ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΑΓΙΟΥ ΝΙΚΟΛΑΟΥ

Εξυπηρέτηση πελατών μέσω Mobile app στις επιχειρήσεις.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Εισηγητής: Μανιαδή Έλενα Α.Μ.69

Επιβλέπων: Δρ. Κωνσταντίνος Παναγιωτάκης, Αναπληρωτής Καθηγητής

2016

TECHNOLOGICAL EDUCATION ISTITUTE OF CRETE

SCHOOL OF MANAGEMENT AND ECONOMICS

DEPARTMENT OF BUSINESS ADMINISTRATION (AGHIOS NIKOLAOS)

Customer service via Mobile app businesses

DIPLOMA THESIS

Student: MANIADI ELENA AM69

Supervisor : DR. PANAGIWTAKIS COSTANTINOS

2016

<u>Υπεύθυνη Δήλωση</u> *: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Διοίκησης Επιχειρήσεων του Τ.Ε.Ι. Κρήτης.*

Περίληψη

Τα τελευταία χρόνια βιώνουμε μία επανάσταση των έξυπνων κινητών τηλεφώνων (smart phones) τα οποία ενσωματώνουν πλέον δυνατότητες που δεν υπάρχουν στα συμβατικά κινητά τηλέφωνα. Τα λειτουργικά συστήματα των συσκευών αυτών ποικίλουν με το Android της Google να περιλαμβάνεται τη στιγμή αυτή στο μεγαλύτερο ποσοστό των smart phones της αγοράς. Σκοπός της παρούσας πτυχιακής εργασίας είναι η ανάπτυξη μίας εφαρμογής που προορίζεται για τα κινητά τηλέφωνα. Η εφαρμογή μπορεί να εκτελεστεί όχι μόνο σε κινητά τηλέφωνα αλλά και σε οποιαδήποτε άλλη ηλεκτρονική συσκευή που περιλαμβάνει λειτουργικό σύστημα Android (π.χ.tablet). Με την εφαρμογή, ο χρήστης θα μπορεί να έχει την πλήρη καταγραφή της τοποθεσίας του και πόση απόσταση θα χρειαστεί να διανύσει έως τον προορισμό του.

Λέξεις κλειδιά: Android, λειτουργικό σύστημα, κινητά, Smartphone, εφαρμογή.

Abstract

In recent years we experience a revolution of smart mobile phones (smart phones) which now incorporate features not found in conventional mobile phones. The operating systems of these devices vary with the Google Android include currently the largest share of the market smart phones. The purpose of this thesis is to develop an application designed for mobile phones. The application can be performed not only in mobile phones and any other electronic device that includes the Android operating system (p.ch. tablet). With the application, the user can have the complete record of the location and how far you need to go to the destination.

Keywords: android, operating system, mobile, Smartphone's, application.

Περιεχόμενα

Ευχαριστίες

Με την ολοκλήρωση της παρούσας εργασίας, θα ήθελα να ευχαριστήσω όλους εκείνους που συνέβαλαν για να έλθει εις πέρας το συγκεκριμένο ερευνητικό έργο.

Αναλυτικότερα, θέλω να ευχαριστήσω προσωπικά τον επιβλέπων καθηγητή Δρ. Παναγιωτάκη Κωνσταντίνο για την βοήθεια του κατά την διάρκεια αυτού του ταξιδιού προς τη γνώση και ταυτόχρονα, γονείς και φίλους, για την υπομονή και την υποστήριξη που έδειξαν όλους αυτούς τους μήνες.

Τέλος, θα ήθελα να ευχαριστήσω τον σύζυγο μου, Νίκο, για την ανοχή και την υπομονή που έδειξε καθώς επίσης και για την υποστήριξη σε κάθε φάση ολοκλήρωσης του παρόντος έργου.

Αντί Προλόγου

«Το να πέσεις δεν είναι και τόσο φοβερό, το να μη θέλεις να σηκωθείς είναι ολέθριο».

