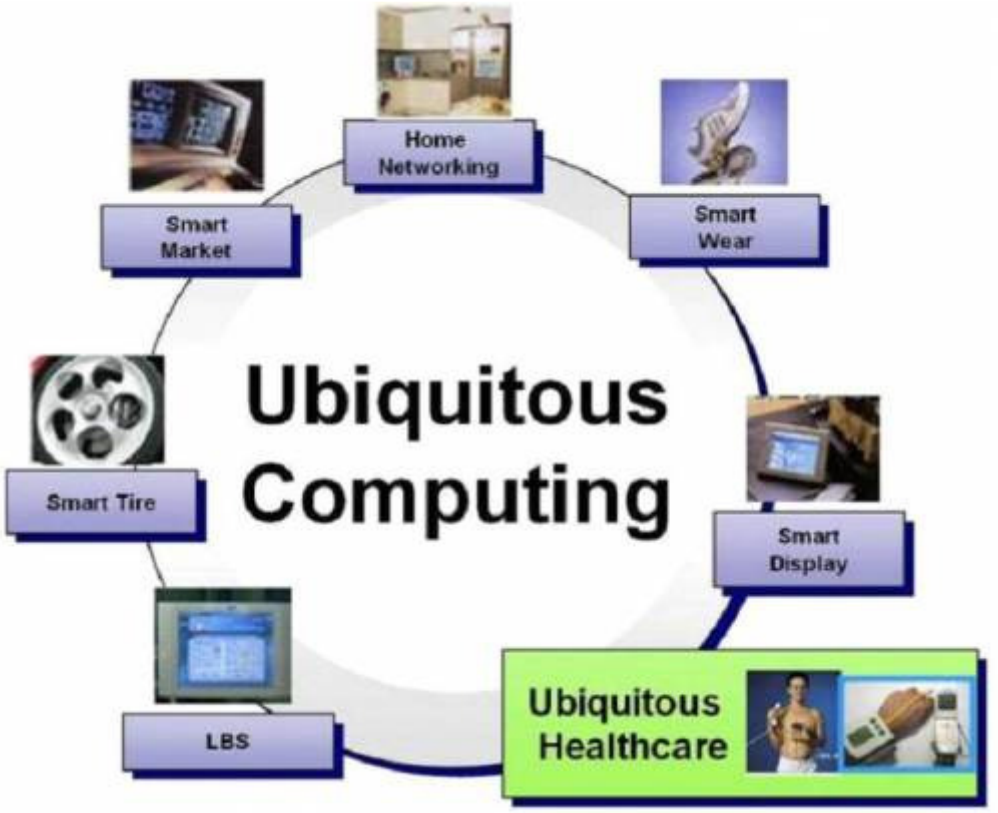
Βιβλιογραφία Κεφαλαίου

1. Pfeifer, T. (2003). *Ubiquitous computing*. Amsterdam: Elsevier.
2. Poslad, S. (2009). *Ubiquitous Computing*.
3. Samourlis, K. (2009). Ubiquitous and Pervasive Networks. Retrieved September 9, 2015, from http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/ergasies/2009/Ubiquitous and Pervasive Networks.pdf
4. Ubiquitous Computing / Persuasive Computing. (n.d.). *Integrierte Informationsarchitektur X.media.press,* 275-283.
5. Καμέας, Α, & Καραγιαννίδης, Χ. (n.d.). Συνεργατικά Συστήματα Διάχυτου Υπολογισμού και Περιρρέουσας Νοημοσύνης. Retrieved September 9, 2015, from http://karagian.users.uth.gr/cscl/15-Kameas-Karagiannidis.pdf
6. Στεφανόπουλος, Γ. (n.d.). Σχεδιασμός και ανάπτυξη οντοτήτων για περιβάλλοντα περιρρέουσας νοημοσύνης. Retrieved September 9, 2015, from http://nemertes.lis.upatras.gr/jspui/handle/10889/3907

ΚΕΦΑΛΑΙΟ 3: Υλικό του Ubiquitous Computing

Προκειμένου να γίνει πραγματικότητα ένα περιβάλλον με Ubiquitous Computing συγκεκριμένες τεχνολογίες είναι απαραίτητες (Aarts – Harwigetal.,2003):

- Τεχνολογίες πρόσβασης όπως κινητά τηλέφωνα, laptop και PDA.
- Τεχνολογίες αντίληψης και πρόσληψης συγκεκριμένων παραμέτρων του περιβάλλοντος όπως αισθητήρες, sensors, RFIDs.
- Τεχνολογίες επικοινωνίας όπως τα ασύρματα δίκτυα.
- Τεχνολογίας ασφαλείας δικτύων όπως firewalls, digital signatures.



Εικόνα 7 - Hardwareκαι περιβάλλον Ubiquitous Computing

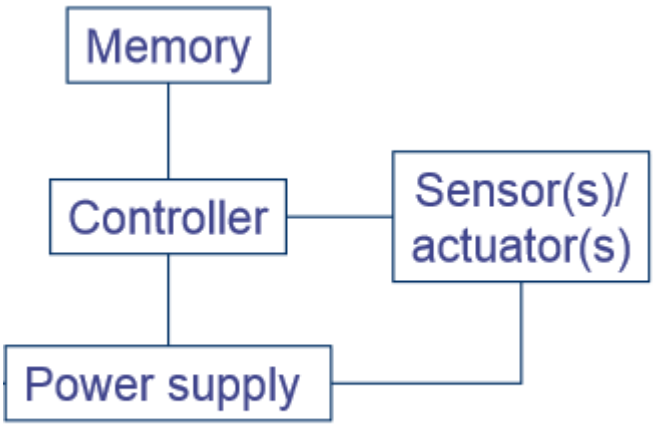
3.1 Τεχνολογίες αντίληψης και πρόσληψης συγκεκριμένων παραμέτρων του περιβάλλοντος

Όταν μπαίνουμε σε κάποιο μοντέρνο κτίριο είναι πλέον συνηθισμένο οι πόρτες να ανοίγουν αυτόματα. Το ίδιο συμβαίνει και όταν μπαίνουμε σε κάποιο σκοτεινό δωμάτιο και τα φώτα ανάβουν αυτόματα. Αυτές οι συνηθισμένες πλέον λειτουργίες υλοποιούνται με την χρήση αισθητήρων αντίληψης (sensors). Στα σπίτια του μέλλοντος όταν εισερχόμαστε σε ένα σπίτι θα μπορούμε να ακούμε το προσωπικό μας καλωσόρισμα και ενδεχομένως την απαραίτητη άδεια για να εισέλθουμε σε συγκεκριμένες περιοχές και δωμάτια του σπιτιού. Για να είναι δυνατή αυτή η υλοποίηση στα σπίτια του μέλλοντος απαραίτητοι είναι οι αισθητήρες που θα μας επιτρέπουν να λαμβάνουμε τα στοιχεία από το περιβάλλον και στην συνέχεια να τα αξιολογούμε και να τα διαχειριζόμαστε (Intille).

Οι σένσορες με την μεγάλη πληθώρα λύσεων που βρίσκονται αυτή την στιγμή στην αγορά, μαζί με το χαμηλό κόστος που τα συνοδεύει έχουν επηρεάσει σε θετικό βαθμό την ζωή μας και μας φέρνουν ένα βήμα πιο κοντά στην διάχυτη υπολογιστική καθώς επίσης και στις εφαρμογές που θα έχει στα σύγχρονα σπίτια του μέλλοντος. Οι αισθητήρες αφού μπορούν πλέον να αποκτηθούν τόσο εύκολα μπορούν να εκμεταλλευτούν ένα ακόμη χαρακτηριστικό της τεχνολογικής μας εποχής που είναι τα ασύρματα δίκτυα. Έτσι οι παράμετροι και τα δεδομένα που «διαβάζουν» και εντοπίζουν, με την χρήση των ασύρματων δικτύων, μεταφέρονται σε υπολογιστικά συστήματα όπου γίνεται η επεξεργασία των δεδομένων.

3.2 Αρχιτεκτονική

Η βασική αρχιτεκτονική ενός συστήματος αισθητήρων για χρήση διάχυτης υπολογιστικής μπορεί να φανεί στο παρακάτω σχήμα.



Εικόνα 8 - Αρχιτεκτονική Controller – Sensor

Τα βασικά του χαρακτηριστικά όπως βλέπουμε είναι

- Ο αισθητήρας.
- Το υπολογιστικό σύστημα ή controller. Στους controllers θα αναφερθούμε στην συνέχεια του κεφαλαίου.
- Η μνήμη που συνήθως βρίσκεται ενσωματωμένη στον επεξεργαστή.
- Την πηγή ενέργειας, που συνήθως είναι κάποιου είδους μπαταρία.

3.3 Είδη αισθητήρων

Τα είδη των αισθητήρων μπορούν να ταξινομηθούν σε 8 μεγάλες κατηγορίες που καλύπτουν σχεδόν όλες τις κατηγορίες.

- Κίνησης, όπου ανιχνεύεται η κίνηση ενός αντικειμένου. Ο αισθητήρας βρίσκεται σε αδρανοποίηση και όταν κάποιο αντικείμενο ανιχνευθεί τότε εκτελείται ένα «ξύπνημα» στον επεξεργαστή.
- Επιτάχυνσης, λειτουργούν σε πρώτο στάδιο όπως οι αισθητήρες κίνησης αλλά επιπλέον μπορούν να υπολογίσουν τροχιές και πορείες των αντικειμένων.
- Φωτός, διάφορες μετρήσεις εντάσεως του φωτός λαμβάνονται ανά τακτά χρονικά διαστήματα και χρησιμοποιούνται κυρίως για την ανίχνευση περιβαλλοντικών συνθηκών.

- Εγγύτητας, δηλαδή πόσο κοντά έρχεται στο σημείο μέτρησης το αντικείμενο που παρακολουθούμε. Ο προσδιορισμός εγγύτητας στις περισσότερες περιπτώσεις γίνεται με παθητικού αισθητήρες υπερύθρων. Συνήθως φέρουν ένα ολοκληρωμένο σχεδιασμό και ενεργοποιούνται εάν υπάρχει δραστηριότητα σε μια περιοχή που παρατηρείται.
- Ήχου, η ανάλυση ακουστικών πληροφοριών από το περιβάλλον μπορεί να να είναι χρήσιμη για την κατανόηση της περιοχής που μελετάμε. Ακόμη και απλοί αλγόριθμοι μπορούν μας παρέχουν πολύτιμες πληροφορίες. Επιπλέον η στάθμη του ήχου μπορεί να οδηγήσει σε συμπεράσματα σχετικά με το επίπεδο δραστηριότητας εγγύτητας (Robinson et al)
- Θερμοκρασίας, όπου ο αισθητήρας λαμβάνει σαν πληροφορία την εξωτερική θερμοκρασία ενός συγκεκριμένου χώρου. Επιπλέον πολύ σημαντική πληροφορία μπορεί να μας δώσει η αλλαγή και αυξομείωση θερμοκρασίας σε περιόδους που εμείς έχουμε ορίσει.
- Μηχανικής πίεσης, είναι οι αισθητήρες που μας επιτρέπουν να ανακαλύψουμε αν υπάρχει κάποιο βάρος ή αντικείμενο καθώς και η αλλαγή αυτής της πίεσης.
- Υγρασίας, η υγρασία του αέρα είναι χρήσιμη για τα δεδομένα μας τόσο σε περιβαλλοντικές όσο και εσωτερικές συνθήκες. Αυτή η μέτρηση μπορεί να αξιοποιηθεί για την παρακολούθηση αντικειμένων κατά την διάρκεια της μεταφοράς τους καθώς και της αποθήκευσης όπως κρασί και πίνακες ζωγραφικής.

Επιπλέον μπορούν να χωριστούν είτε σε παθητικά συστήματα είτε σε ενεργά πχ. ραντάρ. (Beigl et al., 2015)

3.4 Υπολογιστικά συστήματα micro – controller

Με τον όρο micro – controller ή μικροελεγκτή εννοούμε έναν τύπο επεξεργαστή, ουσιαστικά μια παραλλαγή μικροεπεξεργαστή, ο οποίος μπορεί να λειτουργήσει με ελάχιστα εξωτερικά εξαρτήματα, λόγω των πολλών ενσωματωμένων υποσυστημάτων που διαθέτει. Χρησιμοποιείται ευρύτατα σε όλα τα ενσωματωμένα συστήματα (embedded systems) ελέγχου χαμηλού και μεσαίου κόστους, όπως αυτά που χρησιμοποιούνται σε αυτοματισμούς, ηλεκτρονικά καταναλωτικά προϊόντα (από

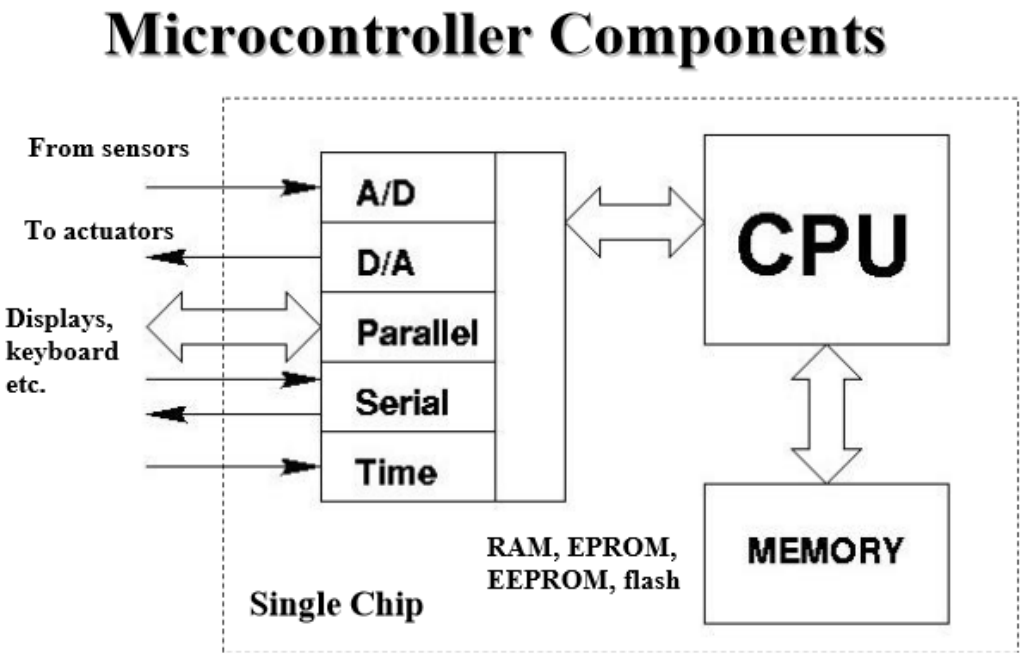
ψηφιακές φωτογραφικές μηχανές έως παιχνίδια), ηλεκτρικές συσκευές και κάθε είδους αυτοκινούμενα τροχοφόρα οχήματα (Durfee, 2011).