PAULO COELLIO

Κεφάλαιο 1. App inventor

1.1 Ετυμολογία – Ορισμός του App inventor

Τα κινητά τηλέφωνα πρώτης γενιάς σχεδιάστηκαν και αναπτύχθηκαν από τους κατασκευαστές σταθερών τηλεφωνικών συσκευών. Ο ανταγωνισμός ήταν άγριος και τα εμπορικά μυστικά φυλάσσονταν με μεγάλη προσοχή. Οι κατασκευαστές δεν ήθελαν να αποκαλύψουν τις εσωτερικές λειτουργίες των συσκευών τους, γι' αυτό και συνήθως ανέπτυσσαν οι ίδιοι το λογισμικό των τηλεφώνων τους. Οι προγραμματιστές, αν δεν συμμετείχαν σ' αυτόν τον κλειστό κύκλο, δεν είχαν καμία δυνατότητα να γράψουν εφαρμογές για τα τηλέφωνα αυτά. Τα πρώτα κινητά τηλέφωνα δεν είχαν ιδιαίτερες λειτουργίες εκτός απ' την πραγματοποίηση και λήψη κλήσεων, ακόμα μπορεί να υπήρχε μία απλή εφαρμογή επαφών που μπορούσαμε στην πραγματικότητα να χρησιμοποιήσουμε. Με τον καιρό οι πελάτες άρχισαν να απαιτούν περισσότερα χαρακτηριστικά για τα κινητά τους τηλέφωνα. Αλλά υπήρχε ένα πρόβλημα για τους κατασκευαστές τηλεφωνικών συσκευών: δεν είχαν τους απαραίτητους πόρους για την κατασκευή των εφαρμογών που επιθυμούσαν οι χρήστες. Έπρεπε να έχουν στη διάθεσή τους κάποιον τρόπο, ώστε να παρέχουν μία πύλη για υπηρεσίες ψυχαγωγίας και πληροφοριών, χωρίς να επιτρέπουν άμεση πρόσβαση στη συσκευή, και έτσι στράφηκαν στο internet.

Εικόνα 1 Ο Martin Cooper από την Motorola MotorolaDynaTAC το πρώτο κινητό τηλέφωνο.

1.2 Αρχιτεκτονική App inventor

Αν και το Android διαθέτει πολλά καινοτόμα χαρακτηριστικά, τα οποία δεν διαθέτουν άλλες πλατφόρμες κινητών τηλεφώνων, οι σχεδιαστές του εκμεταλλεύονται επίσης πολλές δοκιμασμένες προσεγγίσεις, οι οποίες λειτουργούν αποδεδειγμένα στον ασύρματο κόσμο. Πολλά απ' αυτά τα χαρακτηριστικά εμφανίζονται σε υπάρχουσες ιδιωτικές πλατφόρμες, αλλά το Android τα συνδυάζει μ' έναν ελεύθερο και ανοιχτό τρόπο, ενώ ταυτόχρονα λύνει πολλά προβλήματα που έχουν αυτές οι ανταγωνιστικές πλατφόρμες. Το Android είναι η πρώτη πλατφόρμα μίας νέας γενιάς πλατφόρμων κινητών τηλεφώνων, κάτι που χαρίζει στους προγραμματιστές του ένα συγκριτικό πλεονέκτημα. Οι σχεδιαστές του Android εξέτασαν τα πλεονεκτήματα και τα μειονεκτήματα υπαρχόντων πλατφόρμων και κατόπιν ενσωμάτωσαν τα πιο πετυχημένα χαρακτηριστικά τους. Ταυτόχρονα, οι σχεδιαστές του απέφυγαν τα λάθη του παρελθόντος. Από την κυκλοφορία του Android 1.0 SDK και μετά, η ανάπτυξη της πλατφόρμας Android έχει ακολουθήσει μία πολύ γρήγορη πορεία. Για αρκετό καιρό, εμφανιζόταν ένα νέο Android SDK κάθε δύο μήνες. Κάθε SDK συνοδευόταν από ένα όνομα έργου και στην περίπτωση του Android, τα SDK παίρνουν ονόματα γλυκών στα Αγγλικά, τα οποία ακολουθούν αλφαβητική σειρά.