Ένας μικροελεγκτής είναι ένα μικρού, χαμηλού κόστους υπολογιστής ο οποίος συνήθως περιλαμβάνει:

- 8 ή 16 bit μικροεπεξεργαστή (CPU).
- Μια μικρή ποσότητα της μνήμης RAM.
- Προγραμματιζόμενη ROM ή / και τη μνήμη flash.
- Παράλληλες ή / και διαδοχικές εισόδους και εξόδους.

Συχνά χρησιμοποιείται για να τρέξει ειδικό λογισμικό που ελέγχει μία ή περισσότερες εργασίες στη λειτουργία μιας συσκευής ή ενός συστήματος. Αυτός είναι και ο κυριότερος λόγος που μας είναι τόσο απαραίτητοι στην δημιουργία ενός συστήματος Ubiquitous Computing.

Οι συσκευές που χρησιμοποιούν μικροελεγκτές βρίσκονται σε μια πληθώρα αντικειμένων στην καθημερινή μας ζωή όπως, ηλεκτρονικά είδη ευρείας κατανάλωσης (βίντεο, φούρνους μικροκυμάτων, φωτογραφικές μηχανές, συσκευές τηλεειδοποίησης, τα κινητά τηλέφωνα), περιφερειακά υπολογιστών (πληκτρολόγια, εκτυπωτές, μόντεμ). Οι μικροελεγκτές συνήθως έχουν χαμηλές απαιτήσεις ισχύος (~ 05 - 0.1 W σε αντίθεση με ~ 10-50 W που χρειάζονται οι γενικής χρήσης επεξεργαστές CPU’s), και επιπλέον πολλές συσκευές λειτουργούν με μπαταρία.



Εικόνα 9 - Βασικά μέρη ενός μικροελεγκτή

3.5 Είδη micro-controllers

Με την ξέφρενη ανάπτυξη της τεχνολογίας και των υπολογιστικών συστημάτων γενικότερα, είναι πλέον γεγονός η πληθωρά των μικρο-ελεγκτών που μπορούν να βρεθούν στην αγορά. Το κόστος τους είναι πάρα πολύ προσιτό και φυσικά μπορούν να προγραμματιστούν και να υλοποιούν μια τεράστια γκάμα από εργασίες και εφαρμογές κάτι που τους καθιστά απαραίτητους για τις εφαρμογές σε σύγχρονα σπίτια. Τα πιο διαδεδομένα συστήματα που υπάρχουν αυτή την στιγμή είναι τα εξής :

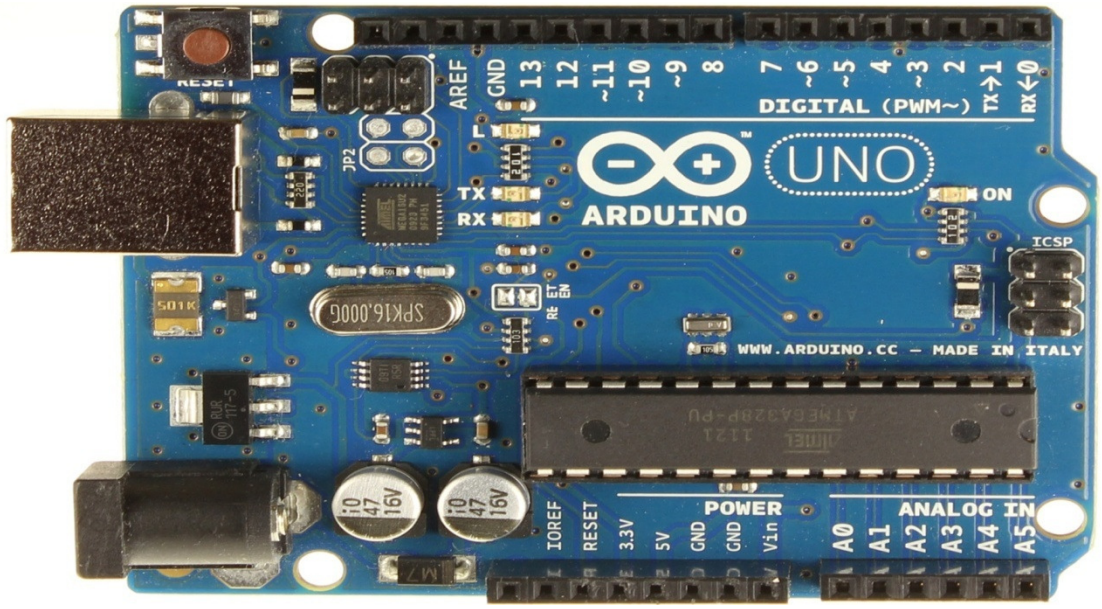
- Arduino
- Raspberry Pi
- BeagleBone
- Teensy 2.0
- STM32 Discovery
- Pinguino PIC32
- Nanode
- MSP 420 LauchPad

Στην συνέχεια θα συζητήσουμε για τα σημαντικότερα εξ αυτών καθώς και τις δυνατότητες τις οποίες παρέχουν.

3.5.1 Arduino

Το Arduino είναι μια ηλεκτρονική πλατφόρμα ανοικτού κώδικα και σχεδιασμού και είναι εύκολο στη χρήση υλικού και λογισμικού. Προορίζεται για καλλιτέχνες, σχεδιαστές, υλοποίηση χόμπι και δραστηριοτήτων, και γενικότερα για οποιονδήποτε ενδιαφέρεται να δημιουργήσει αλληλεπιδραστικά αντικείμενα ή περιβάλλοντα. Για να μιλήσουμε λίγο πιο τεχνικά, υπάρχει ένα κύκλωμα που χρησιμοποιεί μικροελεγκτή, το οποίο μας δίνει ένα αριθμό πυλών οι οποίες μπορούν να λειτουργήσουν είτε ως είσοδοι είτε ως έξοδοι στα κυκλώματά μας. Αυτές τις εισόδους ή εξόδους μπορούμε να τις διαχειριστούμε γράφοντας κώδικα στο περιβάλλον προγραμματισμού Arduino IDE που έχει βασιστεί στη γλώσσα C/C++.

Το κύκλωμα των μονάδων του Arduino είναι ανοικτό, δηλαδή ο σχεδιασμός και τα μέρη του είναι γνωστά και δίνονται από τους κατασκευαστές του, με αποτέλεσμα όποιος θελήσει να μπορεί να το υλοποιήσει. Έτσι, υπάρχει υλικό με την ονομασία Arduino που προέρχεται από τους δημιουργούς και επίσημους κατασκευαστές του στην Ιταλία, ενώ μπορείτε να βρείτε πάρα πολλές ακόμα υλοποιήσεις μονάδων του, απόλυτα συμβατές με τα προγράμματα και κυκλώματα που ενδεχομένως ήδη υπάρχουν και δουλεύουν με τις επίσημες μονάδες Arduino.



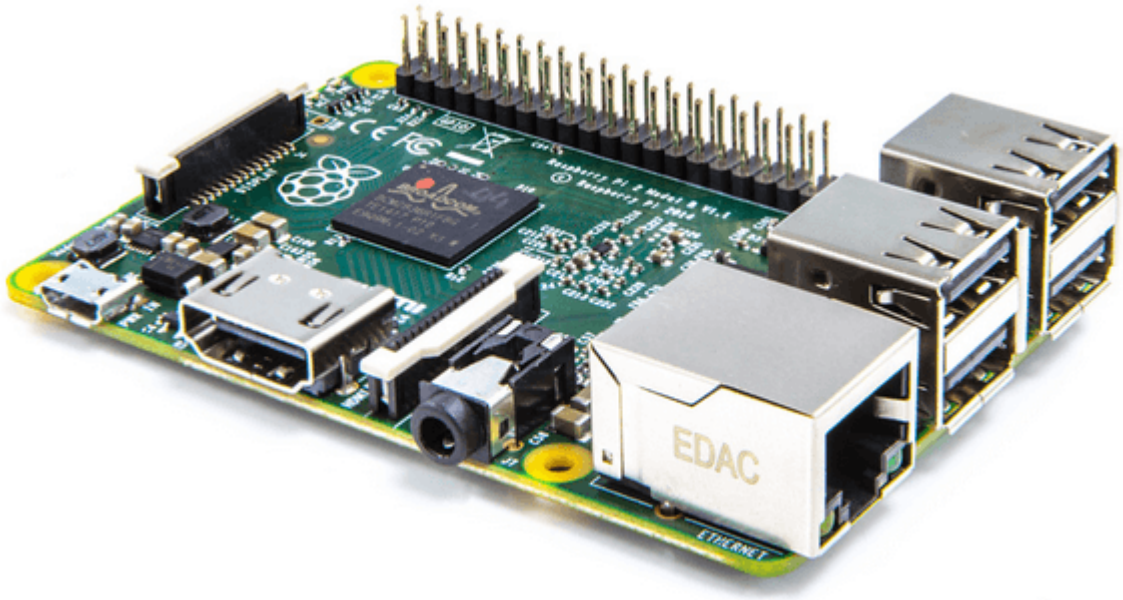
Εικόνα 10 – Arduino

Εκτός από τη βασική έκδοση του περιβάλλοντος Arduino IDE, υπάρχει και μια παραλλαγμένη έκδοση του Scratch, η οποία μπορεί να χρησιμοποιηθεί για να γράψουμε προγράμματα για το Arduino, η S4A - Scratch For Arduino, η οποία επίσης είναι ανοικτού κώδικα και δωρεάν. Το πλεονέκτημα της έκδοσης αυτής είναι ο οπτικός προγραμματισμός (blocks όπως στο Scratch) σε σχέση με το γράψιμο εντολών στο κλασσικό περιβάλλον. Παρόμοιας λογικής είναι και το ArduBlock, το οποίο επίσης χρησιμοποιεί οπτικό προγραμματισμό μέσω έτοιμων blocks για τον προγραμματισμό του. Ακόμα, υπάρχουν οπτικές εκδόσεις στο διαδίκτυο (web περιβάλλοντα), όπως το BlocklyDuino ή τοArduinoMio. (Πουλάκης, 2015)

3.5.2 Raspberry Pi

Το Rasppberry Pi είναι ένας πλήρης υπολογιστής με μέγεθος πιστωτικής κάρτας.

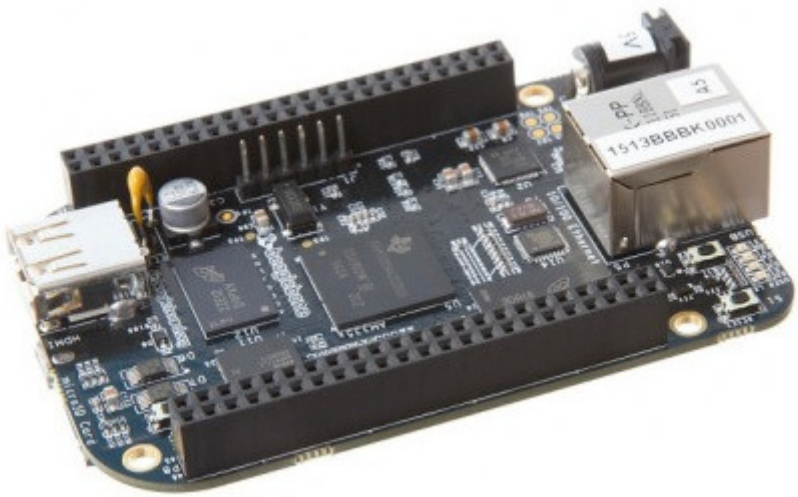
Η τελευταία του έκδοση, Raspberry Pi 2, με τετραπύρηνο επεξεργαστή τύπου ARM και 1GB RAM κοστίζει γύρω στα 45 ευρώ στην Ελλάδα, ενώ ξεχωριστά θα βρούμε το πλήρες kit με όσα χρειάζονται για να το αξιοποιήσουμε.



Εικόνα 11 - Raspberry Pi

Παρά τον ελάχιστον όγκο του, το Raspberry Pi διαθέτει τετραπύρηνο επεξεργαστή 900MHz, διπύρηνη κάρτα γραφικών, 1GB RAM, τέσσερις θύρες USB, έξοδο HDMI, τροφοδοτείται μέσω Micro USB, και 40 pins γενικής χρήσης για σύνδεση με άλλα ηλεκτρονικά και περιφερειακά. Η σημαντικότερη καινοτομία της νέας έκδοσης του Raspberry Pi είναι πως θα μπορεί να τρέξει τα επερχόμενα Windows 10.

3.5.3 BeagleBone



Εικόνα 12 - BeangleBone

Η πλατφόρμα BeagleBoard προέκυψε το 2008 από την συνεργασία της Texas Instruments σε συνεργασία με την Digi-Key και την Newark element14. Η πρώτη υλοποίηση που προέκυψε από την συνεργασία αυτή ήταν ένα υπολογιστικό σύστημα 75×75 χιλιοστών, με επεξεργαστή TI OMAP3530 ARM Cortex-A8 στα 720MHz, με τους TMS320C64x+ DSP και PowerVRSGX530 σταγραφικά,256 MB NAND μνήμη για αποθήκευση και 256 MB RAM, USB και HDMI.