1.3 Βασικά χαρακτηριστικά του App inventor

Τα βασικά χαρακτηριστικά του App inventor είναι τα εξής:

Η πρώτη έκδοση του Android SDK έγινε τον Νοέμβριο του 2007. Πολλοί παράβλεψαν και βιάστηκαν να κατακρίνουν το Android σαν ένα προβληματικό σύστημα. Στην πραγματικότητα όμως, το Android παρουσίαζε προβλήματα τα οποία παρουσιάζει οποιοδήποτε σύστημα σε τέτοια πρώιμη φάση. Το Σεπτέμβριο του 2008, η T-Mobile ανακοινώνει την διαθεσιμότητα του T-Mobile G1, του πρώτου έξυπνου τηλεφώνου (SmartPhone), βασισμένο στην πλατφόρμα του Android. Τον Μάιο του 2009 είχαμε την έκδοση Android 1.5, την ονόμασαν Cupcake, η οποία εισάγει κάποια καινούργια χαρακτηριστικά και ανανεώσεις στη επιφάνεια χρήστη (User Interface). Ικανότητα για καταγραφή και παρακολούθηση βίντεο μέσα από την λειτουργία της βιντεοκάμερας.

• Μεταφόρτωση βίντεο στο YouTube και φωτογραφιών στο Picasa απευθείας από το τηλέφωνο.

• Καινούργιο μαλακό πληκτρολόγιο (αφής) με πρόβλεψη κειμένου.

• Υ• Ικανότητα αυτόματης σύνδεσης σε μικροσυσκευή Bluetooth από μια συγκεκριμένη απόσταση.

• Καινούργια widgets και φάκελοι που μπορούν να δημοσιευτούν στην αρχική οθόνη.

• Κινούμενες μεταβάσεις οθόνης. Η έκδοση Donut ανάμεσα σε άλλες αλλαγές περιλαμβάνει:

• Βελτιωμένο Android Market.

• Ενσωματωμένη φωτογραφική μηχανή, βιντεοκάμερα και διεπαφή (interface) γκαλερί. • Η γκαλερί επιτρέπει πλέον στους χρήστες την επιλογή πολλαπλών φωτογραφιών για Διαγραφή.

• Ανανεωμένη αναζήτηση με φωνή, με ταχύτερη απόκριση και βαθύτερη ολοκλήρωση με εγγενείς (native) εφαρμογές, συμπεριλαμβανομένης της δυνατότητας να καλούμε επαφές. • Ανανεωμένη αναζήτηση με την δυνατότητα αναζήτησης σελιδοδεικτών, ιστορικού επαφών και στο διαδίκτυο από την αρχική οθόνη.

• Ανανεωμένη υποστήριξη τεχνολογιών για CDMA/EVDO, 802.1x, VPNs και με μηχανή μετατροπής κειμένου σε ομιλία (text-to-speech).

• Υποστήριξη για ανάλυση οθονών WVGA.

- Βελτιώσεις στην ταχύτητα για αναζήτηση και για εφαρμογές φωτογραφικής μηχανής
- Υποστήριξη προτύπου Bluetooth A2DP και AVRCP.

1.4 Πάροχοι Υπηρεσιών App inventor

Η δημιουργία της υπηρεσίας app inventor, δημιούργησε ταυτόχρονα επιχειρηματικές ευκαιρίες ανάπτυξης νέων υπηρεσιών όπως αυτών της αναβάθμισης των υπηρεσιών και της υποστήριξης των χρηστών από φορείς που παρέχουν τις υπηρεσίες app inventor. Όμως, η λογική που διέπει το λογισμικό εφαρμόζεται και στις υπηρεσίες app inventor όπου υπάρχουν εφαρμογές Open Source, βασισμένες σε συγκεκριμένη πλατφόρμα βοηθώντας το χρήστη να διαμορφώσει την υπηρεσία σύμφωνα με τις ανάγκες του.