Το σύστημα ήταν σε θέση να λειτουργήσει με Linux, FreeBSD, RISC OS, Symbian καθώς και Android. Ανήκει στον χώρο του «open-source hardware», είναι δηλαδή ανοιχτής αρχιτεκτονικής και στηρίζεται από ανοιχτό λογισμικό, ενώ πωλείται στο κοινό υπό μία τύπου «Creative Commons» άδεια.

Το BeagleBone Black κοστίζει 45 δολάρια ΗΠΑ και απευθύνεται σε προγραμματιστές και χομπίστες. Χρειάζεται μόλις 10 δευτερόλεπτα για να εκκινήσει μια διανομή Linux. Φέρει έναν Sitara ARM Cortex-A8 [2000 MIPS] επεξεργαστή της Texas Instruments, χρονισμένο στο 1GHz, συνεπεξεργαστή γραφικών SGX530, μνήμη 512MB DDR3L 800MHz SDRAM και χρησιμοποιεί 2GB Embedded MMC μνήμη για αποθηκευτικό χώρο. Οι διαστάσεις του είναι 8.6×5.3 εκατοστά και ζυγίζει μόλις 40 γραμμάρια (Ορφανίδης, 2013).

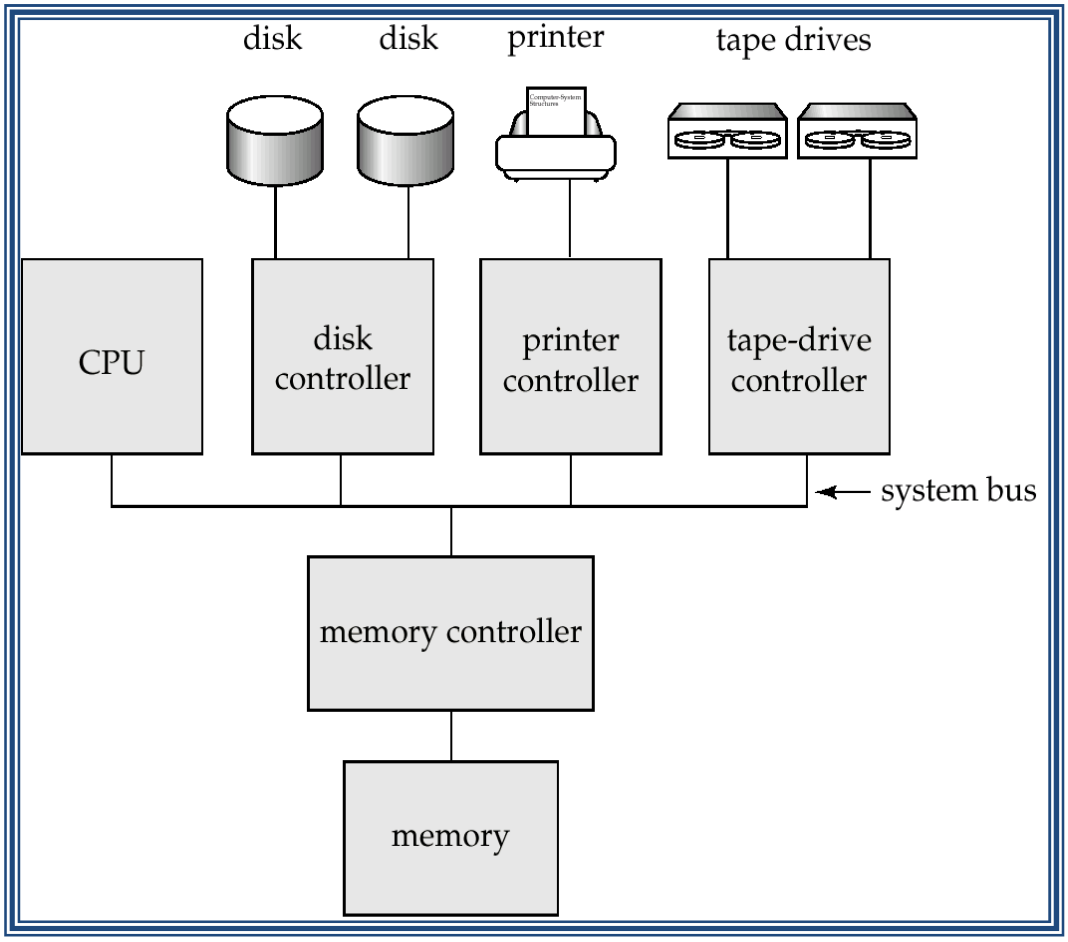
3.6 Βασικές αρχιτεκτονικές Ubiquitous Computing

Το Ubiquitous Computing ακολουθεί τις ίδιες αρχές και λειτουργίες με όλα τα υπολογιστικά συστήματα οπότε είναι λογικό και η δομή που μπορεί να παρουσιάζει να αποτελεί λογική συνέχεια αυτών.

Οι δυο βασικές δομές της πανταχού υπολογιστικής είναι η συγκεντρωτική και κατανεμημένη δομή.

Τα συγκεντρωτικά συστήματα εκτελούνται σε ένα μόνο υπολογιστικό σύστημα και δεν αλληλεπιδρούν με άλλα υπολογιστικά συστήματα. Πρόκειται για υπολογιστικό σύστημα κοινής χρήσης που διαθέτει μία η δύο το πολύ κεντρικούς επεξεργαστές και παρέχεται διαμοιρασμός σε κοινή μνήμη. Το σύστημα αυτό παρουσιάζεται σαν ένα στον χρήστη. Επιπλέον η δομή αυτή είναι ένα σύστημα ενός χρήστη , όπως ο προσωπικός υπολογιστής, όπου και το λειτουργικό σύστημα μπορεί να υποστηρίξει μόνο έναν χρήστη σε οποιαδήποτε στιγμή.

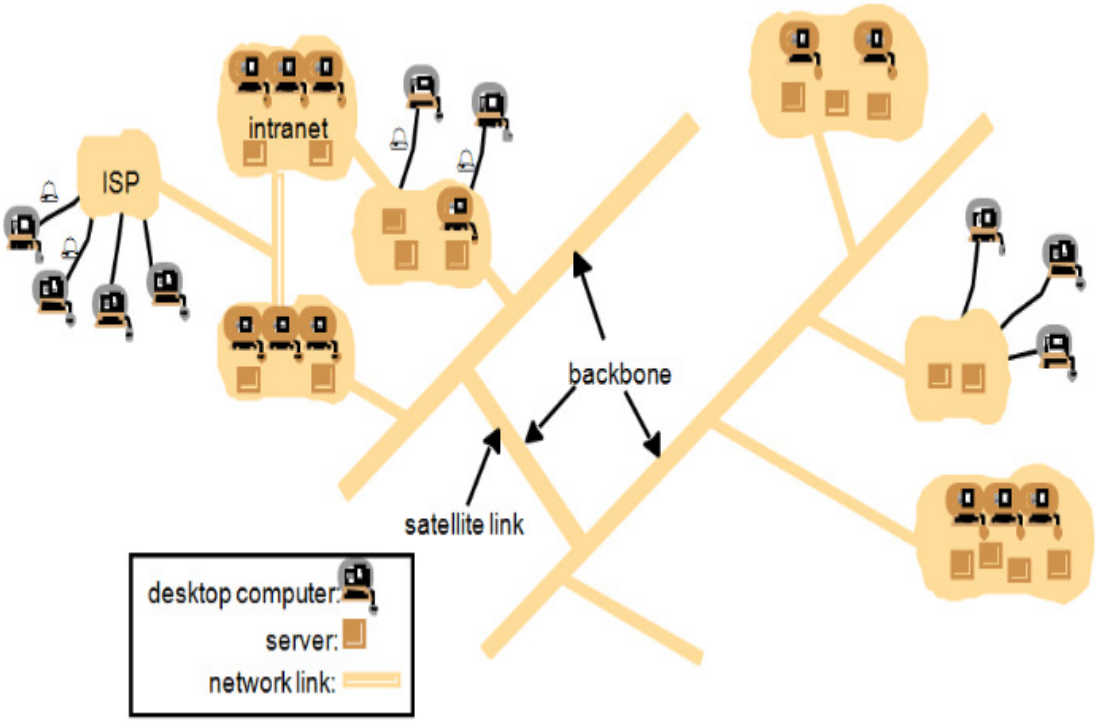
Σχηματικά ένα τέτοιο συγκεντρωτικό σύστημα αποτελεί το παρακάτω.



Εικόνα 13 - Συγκεντρωτικό σύστημα

Τα κατανεμημένα συστήματα (ΚΣ) αποτελούν ένα σύνολο υπολογιστικών συστημάτων κατάλληλα συνδεδεμένα έτσι ώστε να παρουσιάζονται σαν ένα στον τελικό χρήστη. Τα συστατικά αυτού του συστήματος, υλικό και λογισμικό, βρίσκονται σε συνδεδεμένους υπολογιστές που επικοινωνούν μεταξύ τους. Ο βασικός λόγος κατασκευής ενός τέτοιου συστήματος αποτελεί ο διαμοιρασμός πόρων που είτε μπορεί να είναι υλικό ,π.χ. CPU, είτε δεδομένα.

Ένα τέτοιο κατανεμημένο σύστημα είναι το διαδίκτυο που παρουσιάζεται σχηματικά.



Εικόνα 14 - Κατανεμημένα συστήματα - Διαδίκτυο

Βιβλιογραφία Κεφαλαίου

1. Beigl, M., Krohn, A., Zimmer, T., & Decker, C. (n.d.). Typical Sensors needed in Ubiquitous and Pervasive Computing. Retrieved September 9, 2015, from http://www.teco.edu/~michael/publication/inss.pdf
2. Durfee, W. (2011, October 1). Arduino Microcontroller Guide. Retrieved September 9, 2015, from http://www.me.umn.edu/courses/me2011/arduino/arduinoGuide.pdf
3. Grilo, A. (n.d.). Wireless Sensor Networks Chapter 2: Single node architecture. Retrieved September 9, 2015, from http://comp.ist.utl.pt/ece-wsn/doc/slides/sensys-ch2-single-node.pdf
4. Intille, S. (n.d.). Designing a home of the future. *IEEE Pervasive Comput. IEEE Pervasive Computing,* 76-82.
5. McManus, S., & Cook, M. (n.d.). *Raspberry Pi for dummies* (2nd ed.).
6. Robinson, P., & Beigl, M. (n.d.). Trust Context Spaces: An Infrastructure for Pervasive Security in Context-Aware Environments. *Security in Pervasive Computing Lecture Notes in Computer Science,* 157-172.
7. Tapia, E. (2003). *Activity recognition in the home setting using simple and ubiquitous sensors*.
8. Yoder, M., & Kridner, J. (n.d.). *BeagleBone cookbook*.
9. Ορφανίδης, Β. (2013). BeagleBone Black από την BeagleBoard. Retrieved September 9, 2015, from http://fullpc.gr/news/hardware/beaglebone-black-apo-tin-beagleboard-video
10. Γκουμόπουλος, Χ. (n.d.). *Κατανεμημένα Συστήματα Βασικές Έννοιες, Αρχιτεκτονικά Μοντέλα, Σχεδιαστικές Προκλήσεις*. Retrieved September 9, 2015, from http://www.icsd.aegean.gr/kaporisa/index_files/02_distsyst_basic_concepts.pdf
11. Πουλάκης, Ε. (2015). *Προγραμματίζοντας με τον μικροελεγκτή Arduino*. Retrieved September 9, 2015, from http://users.sch.gr/manpoul/docs/arduino/ProgrammingArduino.pdf

ΚΕΦΑΛΑΙΟ 4: Δομές Ασφαλείας του Ubiquitous Computing

Στην σημερινή τεχνολογική εποχή η ανάγκη για ασφάλεια δεδομένων είναι κάτι παραπάνω από επιβεβλημένη. Όμως τι ορίζουμε ασφάλεια δεδομένων και δομές ασφαλείας γενικότερα και τι σχέση που έχουνε με το Ubiquitous Computing; Η λέξη ασφάλεια χαρακτηρίζει πλέον όλες τις πρόσφατες τεχνολογίες και αποτελεί κάποιου είδους μόδα και πάντοτε τροφή για συζήτηση. Οπότε είναι απαραίτητη η κριτική σκοπιά που θα πρέπει να διατηρήσουμε και να αναλύσουμε συγκεκριμένα αντικείμενα.

Καθώς όλο και περισσότερες συσκευές και εφαρμογές με δυνατότητες Internet εισέρχονται στην αγορά, η προστασία αυτών των συσκευών από τους χάκερ γίνεται κρίσιμη και επιβεβλημένη. Δυστυχώς, πολλά από αυτά τα έξυπνα συστήματα, από τις τουαλέτες και τα ψυγεία μέχρι τα συστήματα συναγερμού, δεν χτίστηκαν με γνώμονα την ασφάλεια καθώς αρχικά ήθελα να καλύψουν άλλες ανάγκες.

Τι είναι αυτό όμως που μπορεί να κάνει ο χρήστης και οι εταιρίες κατασκευής τέτοιων συστημάτων; Όταν πρόκειται για το Ubiquitous Computing και των συσκευών που είναι συνδεδεμένα στο σπίτι, είναι καλύτερο να ασφαλίσουμε ενεργά το οικιακό δίκτυο. Δεν υπάρχει λογισμικό προστασίας από ιούς για μια έξυπνη τηλεόραση, αλλά μπορείτε να προστατεύσετε το Wi-Fi του δικτύου σας, έτσι ώστε η τηλεόραση να μη γίνει μια κερκόπορτα στο σπίτι σας.

Η αγορά πλέον των έξυπνων συσκευών αποτελείται από ιλιγγιώδη οικονομικά νούμερα και αναμένεται να ξεπεράσει τα 7.100 δις δολάρια μέχρι το τέλους του 2010. Ευτυχώς όμως οι έρευνες ότι οι χρήστες ήδη είναι επιφυλακτικοί και προσεκτικοί όσον αφορά τον τομέα της ασφάλειας. Σε δείγμα 1801 κατόχων τεχνολογίας έξυπνων σπιτιών, σε 11 χώρες, το 70 % απάντησε ότι είναι ιδιαιτέρως ανήσυχο για την ασφάλεια και μια ενδεχόμενη διαρροή προσωπικών στοιχείων [11].

Η προστασία των προσωπικών δεδομένων είναι μια ευρεία έννοια και προκειμένου να συζητήσουμε θέματα που αφορούν την ιδιωτική ζωή, είναι

σημαντικό να συνειδητοποιήσουμε τι είναι. Ο ορισμός είναι ο εξής (Berg, Borcea-Ptzmann, 2011):

Η προστασία προσωπικών δεδομένων μιας οντότητας είναι το αποτέλεσμα της διαπραγμάτευσης και της επιβολής πότε, πώς, σε ποιο βαθμό, και σε ποιο πλαίσιο τα οποία δεδομένα του εν λόγω φορέα αποκαλύπτονται σε κάποιον τρίτον.

Αρχικά στον όρο ασφάλεια θα πρέπει να διαχωρίσουμε τα αντικείμενα τα οποία θέλουμε να διαφυλάξουμε, έπειτα να αναρωτηθούμε για τις ενδεχόμενες απειλές που θα μπορούσαν να συμβούν, να δούμε συγκεκριμένες ευπάθειες του συστήματος μας, τις διαθέσιμες τεχνικές επίθεσης που ενδεχομένως να χρησιμοποιήσει κάποιος τρίτος εναντίον μας καθώς και τους κινδύνους και τα αποτελέσματα τα οποία προκύπτουν εάν αυτή η επίθεση καταστεί επιτυχής. Τέλος αναγνωρίζουμε διαθέσιμα και απαραίτητα αντίμετρα και δικλείδες ασφαλείας που θα μας προστατεύσουν.

Οι βασικές απειλές κατά των συστημάτων πληροφοριών κατατάσσονται με βάση τρεις θεμελιώδεις ιδιότητες ασφαλείας που θα μπορούσαν να παραβιάζουν:

- Εμπιστευτικότητα, ότι μόνο εξουσιοδοτημένοι αρχές μπορούν να διαβάσουν τις πληροφορίες.
- Ακεραιότητα, εξασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να τροποποιήσουν τις πληροφορίες.
- Διαθεσιμότητα, εξασφαλίζοντας, ότι οι χρήστες μπορούν να έχουν πρόσβαση και να χρησιμοποιήσουν το σύστημα, χωρίς αδικαιολόγητες καθυστερήσεις.

Θα διαπιστώσετε ότι σε πολλές περιπτώσεις οι άνθρωποι αυτόματα υποθέτουν ότι το πρωταρχικό μέλημα ασφαλείας είναι η προστασία του απορρήτου (εμπιστευτικότητα) αλλά με μια δεύτερη ματιά, διαπιστώνουμε ότι η ακεραιότητα είναι μακράν πιο σημαντική.

Η προστασία των προσωπικών δεδομένων είναι ένα περίπλοκο ζήτημα για την διάχυτη υπολογιστική όπου ο στόχος μας είναι η προστασία της ιδιωτικής ζωής του χρήστη. Αυτό όμως το κάνει ποιο δύσκολο το γεγονός ότι οι χρήστες δεν φαίνεται να ενδιαφέρονται ιδιαίτερα για την προστασία των προσωπικών τους δεδομένων και

δεύτερον πάντα υπάρχουν οικονομικοί περιορισμοί στην αναζήτηση ασφάλειας δεδομένων.

Ο καλύτερος τρόπος να αναλύσουμε την έννοια της ασφάλειας στην διάχυτη υπολογιστική είναι να δούμε τα ενδεχόμενα σενάρια επιθέσεων στις τεχνολογίες που χρησιμοποιούμε όπως Bluetooth, Wi-Fi, NFC, και άλλα καθώς και παραδείγματα αυτών των επιθέσεων.

Οι απαιτήσεις και οι λύσεις ενός ασφαλούς συστήματος είναι οι παρακάτω.

- Διαλειτουργικότητα, κάθε σύστημα θα πρέπει να συνδυάζεται και να συνεργάζεται με τις ήδη τεχνικές ασφαλείας.
- Διαθεσιμότητα, όπου πρέπει η εφαρμογή μας να είναι συνεχώς προσβάσιμη.
- Προστασία, πρωτόκολλα διαπιστευτηρίων όπως SSL και IP Protection να υπάρχουν σε όλα τα επίπεδα ασφαλείας.
- Αντιπροσώπευση, αν μια υπηρεσία τρέχει για διάφορα δίκτυα και τα κινητά μέρη τους μπορούν να αλλάξουν το δίκτυο για αυτό είναι απαραίτητο για τους χρήστες να εξουσιοδοτήσουν τις αλλαγές και να εκχωρήσουν το δικαίωμά τους σε μια λειτουργία διαχείρισης που εκτελείται για λογαριασμό τους.
- Προστασία πλατφόρμας, να μην επιτρέπεται να κατεβάζει κάποιος και να τροποποιήσει την εφαρμογή για να λειτουργεί με διαφορετικό τρόπο από τον αρχικό.
- Προστασία δεδομένων, όπου τα δεδομένα δεν θα πρέπει να παραποιούνται.

4.1 Διαθέσιμες μορφές Ubiquitous Computing και ασφάλεια

4.1.1 Wearable Technology

Όσο οι υπολογιστές γίνονται όλο και πιο μικροί, φθηνοί και ακόμη πιο δυνατοί τόσο πιο εύκολο μας γίνεται να τους κουβαλάμε πάνω μας και παντού. Η πραγματική ιδέα και ορισμός του Ubiquitous Computing είναι φυσικά αυτό, να έχουμε παντού πρόσβαση σε υπολογιστικά συστήματα και αυτό κατά κάποιο τρόπο συμβαίνει ήδη σήμερα με την χρήση των κινητών τηλεφώνων. Καθώς όλο και

περισσότερα από αυτά τα τηλέφωνα αποκτούν την ικανότητα να συνδεθούν με το Internet, για να τρέξουν εξωτερικές εφαρμογές και να ενεργούν και να χρησιμοποιούνται για χρήση ηλεκτρονικού ταχυδρομείου, η αρχιτεκτονική τους είναι παρόμοια με τους κοινούς υπολογιστές που χρησιμοποιούμε . Αυτό σημαίνει ότι μοιράζονται και τις ίδιες ευπάθειες συστήματος και είναι επιρρεπείς στις ίδιες τεχνικές επιθέσεων όπως ιοί, worms και Trojan horses. Δεδομένου ότι η συνάφεια μεταξύ των κινητών και των υπολογιστών είναι τόσο κοντινή είναι εύκολο πλέον οι επιθέσεις να ενοποιηθούν και στα δυο συστήματα.

Οι wearable κάμερες τύπου gopro αποτελούν πραγματικότητα και είναι ολοένα αυξανόμενος ο κόσμος που χρησιμοποιεί μια τεχνολογία που παλιότερα ήταν σενάριο επιστημονικής φαντασίας. Αυτό δείχνει ότι η wearable τεχνολογία βρίσκεται παντού τριγύρω μας και παρουσιάζει νέα προβλήματα και ανησυχίες ασφάλειας και προστασίας των προσωπικών δεδομένων. Καθώς η τεχνολογία κυριολεκτικά φοριέται και ταξιδεύει μαζί μας, αφού η wearable τεχνολογία όπως ψηφιακές κάμερες, κινητό τηλέφωνο, USB sticks και άλλα είδη βρίσκεται πάντα στην τσέπη μας. Οπότε αυτομάτως διατρέχουμε τον κίνδυνο απώλειας των δεδομένων που αποθηκεύονται σε αυτές τις συσκευές, καθώς παρά το μέγεθός τους επιτρέπεται η αποθήκευση στοιχείων αρκετών GB, αλλά πιο ανησυχητικό είναι το γεγονός της κλοπής προσωπικών στοιχείων για κακόβουλες πράξεις.

Για παράδειγμα, ζώνες και gadgets γυμναστικής που παρακολουθούν βιομετρικά στοιχεία π.χ. χτύποι καρδιάς μπορούν να αποκαλύψουν την τοποθεσία του χρήστη και θα μπορούσε να δώσει στους χάκερς λεπτομέρειες για τις καθημερινές ρουτίνες και συνήθειες του χρήστη. Έτσι θα μπορούσε να προσπελάσει τα συστήματα συναγερμού από απόσταση μέσω smartphone εφαρμογές. Οι διαρρήκτες θα μπορούσαν να χρησιμοποιήσουν τα δεδομένα που έχουν κλαπεί από κάθε τύπο συσκευής και να γνωρίζουν πότε είναι η κατάλληλη στιγμή να επιτεθούν στα άδεια σπίτια ενώ οι κάτοικοι είναι μακριά.

Τέλος υπάρχουν και άλλα προβλήματα ασφαλείας στις wearable τεχνολογίες που δεν είναι προφανή και σχετίζονται με την προστασία των προσωπικών δεδομένων περιοχής και τοποθεσίας και θα συζητηθεί στο επόμενο μέρος.

4.1.2 Προστασία Τοποθεσίας

Η τελευταία τεχνολογική εξέλιξη που χρησιμοποιείται κατά κόρον στις μέρες είναι οι τεχνολογίες και εφαρμογές που χρησιμοποιούν την τοποθεσία μας για να παράγουν το καλύτερο δυνατό αποτέλεσμα με βάση την περιοχή που βρισκόμαστε. Οι εφαρμογές αυτές ονομάζονται “location-based services”. Για παράδειγμα μία τέτοια εφαρμογή αποτελεί το google maps όπου με βάση την τοποθεσία μας μπορεί να μας προτείνει προορισμούς και διαδρομές με αφετηρία την αρχική μας θέση. Βέβαια το γεγονός αυτό προξενεί σημείο τριβής για τους επιστήμονες και τους ερευνητές, η προστασία αυτών των δεδομένων, ειδικά τώρα που τα σύγχρονα κινητά τηλέφωνα έχουν ευκρίνεια θέσης μικρότερη από τα 10 μέτρα.

Το γεγονός ότι η εφαρμογή μπορεί να γνωρίζει ανά πάσα στιγμή το που βρίσκεται ο χρήστης προκαλεί τεράστια ζητήματα προστασίας και ασφάλειας και δεν είναι φυσικά αποδεκτό τέτοιες πληροφορίες να διαβιβαστούν σε τρίτους χωρίς την σύμφωνη γνώμη του χρήστη. Η προστασία της τοποθεσίας δεν αφορά μόνο κινητές συσκευές όπως το κινητό τηλέφωνο αλλά και σταθερούς και παραδοσιακούς υπολογιστές. Άλλωστε όπως αναφέραμε και προηγουμένως αυτά τα δυο είναι άρρηκτα συνδεδεμένα μεταξύ τους και διαμοιράζουμε τις ίδιες ευπάθειες και ρίσκα. Για παράδειγμα από οποιαδήποτε συσκευή που χρησιμοποιεί το internet είναι δυνατή η ταυτοποίηση της τοποθεσίας του χρήστη μέσω της διεύθυνσης MAC και IP. Αυτό είναι δυνατό να συμβεί, και σε μεγαλύτερο βαθμό φυσικά, σε περιοχές όπου το δίκτυο που συνδεόμαστε είναι δημόσιο όπως μια καφετέρια ή στο αεροδρόμιο. Επιπλέον όλες οι τράπεζες διατηρούν αρχεία με τις κινήσεις και τις τοποθεσίες του κάθε πελάτη και μπορούν να εντοπίζουν τις συναλλαγές που έγιναν στα καταστήματά τους μέσω των ATM μηχανημάτων.

Η πρώτη έρευνα σχετικά για την προστασία των δεδομένων στην υπηρεσίες τοποθεσίας έγινε από τον Ian Jackson (Jackson 1998) όπου δημιούργησε ένα σύστημα όπου οι πληροφορίες που έδινε ένας χρήστης μετατρέπονταν σε ανώνυμες και δεν μπορούσες να γνωρίζεις σε ποιο ανήκαν. Πρωταρχικός σκοπός ήταν η δυνατότητα του χρήστη σε ποιον θα διαμοιράσει την προσωπικές του πληροφορίες. Το σύστημά του αποτελούσε ένα σύστημα διαμεσολαβητή που απέκρυπτε τις πληροφορίες που έστελνε ο χρήστης. Η εφαρμογή μπορούσε να λειτουργήσει όπως

ακριβώς είχε σχεδιαστεί αλλά γνώριζε μόνο την τοποθεσία και όχι την ταυτότητα του χρήστη.

Ο πιο αποτελεσματικός τρόπος για την προστασία των δεδομένων της τοποθεσίας είναι να αντιστρέψουμε την διαδικασία με την οποία λειτουργούν location-based services και το GPS. Συγκεκριμένα, αντί ο χρήστης να κάνει ένα ερώτημα στον Server σχετικά με ποια εστιατόρια, για παράδειγμα, βρίσκονται κοντά στην περιοχή του να συμβεί το αντίστροφο. Να σταλεί ένα μήνυμα σε όλους τους διαθέσιμους δέκτες που επιτρέπουν την εφαρμογή ενημέρωσης σχετικά με τα εστιατόρια.

Σε έρευνες από το Δανέζη και άλλους ερευνητές (Danezis et al., 2005;Cvrcek et al.,2006) μελετήθηκε το πρόβλημα από μια άλλη οπτική πλευρά και συγκεκριμένα πως οι χρήστες εκτιμούν τα προσωπικά τους δεδομένα και την διατήρηση αυτών. Οι έρευνες χρησιμοποιώντας τεχνικές ψυχολογίας και οικονομίας έδειξαν ότι οι χρήστες κατά μέσο όρο θα μπορούσαν να πουλήσουν τα δεδομένα τοποθεσίας του για έναν μήνα με το ποσό των 50 ευρώ.