Ορισμένοι από τους σημαντικότερους παρόχους υπηρεσιών app inventor είναι:

- η Amazon,
- η Google,
- η Microsoft,
- η Eucalyptus,
- η Yahoo,
- η IBM και
- η Sales force.

Η Amazon αποτελεί μία από τις μεγαλύτερες εταιρείες στον κόσμο στον τομέα του εμπορίου, αφού ξεκίνησε αρχικά ως ένα μικρό βιβλιοπωλείο και στην συνέχεια εξελίχθηκε στην πρώτη επιλογή για τους χρήστες του app inventor. Το 2006 παρουσίασε για πρώτη φορά στις Ηνωμένες Πολιτείες την υπηρεσία Amazon S3 (Simple Storage Service). Η υπηρεσία αυτή αποτελούσε μία απλή εφαρμογή αποθήκευσης η οποία διέθετε ένα αρκετά φιλικό προς το χρήση περιβάλλον εργασίας (interface). Σε πρώτη φάση, η χρέωση της υπηρεσίας γινόταν αποκλειστικά με βάση τον όγκο αποθήκευσης των δεδομένων του χρήστη και το εύρος της πληροφορίας που κατέβαζε. Σήμερα, έχει αρκετά χαμηλό κόστος ενώ μπορεί να αποθηκεύσει αντικείμενα έως 5 TB (terabytes) ακολουθούμενα από έως και 2 KB μετά-δεδομένων. (Παπαδάτος, 2011)

Ένα χρόνο αργότερα, το 2007, εγκαινιάζει για πρώτη φορά το Amazon EC2. Η εφαρμογή αυτή αποτελεί τον βασικό πυρήνα της υπηρεσίας app inventor της Amazon διαθέτοντας την τεχνική των εικονικών εξυπηρετητών η οποία ελαχιστοποιεί το χρόνο που απαιτεί η απόκτηση και εκκίνηση του εξυπηρετητή δίδοντας έτσι μεγαλύτερη ευελιξία ή/και μείωση των υπολογιστικών πόρων βασιζόμενη πάντα στις ανάγκες της εκάστοτε επιχείρησης. (Ηλιοπούλου, 2014)

Η Google, τον Ιούνιο του 2012, ανήγγειλε τη δημιουργία ενός προϊόντος IaaS, το Google Compute Engine, το οποίο χρησιμοποιεί το hypervisor, υποστηρίζοντας μόνο εικόνες που τρέχουν σε λειτουργικό σύστημα Linux. Μέσα από μία ξεκούραστη API εφαρμογή διαχείρισης πόρων, η οποία υποστηρίζεται από το λειτουργικό σύστημα Debian και συγκεκριμένα τις εκδόσεις 6.0 και 7.0, η Google, ξεκινά τη λειτουργία του Cloud Computing με ένα μόνο πόρο του δίσκου. Σημαντικό ρόλο διαθέτει ο τύπος μηχανής, ο οποίος καθορίζει αν ο πόρος ξεκινά με μηδενικό χώρο στο δίσκο ή όχι. (Σολδάτου,2013)

Λίγο καιρό μετά, εξελίσσεται και δημιουργεί το Google App Engine. Η εφαρμογή αυτή δίδει στο χρήστη τη δυνατότητα να εκτελεί εφαρμογές διαδικτύου μέσω της ηλεκτρονικής πλατφόρμας της Google. Με τον τρόπο αυτό λύνει τα χέρια των κατασκευαστών αφού εξαλείφει τα προβλήματα της εγκατάστασης, διαχείρισης, αποθήκευσης και συντήρησης μεγάλου όγκου εφαρμογών και πληροφοριών. Ακόμα πιο σημαντικό στην πλατφόρμα αυτή της Google είναι ότι δεν υπάρχει ανάγκη για διακομιστές. Ο χρήστης ανεβάζει την εφαρμογή, η οποία δίδει ταυτόχρονα πρόσβαση σε όλους τους ενδιαφερόμενους χρήστες και δεν επιτρέπει την ελεύθερη πρόσβαση. (Ηλιοπούλου, 2014)