4.2 RFID

Τα RFID (radio frequency identification) όπως αναφέραμε και σε προηγούμενο κεφάλαιο αποτελούν βασικό συστατικό της έννοιας της διάχυτης υπολογιστικής. Το πολύ χαμηλό τους κόστος σε συνάρτηση με τις δυνατότητες που παρέχουν όπως η επικοινωνία σε κοντινές αποστάσεις χρησιμοποιούνται κυρίως σε εφαρμογές όπου χρειάζεται να διαβάσουμε δεδομένα. Τα RFID είναι πλέον τόσο μικρά που χρησιμοποιούνται σε κάρτες εισόδου-εξόδου, εισιτήρια και διαβατήρια και αποτελούν τον καλύτερο τρόπο απόδειξης ότι το Ubiquitous Computing είναι ήδη γεγονός και παντού δίπλα μας.

4.2.1 Barcodes και RFID

Εκ πρώτης όψης μπορεί για κάποιους να μοιάζουν όμοια αλλά στην πραγματικότητα είναι δυο τελείως διαφορετικά πράγματα. Οι διαφορές είναι ότι ο τρόπος παρουσίασης του κωδικού είναι διαφορετικός διότι το barcode χρησιμοποιεί την κωδικοποίηση EAN ενώ το RFID τσιπάκι ανατρέχει στο δικό του κωδικό που έλαβε από τον κατασκευαστή.

Η επόμενη διαφορά είναι ότι το RFID επιτρέπει την αποστολή στοιχείων και δεδομένων. Δεν χρειάζεται κάποιο μηχάνημα να διαβάσει απευθείας τον κωδικό, γιατί οι πληροφορίες διαδίδονται ασύρματα στον δέκτη.

Καθώς όμως και οι δυο τεχνικές χρησιμοποιούνται κυρίως στην ταξινόμηση αντικειμένων και προϊόντων που είναι για πώληση, για παράδειγμα σε ένα σούπερ-μάρκετ, τα δεδομένα αυτά πρέπει να παραμείνουν προσωπικά και να μην αποθηκευτούν διότι δείχνουν τις καταναλωτικές προτιμήσεις των πελατών.

4.2.2 RFID και κίνδυνοι

Ποιοι διαθέσιμοι κίνδυνοι προκύπτουν όμως από την χρήση των RFID; Αρχικά όπως είπαμε και προηγουμένως είναι ο κίνδυνος υποκλοπής των καταναλωτικών προτιμήσεων με σκοπό την δημιουργία στοχευμένων διαφημίσεων.

Επιπλέον οι κίνδυνοι των RFID δεν αποτελούν μόνο πρόβλημα για τον χρήστη αλλά και για την ίδια την εταιρία και το κατάστημα τα οποία τα χρησιμοποιούν. Αφού λοιπόν επιτρέπουν την τιμολόγηση των αντικειμένων είναι εύκολο για κάποιον να αλλάζει θέση και να βάλει κάποιο πολύ φθηνότερο.

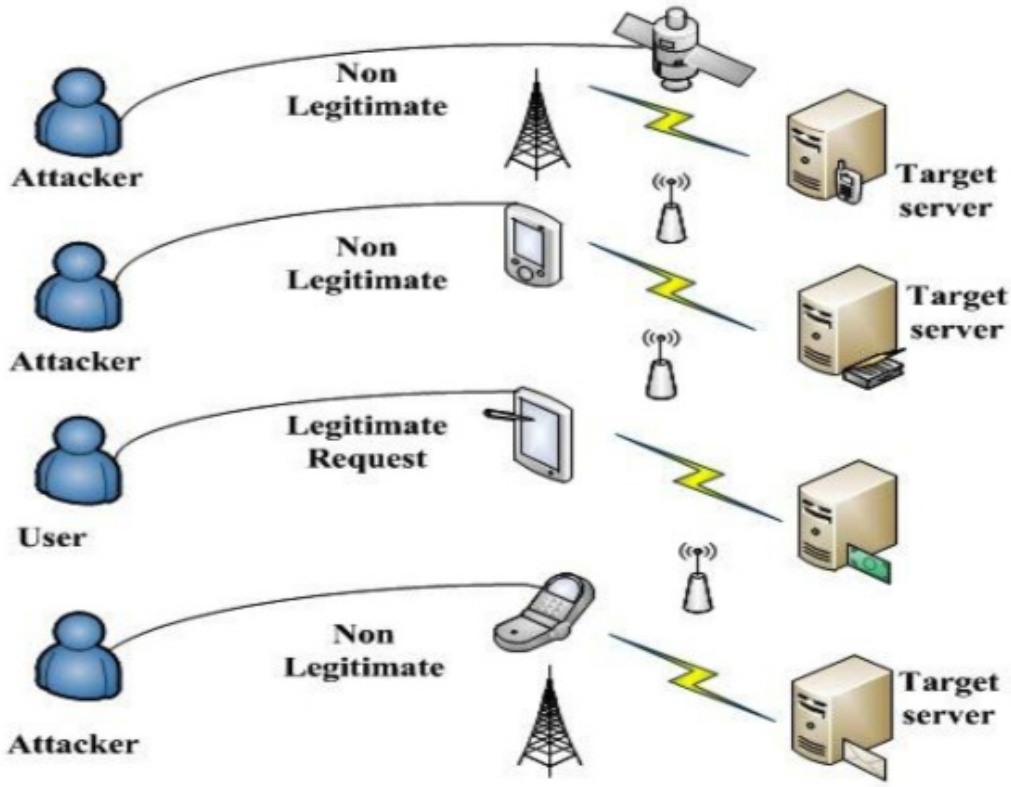
Ακόμη μπορούν να χρησιμοποιηθούν για κακόβουλη και μη εξουσιοδοτημένη πρόσβαση σε συστήματα. Ο Melanie Rieback. (Rieback et al.,2006) έδειξε ότι μπορούμε να αποθηκεύσουμε κακόβουλο κώδικα σε RFID chip και στην συνέχεια εκμεταλλευόμενος μια ευπάθεια στο σύστημα SQL να αποκτήσουμε πρόσβαση στο τερματικό.

Ένα ακόμη σημείο που πρέπει να μελετηθεί είναι κατά πόσο είναι εφικτό και εύκολο να «κλωνοποιηθεί» ένα RFID chip. Εάν συμβαίνει τότε μπορεί εκτός από οπτικά να είναι ίδιο θα μπορεί να περάσει τον έλεγχο και να μεταφέρει τα δεδομένα με τον ίδιο τρόπο όπως το πρωτότυπο;

Φυσικά στην πτυχιακή μας θα επικεντρωθούμε στους κινδύνους όπου ένα μπορεί να έχει στα σύγχρονα σπίτια. Έστω για παράδειγμα ένα έξυπνο σπίτι να διαθέτει και να επιτρέπει πρόσβαση μέσω κάρτας RFID παρόμοια με άλλα συστήματα όπως τα εισιτήρια. Ποιο θα είναι το πρωτόκολλο που θα αποφασίζει εάν είναι το σωστό άτομο που θα πρέπει να έχει πρόσβαση; Και πως θα αποτραπεί μια είσοδος σε κάποιον ο όποιος βρήκε την κάρτα και προσπαθεί να μπει παράνομα. Ο κίνδυνος είναι ο ίδιος με το παραδοσιακό κλειδί όμως με την πανταχού υπολογιστική υπάρχουν τρόποι αποτροπής που θα τα συζητήσουμε στην συνέχεια του κεφαλαίου.

4.3 Τύποι επιθέσεων

- Man-in-the-middle attack: Η πιστοποίηση των χρηστών και των εφαρμογών είναι πάρα πολύ σημαντική. Ο χρήστης πιστοποιεί ότι είναι ο νόμιμος κάτοχος με την χρήση κάποιου κωδικού ή κωδικού PIN.Η Man-in-the-middle επίθεση σκοπό έχει να ξεγελάσει τον χρήστη ώστε να υποκλέψει αυτά τα στοιχεία. Για παράδειγμα σε κάποιο ATM τερματικό μια συσκευή παρεμβάλλεται ανάμεσα στον χρήστη και την νόμιμη εφαρμογή.
- Sniffing, όπου μπορεί να υποκλαπεί κάποιο πακέτο του δικτύου, που θα μπορούσε να έχει απόρρητα δεδομένα όπως κωδικούς, οικονομικά στοιχεία κ.α.
- Παράνομη πρόσβαση στο δίκτυο, όπου εάν σε ένα δίκτυο ένας επιτιθέμενος αποκτήσει πρόσβαση στο βασικό δρομολογητή του δικτύου τότε αυτομάτως έχει πρόσβαση και σε όλο το υπόλοιπο.
- Τροποποίηση στοιχείων, που διαβάζει ο χρήστης σκοπό να τον ανακατευθύνουν σε άλλες ιστοσελίδες. Οι τεχνικές κρυπτογράφησης και αποκρυπτογράφησης μπορούν να λύσουν αυτό το πρόβλημα.
- Social Engineering, όπου ο επιτιθέμενος μπορεί να προσποιηθεί κάποιον τεχνική με σκοπό να μας εξαπατήσει και να πάρει τα προσωπικά μας στοιχεία.
- Denial of Service (DOS), και εδώ βρίσκεται η απαίτηση της προσβασιμότητας, όπου ο επιτιθέμενος μπορεί να φορτώσει το δίκτυο και το σύστημα κατά τέτοιο τρόπο ώστε να μην είναι σε θέση να διαχειριστεί κανένα αίτημα από τους χρήστες.



Εικόνα 15 - Τύποι Επιθέσεων

Σχηματικά μπορούν οι τύποι των επιθέσεων να παρουσιαστούν ως εξής.

4.4 Τρόποι προστασίας

Η ασφάλεια έχει σημαντικό ρόλο για την πανταχού υπολογιστική. Στην πραγματικότητα, προκύπτει για πολλούς ανθρώπους ως κύριο πρακτικό πρόβλημα. Σε αυτά τα είδη των περιβαλλόντων και των δικτύων, ορισμένες λύσεις για να αντιμετωπίσουν με τα πιθανά θέματα που προτείνονται (Daugman, 2004).

4.4.1 Συστήματα αποτροπής πραγματικού χρόνου.

Τα συστήματα αποτροπής πραγματικού χρόνου IDS παρόλο που διαθέτουν μια σειρά από αδυναμίες μπορούν να μας προστατεύουν στην προσπάθεια για ασφάλεια στο Ubiquitous Computing. Οι αδυναμίες αυτές έχουν να κάνουν με την παραμετροποίηση του συστήματος καθώς και με την διαχείριση των πόρων που καταναλώνει. Για να λύσουμε αυτό το πρόβλημα πρέπει να υλοποιήσουμε συστήματα με βασικό τομέα τον χρήστη (SUIDS). Τα συστήματα αυτά λειτουργούν ως εξής. Σε μακροχρόνια περίοδο και βάση οι επιλογές και προτιμήσεις του χρήστη αποθηκεύονται και παρατηρούνται. Αυτές με την σειρά τους αποτελούν κάποιο συγκεκριμένο μοντέλο χρήσης που δουλεύει ο κάθε χρήστης. Εάν κάποιος ο οποίος δεν ακολουθεί τις συγκεκριμένες διαδικασίες εμμέσως αποτελεί κάποιον που το σύστημα δεν τον αναγνωρίζει και τον αποκόπτει από το υπόλοιπο δίκτυο.

4.4.2 Πρόσβαση με βάση τον ρόλο

Τα συστήματα αυτά επιτρέπουν την πρόσβαση σε συγκεκριμένα υποσυστήματα μέσω κάποιου είδους ιεραρχίας. Ένας χάρτης κανόνων υπάρχει για τα διαθέσιμα προγράμματα και είναι ανάλογος των ρόλων που έχουν δοθεί στους χρήστες.

4.4.3 Προστασία με RFID συστήματα

Όπως συζητήσαμε και προηγουμένως τα RFID παρόλο τους περιορισμούς και τους κινδύνους που εμπεριέχουν αποτελούν έναν πολύ καλό σύμμαχο για τον τομέα της ασφάλειας. Ακόμα κι αν η τεχνολογία RFID είναι γνωστό ότι είναι κατάλληλη

για να συνδέει το φυσικό με τον εικονικό κόσμο, παρόλα αυτά υπάρχουν αρκετές προκλήσεις που πρέπει να λύσει. Αυτές οι προκλήσεις περιλαμβάνουν την ασφάλεια, την ιδιωτική ζωή, την ανάπτυξη του συστήματος, καθώς και τεχνικές προκλήσεις, όπως αποτυχίες του συστήματος και τα λάθη των δεδομένων εισόδου.

4.4.4 Βιομετρικά στοιχεία

Τα βιομετρικά στοιχεία έχουν μελετηθεί κατά κόρον στις τεχνολογικές εξελίξεις και ήδη σε πολλές εφαρμογές χρησιμοποιούνται τα δακτυλικά αποτυπώματα σαν τρόπος πρόσβασης σε συγκεκριμένες υλοποιήσεις. Ήδη κάποια κινητά τηλέφωνα και laptops διαθέτουν βασικά συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων. Άλλα βιομετρικά στοιχεία που μπορεί να αξιοποιηθούν είναι η συμμετρία του χεριού, η φωνή και η ίριδα του ματιού. Ένα αναπόφευκτο πρόβλημα είναι ότι προς το παρόν κανένα σύστημα δεν είναι τέλειο και μπορεί να έχει προβλήματα αναγνώρισης. Μπορεί είτε να κρίνει κάποιον μου θα έπρεπε να έχει πρόσβαση αρνητικά και κάποιον που δεν θα έπρεπε θετικά. Τεχνολογικά το καλύτερο σύστημα αυτή την στιγμή χρησιμοποιεί την ίριδα του ματιού και χρησιμοποιείται σε αεροδρόμια (Daugman,2004).

Το βασικό πρόβλημα με τα βιομετρικά στοιχεία είναι ότι μπορούν να αντιγραφούν μέσω πλαστικής επέμβασης. Για παράδειγμα μπορούμε να κάνουμε τα δαχτυλικά μας αποτυπώματα να είναι τα ίδια με κάποιο άλλο άτομο. Εάν υποκλαπούν αυτά τα στοιχεία σου μετά δεν μπορείς απλά να τα αλλάξεις.

Ένα δεύτερο βασικό πρόβλημα ασφαλείας που προκύπτει εάν χρησιμοποιείς τα βιομετρικά σου στοιχεία και εισέρχεσαι σε κάποιους χώρους τότε αυτά τα στοιχεία σου δείχνουν που πήγες, τι έκανες και τι προτιμήσεις έχεις κάτι που προκαλεί νέα προβλήματα στην ιδιωτικότητα του ατόμου.

Οπότε παρόλο που σωστά θεωρούμε ότι τα βιομετρικά στοιχεία είναι μοναδικά για έναν χρήστη δεν θα πρέπει να το συγχέουμε με την μυστικότητα διότι αυτά τα στοιχεία δεν μπορούν να παραμείνουν κρυφά.

4.5 Ιδιωτικότητα

4.5.1 Ορισμός

Η ευρεία γκάμα των χρήσεων του Ubiquitous Computing και των δυνατοτήτων που παρέχει σαν τεχνολογία μπορεί να δημιουργήσει παράπλευρα προβλήματα ασφαλείας. Ο λόγος που η έννοια της ασφάλειας έχει τοποθετηθεί στην πτυχιακή μας εργασία είναι διότι αποτελεί έναν πάρα πολύ σημαντικό παράγοντα και εμπόδιο που πρέπει να ξεπεράσουμε. Η δυνατότητα να έχουμε πρόσβαση από παντού μας περιορίζει κατά κάποιον τρόπο διότι δεν μπορούμε πάντοτε να γνωρίζουμε ποια διεργασία ή ποιο μέσο και από πού μας ζητάει πρόσβαση. Για αυτό τον λόγο μπορεί να είναι κάποια κακόβουλη πράξη και το δίκτυο μας να μην μπορεί να αναγνωρίσει την πραγματική προέλευση της διεργασίας αυτής.

Η ιδιωτικότητα έχει οριστεί από τον Alan Westin ως εξής : *"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].

Η αυτό-διαχείριση ενός συστήματος Ubiquitous Computing έχει σαν σκοπό την ευκολία χρήσης και διαχείρισης από τον μέσο χρήστη χωρίς να τον αποσπά από τεχνικές λεπτομέρειες για την διαχείριση του συστήματος και να του παρέχει ελευθερία κινήσεων. Όμως πιστεύουμε ότι αυτό θα οδηγήσει σε προβλήματα ασφαλείας. Και η κατάσταση επιβαρύνεται από το γεγονός ότι είναι δύσκολο να υπάρξει σωματική προστασία του συστήματος λόγω της ελεύθερης φύσης του.

4.5.2 Συζήτηση και προτάσεις

Προκειμένου για να καταστεί ένα σύστημα απανταχού υπολογιστικής περισσότερο ασφαλές προτείνουμε τις παρακάτω προτάσεις για να ληφθούν υπόψη. Προτείνουμε αντί για διαφάνεια σε όλες τις διεργασίες, να γίνει ένα προαιρετικό γνώρισμα. Μόνο εάν ο χρήστης αρχικά επιτρέψει την διαδικασία να λειτουργήσει, σε οποιαδήποτε άλλη περίπτωση όλες οι διαθέσιμες πληροφορίες θα μεταφέρονται στον χρήστη όπου αυτός θα επιτρέπει την χρήση του συστήματος.

Οι όποιες ρυθμίσεις ασφαλείας θα πρέπει να δημιουργηθούν στην αρχική φάση δημιουργίας του συστήματος ώστε να αποτρέψουν να «κληρονομηθούν» σε μετέπειτα στάδια. Προκειμένου να παραστεί μια αποτελεσματική και ευέλικτη ασφάλεια και διαχείριση ιδιωτικότητας προτείνουμε ένα πολύ-επίπεδο σύστημα ασφαλείας. Με βάση αυτό το μοντέλο κάθε μέλος του συστήματος εμπιστεύεται το λιγότερο δυνατό το άλλο και τους θεωρεί εν δυνάμει κακόβουλους χρήστες. Οποιεσδήποτε διενέξεις θα λύνονται με μηνύματα αυθεντικότητας. Το μοντέλο αυτό θα διαθέτει μηχανισμούς ιδιωτικότητας όπου θα ορίζουμε τον βαθμό των δεδομένων και προσωπικών στοιχείων που θα μπορούμε να μοιράσουμε.

Για να προσφέρει ένα σύστημα απανταχού υπολογιστικής αυτοματοποιημένες διαδικασίες και ευελιξία συγκεκριμένες ενέργειες και εξουσιοδότηση θα πρέπει να προσφέρονται από το σύστημα. Αυτό σημαίνει ότι ο χρήστης συμφωνεί ότι ένα σύνολο ενεργειών μπορεί να επιλυθεί από ένα άλλο μέλος σύμφωνα με τις προτιμήσεις του χρήστη, για παράδειγμα ο χρήστης εξουσιοδοτεί το σύστημα να κινήσει κάποιες λειτουργίες από κάποιο άλλο μέλος του συστήματος.

Επιπλέον ένας ακόμη τρόπος για την βελτίωση της ασφάλειας έχει αναφερθεί: “Κάνοντας προσωποποιημένο φιλτράρισμα από τις κινητές συσκευές επιτρέπεται η αλλαγή κατεύθυνσης πληροφορίας από το σταθερό περιβάλλον στον χρήστη αντί για την μεταφορά από τον χρήστη στο σύστημα. Αυτή η αλλαγή της πληροφορίας επιτρέπει ένα μεγάλο βήμα στην προστασία της ιδιωτικότητας με το να αποφεύγετε η πιθανότητα να συγκεντρώνονται μεγάλες ποσότητες προσωπικών δεδομένων.” (Pfitzmann,2011).

Επομένως τα παρακάτω βήματα θα επιτρέψουν την δημιουργία ενός συστήματος Ubiquitous Computing με γνώμονα την ιδιωτικότητα και τη ασφάλεια.

1. Ενσωμάτωση μηχανισμών ασφαλείας στο σύστημα ήδη στην φάση σχεδιασμού του συστήματος. Η πρόκληση εδώ είναι ο συνεπής καθορισμός των προδιαγραφών ασφαλείας και κυρίως ιδιωτικότητας, δηλαδή χρειάζεται ένα μοντέλο ασφαλείας το οποίο θα επιτρέπει την συνεχή μετατροπή σε εφαρμόσιμες απαιτήσεις.
2. Εφαρμογή της διαφάνειας σαν προαιρετικό γνώρισμα, επιτρέποντας τον διαμοιρασμό όλων των αναγκαίων τεχνικώς λεπτομερειών σχετικά με την κάθε αίτηση του χρήστη.
3. Ενίσχυση της ιδιωτικής ζωής ενός ατόμου με την αλλαγή της κατεύθυνσης πληροφορίας με την χρήση φίλτρων. Επιπλέον σε αυτό το στάδιο μπορούν να παρέχονται συμβουλές ασφάλειας και προστασίας ιδιωτικής ζωής.
4. Πολύ-επίπεδο σύστημα ασφαλείας όπου τα επιμέρους συστήματα επικοινωνούν μεταξύ τους με μηχανισμούς ελέγχου και επικύρωσης διαπιστευτηρίων.

4.5.3 Πόσο απαραίτητη είναι η ασφάλεια

Μια από τις ερωτήσεις που μπορεί να προκύψει είναι κατά πόσο είναι απαραίτητο να λάβουμε υπόψη και να διορθώσουμε ζητήματα ιδιωτικότητας και ασφάλειας στο Ubi Comp. Είναι φανερό ότι η ενσωμάτωση μηχανισμών ασφαλείας σε ένα τέτοιο σύστημα θα ανεβάσει το κόστος υλοποίησης. Αναντίλεκτα όμως είναι απαραίτητο να λύσουμε αυτά τα προβλήματα για μια σειρά από λόγους:

- Η ασφάλεια και η ιδιωτικότητα αποτελεί ένα από τα σημαντικότερα εμπόδια στον δρόμο για να αποδεχθεί η κοινωνία ένα Ubiquitous σύστημα. Ο μέσος χρήστης δεν είναι συνήθως ενήμερος με τα θέματα ασφάλειας και ενδεχομένως να διαμοιραστεί εν αγνοία του προσωπικά δεδομένα. Η συνθήκες φαίνονται πλέον όμως να αλλάζουν. Οι εταιρίες δημιουργούν συστήματα που ενσωματώνουν δικλείδες ασφαλείας που είναι πιο πιθανό να

αποκτήσουν εμπορική επιτυχία σε σχέση με άλλα που δεν έχουν επενδύσει στην ιδιωτικότητα και την ασφάλεια.

- Όταν μια δομή έχει δημιουργεί, είναι σχετικά εύκολο να ενσωματωθεί στο σύστημα. Οπότε ένα σύστημα με καλή ασφάλεια και μηχανισμούς είναι πιο εύκολο να γίνει αποδεκτό από την πλειοψηφία των χρηστών, να τοποθετηθεί πιο εύκολα και να γίνει εμπορικά επιτυχές, όπου επιπλέον προσθήκες ασφάλειες και δικλείδες ιδιωτικότητας να προστεθούν.

4.6 Ενέργειες προστασίας από την πλευρά του χρήστη

Αφού είδαμε υλοποιήσεις και βελτιώσεις σε επίπεδο σχεδιασμού τώρα ας αναφέρουμε και τις κινήσεις που θα μπορούσε να κάνει ο χρήστης για να ασφαλίσει το έξυπνο σπίτι - σύστημά του. Τι είναι αυτό που έχουν σαν κοινό στοιχείο όλα τα υπομέρους στοιχεία του συστήματος, είτε είναι κάποιος σένσορας, μία κάμερα, ένας μικρο ελεγκτής ή ένα router; Όλα ανήκουν στο ίδιο δίκτυο . Η δικτύωση μέσω Internet έχει κάνει εφικτό το Ubiquitous Computing όποτε είναι όλο και πιο αναγκαίο να θωρακίσουμε το δίκτυο. Σε ένα έξυπνο σπίτι είναι σχεδόν αδύνατο να ασφαλίσουμε μόνο μία συσκευή αλλά ένα ολοκληρωμένο σύστημα μπορεί.

4.6.1 Ασφάλιση του δικτύου μας

Βήματα για να κάνουμε το έξυπνο σπίτι μας πιο ασφαλές.

- Χρήση κωδικού στο ασύρματο δίκτυο. Το παλιό WEP (Wired Equivalent Privacy) δεν είναι επαρκές και είναι εύκολο να «σπάσει». Αντίθετα προτείνεται η χρήση WPA2 πρωτοκόλλου που διορθώνει εγγενής παθογένειες του παλιού.
- Αλλαγή ονόματος δικτύου, ή κοινώς το SSID σε κάποιο που δεν θα δίνει λεπτομέρειες στον επιτιθέμενο.
- Απενεργοποίηση πρόσβασης Guest στο δίκτυο, ώστε να γνωρίζουμε ποιος είναι συνδεδεμένος στο δίκτυο.
- Δημιουργία και δεύτερου ασύρματου δικτύου. Αρκετά router επιτρέπουν την δημιουργία πολλαπλών δικτύων. Οπότε μπορεί ο χρήστης να χρησιμοποιήσει ένα για τον υπολογιστή, το κινητό και το tablet και ένα ακόμη όπου θα είναι μόνο συνδεδεμένες οι έξυπνες συσκευές του σπιτιού.
- Αλλαγή κωδικών πρόσβασης, με μεγαλύτερη πολύπλοκότητα είναι επιβεβλημένη . Όλοι οι κωδικοί των διαχειριστών θα πρέπει να είναι κάποιος πολύπλοκος με σύμβολα και αριθμούς. Επιπλέον όπου είναι δυνατόν να γίνεται αλλαγή και του ονόματος χρήστη ώστε να είναι ακόμη πιο δύσκολες οι επιθέσεις τύπου brute-force.

- Τοποθέτηση τείχους ασφαλείας – Firewall. Ρύθμιση του Firewall ώστε να επιτρέπει κίνηση από θύρες που γνωρίζουμε.
- Εγκατάσταση συστήματος UTM (Unified Threat Management). Τα συστήματα αυτά αντίθετα από τα Firewall που είναι πρόγραμμα - software, αποτελούν hardware λύση και προτείνονται σε μεγάλα συστήματα έξυπνων σπιτιών.

4.6.2 Πέρα από το δίκτυο

Όταν θωρακίσουμε το δίκτυο στην συνέχεια θα πρέπει να εξετάσουμε κάθε συσκευή ξεχωριστά. Θα πρέπει να απενεργοποιήσουμε οποιαδήποτε απομακρυσμένη πρόσβαση εάν δεν χρησιμοποιείτε. Για παράδειγμα κάμερες και αισθητήρες μπορούν να συνδεθούν από απομακρυσμένες τοποθεσίες οπότε αυτή η δυνατότητα θα πρέπει να παραμείνει κλειστή.

Εγκατάσταση προγράμματος ασφαλείας σε όσες συσκευές είναι αυτό δυνατόν. Εάν κάποιος χάκερ αποκτήσει πρόσβαση π.χ. σε έναν έξυπνο θερμοστάτη [12] μέσω android τότε ολόκληρο το σύστημα είναι υπό κίνδυνο.

Ελέγξτε για διαθέσιμες ενημερώσεις λογισμικού σε συχνή βάση. Οι κατασκευάστριες εταιρίες συχνά διαθέτουν ενημερώσεις που λύνουν προβλήματα ασφαλείας οπότε η αναβάθμιση του firmware κρίνεται αναγκαία.

Προσέξτε τα χαρακτηριστικά των συσκευών που αγοράζετε. Εάν δεν έχει τα χαρακτηριστικά ασφαλείας που χρειαζόμαστε πάντα μπορούμε να πάμε σε άλλες συσκευές.

Η εταιρίες δείχνουν όμως ότι λαμβάνουν την ασφάλεια των έξυπνων συσκευών σοβαρά υπόψη καθώς είναι κάτι που το θέλουν και οι ίδιοι οι χρήστες. Στην έρευνα της Fortinet [11] το 40% των ερωτηθέντων απάντησαν ότι σίγουρα θα αγόραζαν ένα router που θα είναι βελτιστοποιημένο για έξυπνα σπίτια και το 47 % απάντησε πιθανόν, κάτι που δείχνει ότι η τάση για ασφάλεια στα έξυπνα σπίτια είναι δεδομένη και αυξανόμενη.

Βιβλιογραφία Κεφαλαίου

1. Danezis G, Lewis S, Anderson R (2005) *How much is location privacy worth?* In: Proceedings of Workshop on Economics of Information Security (WEIS), URLhttp://infosecon.net/workshop/pdf/location-privacy.pdf

2. Daugman J (2004) How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology 14(1), URL http://www.cl.cam.ac.uk/users/jgd1000/csvt.pdf

3. Ivan Gudymenko and Katrin Borcea-Pfitzmann. Privacy in Ubiquitous Computing. In Interconnecting Smart Objects with the Internet Workshop, Prague, March 2011.

4. Jackson IW (1998) Who goes here? confidentiality of location through anonymity. PhD thesis, University of Cambridge, URL http://www.chiark.greenend.org.uk/~ijackson/thesis/

5. Kulkarni. D., Tripathi., "Context-Aware Role-based Access Control in Pervasive Computing Systems", Dept. of Computer Science, University of Minnesota Twin Cities

6. Manuela Berg and Katrin Borcea-Ptzmann. Implementability of the Identity Management Partin Ptzmann/Hansen's Terminology for a Complex Digital World. In Simone Fischer-H ubner, Marit Hansen, Penny Duquenoy, and Ronald Leenes, editors,Proceedings of PrimeLife / IFIP Summerschool on Privacy and Identity Management for Life, IFIP Advances in Information and CommunicationTechnology. Springer, 2011.

7. Pfitzmann Andreas, "Accompanying Ambient Intelligence *(AAmI) – why* you should take *your* sensors with you". A sketch, April 2010

8. Rieback MR, Crispo B, Tanenbaum AS (2006) Is your cat infected with a computer virus? In: PERCOM '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications, IEEE Computer Society, Washington, DC, USA, pp 169–179, DOI http://dx.doi.org/10.1109/PERCOM.2006.32

9. Sharifi A, Khosravi M, Shah A. Security Attacks and Solutions On Ubiquitous Computing Networks. International Journal of Engineering and Innovative Technology (IJEIT). 2015;3(4). Available at: http://www.ijeit.com/Vol%203/Issue%204/IJEIT1412201310_07.pdf. Accessed November 22, 2015.

10. Stajano F. Security Issues In Ubiquitous Computing. 1st ed. Available at: http://www.cl.cam.ac.uk/~fms27/papers/2008-Stajano-ubiquitous.pdf. Accessed November 22, 2015.

11. Fortinet Reveals "Internet of Things: Connected Home" Survey, Available at: https://www.fortinet.com/corporate/about-us/news-events/press-releases.html?limit=30&publication-year=2014&region= Accessed 5 May 2016

12. Nest Smart Thermostat Can Be Hacked to Spy on Owners, Available at: http://www.tomsguide.com/us/nest-spying-hack,news-19290.html Accessed 5 May 2016

ΚΕΦΑΛΑΙΟ 5: ΣΕΝΑΡΙΑ ΕΞΥΠΝΩΝ ΣΠΙΤΙΩΝ

Για μεγαλύτερη ευκολία το πλάνο μας για το έξυπνο σπίτι θα χωριστεί σε δύο σενάρια. Στο πρώτο θα αναλύσουμε το σύστημα ασφαλείας και στο δεύτερο θα δούμε συστήματα που μας βοηθούν στην καθημερινότητά μας.

Στο πρώτο σενάριο θα αναπαραστήσουμε σχηματικά το μοντέλο ενός έξυπνου σπιτιού που διαθέτει ολοκληρωμένο πακέτο αποτροπής και φύλαξης από ανεπιθύμητους επισκέπτες. Διαθέτει συστήματα αισθητήρων, καμερών και άλλων στοιχείων που θα συζητηθούν αναλυτικά στην συνέχεια.

Για την αναπαράσταση χρησιμοποιήσαμε το εργαλείο Google SketchUp. Το εν λόγω πρόγραμμα είναι ένα ελεύθερο σχεδιαστικό πρόγραμμα που επιτρέπει την δημιουργία τρισδιάστατων μοντέλων. Είναι αρκετά απλό στην λειτουργία του για αυτό τον λόγο χρησιμοποιήθηκε στην πτυχιακή μας εργασία.

Το σπίτι που θα χρησιμοποιήσουμε στην σχεδίαση του έξυπνου σπιτιού για εργασία μας είναι το εξής.

Εικόνα 15 - Το μοντέλο στο Google SketchUp

Ο λόγος που επιλέχτηκε το παραπάνω μοντέλο είναι διότι θέλαμε ένα σχέδιο που να ενσωματώνει συγκεκριμένες προδιαγραφές που έχουν τα σύγχρονα σπίτια. Αυτό μας δημιουργεί επιπλέον ανάγκες που όμως αποτελούν αντιπροσωπευτικό δείγμα της σύγχρονης οικοδομικής κουλτούρας μας. Συγκεκριμένα το παραπάνω σπίτι διαθέτει πολλαπλά παράθυρα, πίσω πόρτα καθώς και δεύτερο όροφο και υπόγειο. Όλα αυτά αυξάνουν τα μέτρα που χρειάζεται να παρθούν και έχουν ληφθεί υπόψη στην σχεδίαση ενός έξυπνου σπιτιού με σκοπό την φύλαξή του.

Σενάριο 1

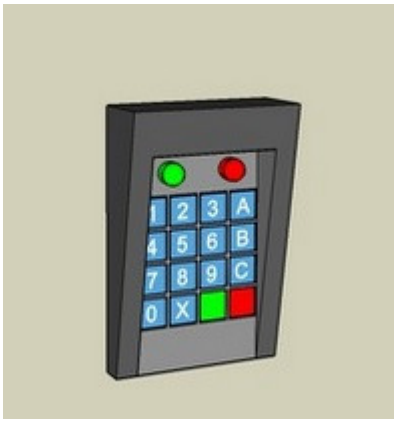
Το σενάριο αυτό περιλαμβάνει την περίπτωση που κάποιος κλέφτης έχει βάλει σαν στόχο το σπίτι μας. Οι κινήσεις του γίνονται αρχικά αντιληπτές από τους αισθητήρες κίνησης που υπάρχουν περιμετρικά του σπιτιού και στα παράθυρα. Επιπλέον υπάρχει καταγραφή των κινήσεων μέσω των καμερών IP. Η προσπάθεια να εισέλθει στο σπίτι θα είναι μάταιη διότι υπάρχει σύστημα βιομετρικής εισόδου και στην αποτυχημένη προσπάθεια η σειρήνα που βρίσκεται στον δεύτερο όροφο ενεργοποιείται μαζί με το GSM Dialer που καλεί την αστυνομία. Όμοια το ίδιο συμβαίνει εάν καταφέρει και βρεθεί στο εσωτερικό του σπιτιού.

Αρχικά θα σχεδιάσουμε το σύστημα στο εξωτερικό και στην συνέχεια θα περάσουμε και στο εσωτερικό του σπιτιού. Τα στοιχεία που θα χρησιμοποιήσουμε είναι:

- PIR αισθητήρας (Passive Infrared Sensor), ο οποίος θα χρησιμοποιηθεί σαν αισθητήρας κίνησης.

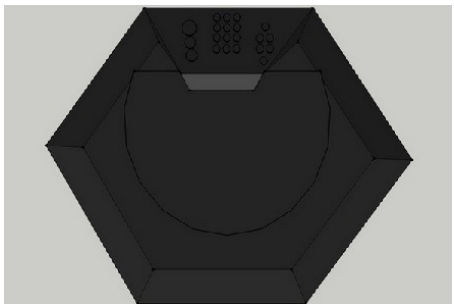
Εικόνα 16 - PIR Sensor

- Ηλεκτρονική κλειδαριά, Keypad, στην είσοδο του σπιτιού αλλά και στο πίσω μέρος.



Εικόνα 17 - Electric Keypad

- GSM Dialer, που είναι το σύστημα που μέσω δικτύου κινητής τηλεφωνίας ενημερώνει τον κάτοικο και την αστυνομία για παράνομη είσοδο στον χώρο του σπιτιού.



Εικόνα 18 - GSM Dialer

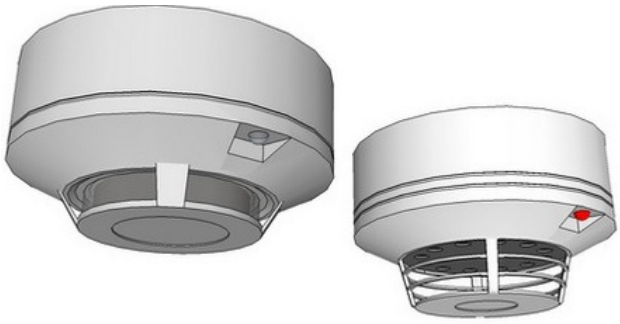
- Κάμερα παρακολούθησης, IP camera , όπου θα βρίσκεται συνδεδεμένη στο δίκτυο και μπορούμε να έχουμε πρόσβαση σε αυτή από το Internet.

Εικόνα 19 - Κάμερα παρακολούθησης

- Σειρήνα για προειδοποίηση.

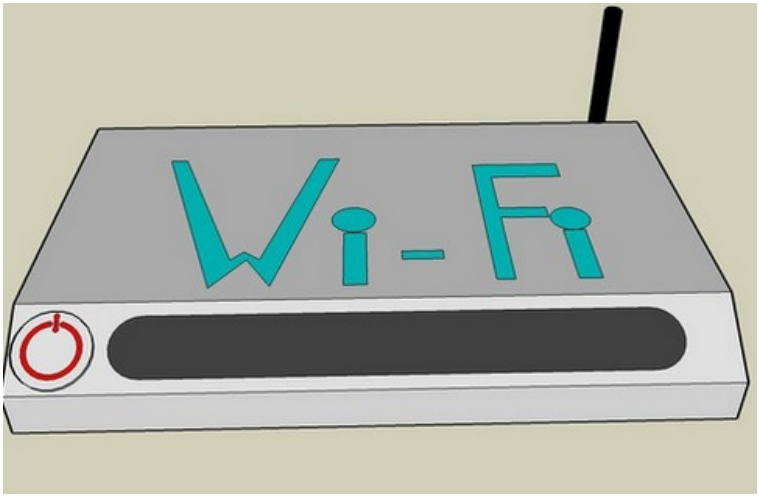
Εικόνα 20 – Σειρήνα

- Αισθητήρας φωτιάς και καπνού.



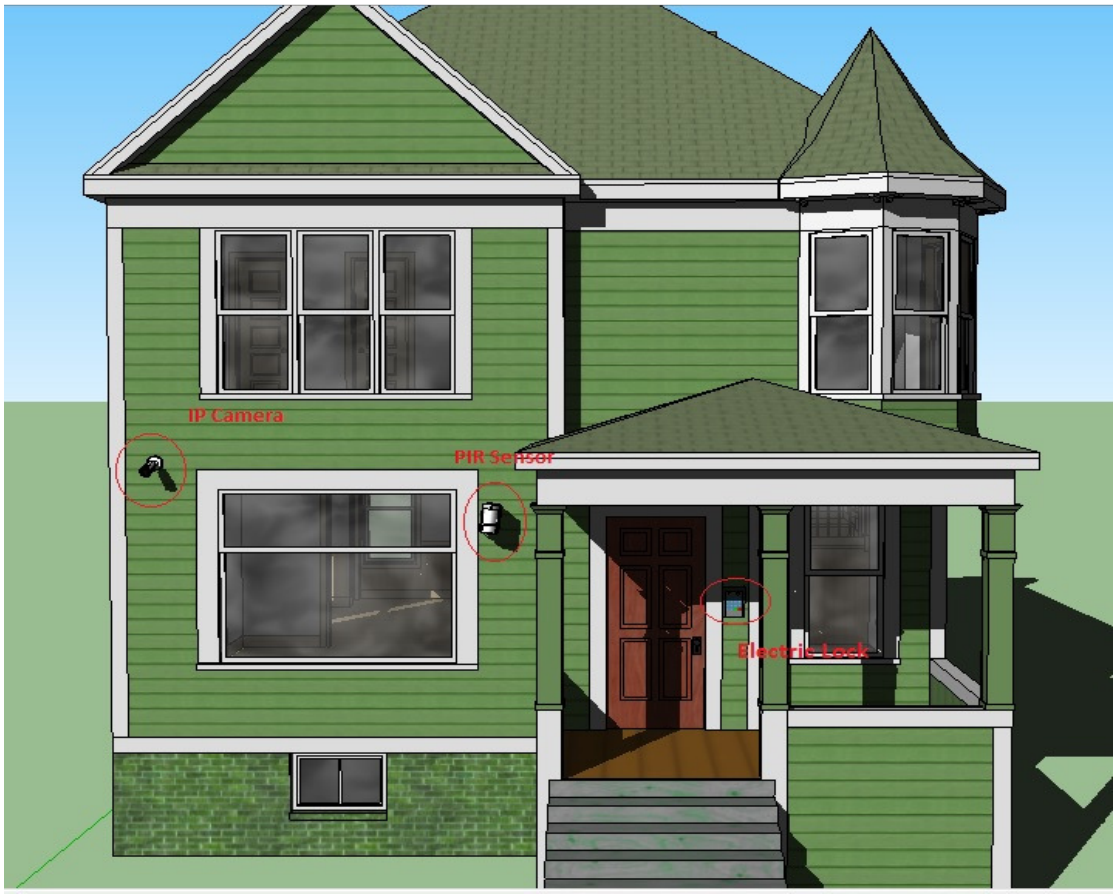
Εικόνα 21 - Smoke Detector

- Ασύρματο router



Εικόνα 22 - Router

Οπότε η σχεδίαση που ακολουθήσαμε στο εξωτερικό του σπιτιού είναι η εξής. Διακρίνονται η ηλεκτρική κλειδαριά στην είσοδο της πόρτας, αριστερά καλύπτει όλη την επιφάνεια ένας αισθητήρας κίνησης και ακόμη πιο αριστερά μια κάμερα. Όμοια υλοποίηση χρησιμοποιήθηκε και στο πίσω μέρος του σπιτιού όπου υπάρχουν τα ίδια συστήματα.



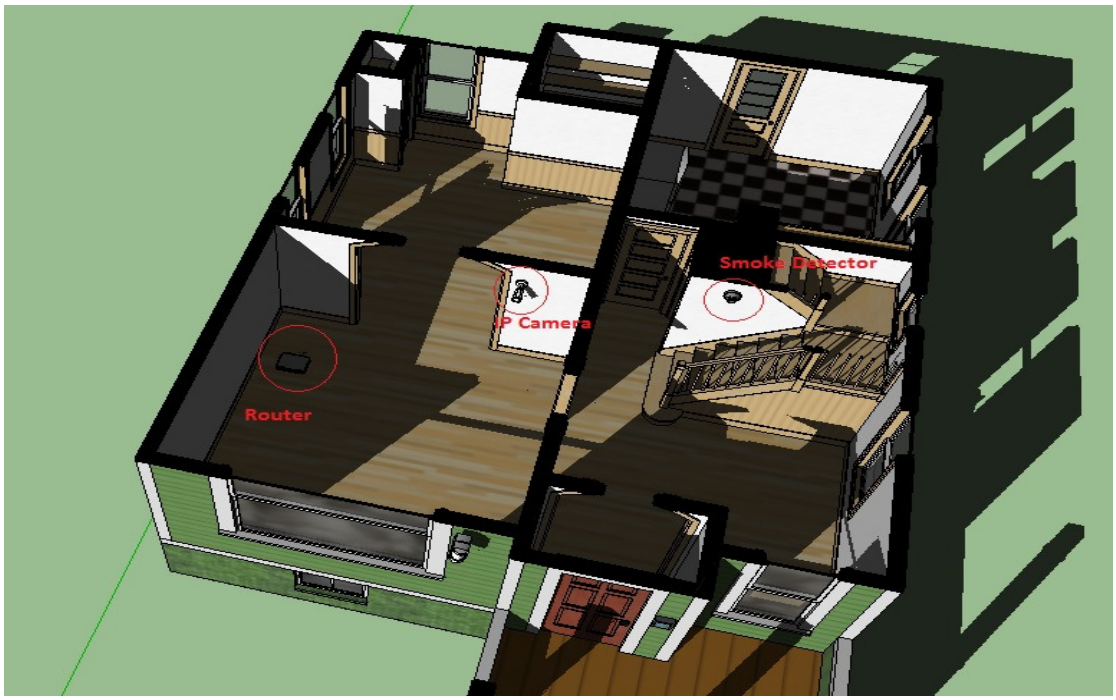
Εικόνα 23 - Είσοδος

Εικόνα 24 - Πίσω πόρτα

Και στις δυο πλευρές του σπιτιού υπάρχει από ένας αισθητήρας κίνησης. Εφόσον οι αισθητήρες καλύπτουν τουλάχιστον 10 μέτρα μόνο ένας είναι αρκετός για κάθε πλευρά.

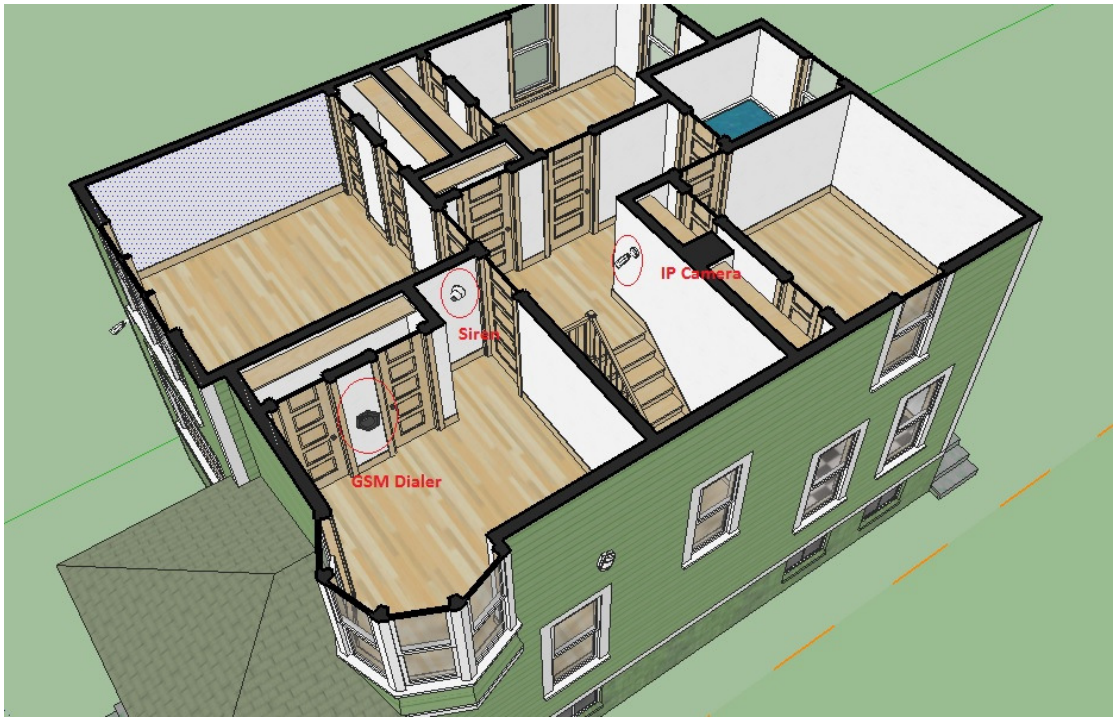
Εικόνα 25 - Πλαϊνή όψη Κτιρίου

Περνάμε στο εσωτερικό και τον πρώτο όροφο όπου τοποθετείται το ρούτερ, μια κάμερα και ο ανιχνευτής καπνού.



Εικόνα 26 - Εσωτερικό σπιτιού 1ος όροφος

Και στον δεύτερο όροφο υπάρχει τοποθετημένη μια σειρήνα συναγερμού, μια κάμερα και ο GSM Dialer.



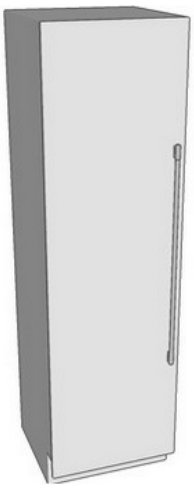
Εικόνα 27 - Εσωτερικό σπιτιού 2ος όροφος

Παρακάτω μπορείτε να δείτε το σενάριο με μορφή animation.

scenario1+text.mp4

Σενάριο 2

Στην συνέχεια θα περάσουμε στα επόμενα στοιχεία του έξυπνου σπιτιού όπως θερμοστάτες και ενεργειακή διαχείριση, αυτόματες πόρτες, έλεγχος φώτων και έξυπνες συσκευές. Το εσωτερικό του σπιτιού διαθέτει έξυπνες συσκευές όπως Smart - TV , κουζίνα και ψυγείο που συνδέονται στο ασύρματο δίκτυο του σπιτιού.



Εικόνα 28 - Smart fridge

Εικόνα 29 - Smart TV

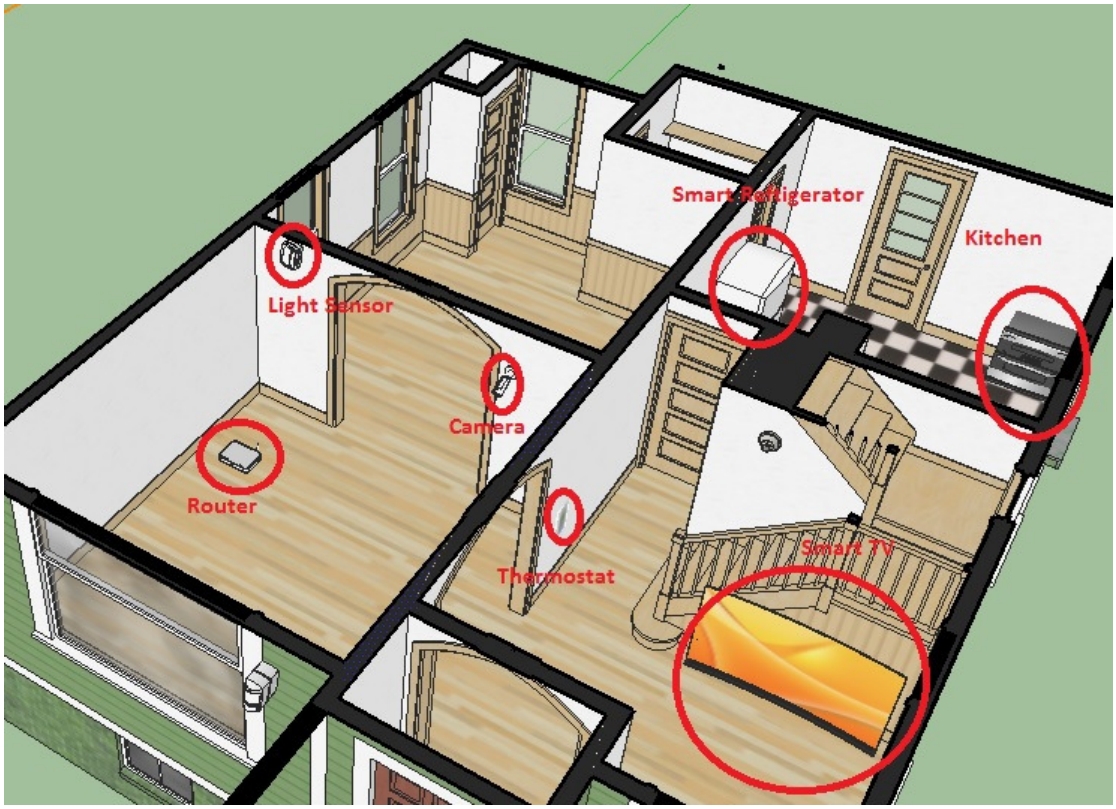
Εικόνα 30 - Kitchen Oven

Επιπλέον για την ενεργειακή κάλυψη των αναγκών του σπιτιού έχει τοποθετηθεί έξυπνος θερμοστάτης. Με σύνδεση μέσω διαδικτύου ελέγχει την θερμοκρασία και μπορούν να καθοριστούν οι επιθυμητές συνθήκες. Επιπλέον γνωρίζει πότε βρίσκεστε εντός ή εκτός σπιτιού και με βάση το πρόγραμμα καθορίζει την θερμοκρασία.

Μεταξύ άλλων λειτουργιών, ο έξυπνος θερμοστάτης, υπολογίζει πόση ώρα χρειάζεται για να ζεσταθεί το σπίτι σας, υπολογίζει για την ενέργεια που έχετε καταναλώσει και βοηθά στην εξοικονόμηση της προτείνοντας προγράμματα λειτουργίας.

Εικόνα 31 - Θερμοστάτης

Τέλος έχουν προστεθεί ανιχνευτές κίνησης που ενεργοποιούν τον φωτισμό στα επιμέρους δωμάτια. Σχηματικά το εσωτερικό του σπιτιού φαίνεται παρακάτω.



Εικόνα 32 - Εσωτερικό του σπιτιού με τα επιμέρους συστήματα.

Σενάριο 2 με την μορφή animation.

scenario2+text.mp4

Επίλογος

Οι σύγχρονες τεχνολογικές εξελίξεις είναι συνεχείς και η αδιάκοπη προσπάθεια για μια ενσωμάτωση των πάντων σε μια δομή, όπως είχε ονειρευτεί ο Mark Weiser το 1988 τείνει να γίνει πραγματικότητα. Το Ubiquitous Computing είναι στην πόρτα μας πλέον, είτε μεταφορικά είτε κυριολεκτικά. Οι υλοποιήσεις που μπορούμε να χρησιμοποιήσουμε από αυτή την τεχνολογία, ενώ παλαιότερα αποτελούσαν επιστημονική φαντασία, τώρα είναι πέρα από προφανή. Οι δυνατότητες μπορούν πλέον να είναι άπειρες και εύκολα συστήματα έχουν τοποθετηθεί στα περισσότερα σπίτια. Βέβαια θα χρειαστεί αρκετός χρόνος ακόμη να αποκτήσουμε ένα ολοκληρωμένο σύστημα αλλά ακόμη βρισκόμαστε στα πρώτα βήματα. Αφού λυθούν τα προβλήματα ασφαλείας και ιδιωτικότητας, που αποτελούν αυτή την στιγμή σοβαρό εμπόδιο, είναι σίγουρο ότι μια πλειάδα εφαρμογών και κατασκευών θα λάβει μέρος όπου το έξυπνο σπίτι θα είναι από τους πρώτους τομείς που το Ubiquitous Computing θα δείξει το τεχνολογικό μέλλον. Και είναι βέβαιο ότι το μέλλον του Ubiquitous Computing προμηνύεται λαμπρό.

Βιβλιογραφία Κεφαλαίου

1. Charles E. Bullock. Energy Savings through Thermostat Setback with Residential Heat Pumps.ASHRAE Transactions, 83(AL-78-1):352–361, 1978

2. EnergyStar.Programmable Thermostats Setpoint Times & Temperatures. http://www.energystar.gov/index.cfm?fuseaction=find_a_product.showProductGroup&pgw_code=TH, Accessed at 5 May 2016

3. Google Sketchup Tutorial Packet, Available at : http://oedk.rice.edu/Resources/Documents/FabShops%20Resources/Google%20Sketchup%20Tutorial%20Packet.pdf, Accessed at 5 Mat 2016

4. J. Lu, T. Sookoor, V. Srinivasan, G. Gao, B. Holben, J. Stankovic, E. Field,and K. Whitehouse. The smart thermostat: using occupancy sensors to save energy in homes. In Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems , SenSys '10, pages 211–224, 2010

5. SketchUp Basics, Available at : http://academics.triton.edu/faculty/fheitzman/Sketchup%20basics.pdf, Accessed at 5 May 2016