Η Microsoft, από την άλλη, δίδει τις δικές της λύσεις στις υπηρεσίες app inventor μετατρέποντας τις βασικές καθημερινές εφαρμογές σε διαδικτυακές. Χαρακτηριστικά παραδείγματα των εφαρμογών αυτών είναι το Microsoft Office 365, Microsoft Exchange Online, Microsoft SharePoint Online, το Microsoft Office Live Meeting, το Microsoft SQL Azure και το Windows Azure. Όλες οι παραπάνω εφαρμογές χρησιμοποιούνται κυρίως από τον επιχειρηματικό κόσμο ενώ η διαδικτυακή τους έκδοση παρέχεται με ελάχιστη μηνιαία χρέωση παρέχοντας όλες τις αναβαθμίσεις και τις απαραίτητες συντηρήσεις. (Τσακανίκας, 2012)

Εκτός όμως από τις εφαρμογές με εμπορικό χαρακτήρα δημιουργήθηκαν και εφαρμογές ανοικτού κώδικα. Η Eucalyptus αποτελεί μία εφαρμογή ανοικτού κώδικα με στόχο τη δημιουργία IaaS σύννεφων. Η αρχιτεκτονική της είναι βασισμένη σε αυτή του Amazon EC2 με αποτέλεσμα οι χρήστες της Eucalyptus να χρησιμοποιούν παρόμοια εργαλεία για την είσοδο τους. Η διαφορά τους όμως είναι ότι στο Eucalyptus παρέχεται δωρεάν σύννεφο αποθήκευσης με τεχνολογία API όπου ο χρήστης μπορεί να αποθηκεύσει δεδομένα και εικόνες. (Παπαδάτος, 2011)

Μία ακόμα γνωστή εταιρεία παροχής υπηρεσιών app inventor είναι η Yahoo. Η Yahoo δημιούργησε έναν εσωτερικό χώρο αποθήκευσης app inventor ενισχύοντας αρχικά την δυναμικότητα της σκοπεύοντας μελλοντικά να γίνει μία ανοικτού κώδικα εφαρμογή cloud δίδοντας σε επιχειρήσεις και προγραμματιστές τη δυνατότητα να δημιουργήσουν το δικός τους σύννεφο. Η μηχανή app inventor βοηθάει τους χρήστες να δομούν πάνω σε virtual-machine containers, επιτρέποντας έτσι τη χρήση εφαρμογών που έχουν ήδη αποθηκευτεί. Η γλώσσα προγραμματισμού που είναι γραμμένος ο κώδικας της εφαρμογής είναι Java και C++ ενώ υποστηρίζει παράλληλα PHP και Javascript. Αξίζει να σημειωθεί ότι λίγο πριν από την αλλαγή της εφαρμογής σε ανοικτού κώδικα η Yahoo πρόκειται να αφαιρέσει μεγάλο μέρος των δυνατοτήτων που αφορούσαν αποκλειστικά τη δική της λειτουργία. (Σολδάτου, 2013)

Η IBM, γνωστή εταιρεία πληροφορικής, θέλοντας να παραμείνει ανοδική η πορεία της δημιούργησε την διαδικτυακή εφαρμογή app inventor. Χρησιμοποιώντας την τεχνολογία της IBM, οι πελάτες της αλλά και κάθε ενδιαφερόμενος μπορεί να χρησιμοποιήσει τη συγκεκριμένη εφαρμογή ως επέκταση στα κέντρα δεδομένων τους. Στόχος της δημιουργίας της εφαρμογής αυτής ήταν να παρατηρήσει τη συμπεριφορά του κοινού απέναντι σε ένα τέτοιο εγχείρημα και να το βοηθήσει να χρησιμοποιήσει νέους τρόπους αποθήκευσης πληροφοριών για την καλύτερη λειτουργία της επιχειρηματικής επικοινωνίας. (Γαρεφαλάκης, 2014)

Τέλος, ένας ακόμα πολύ γνωστός πάροχος υπηρεσιών app inventor είναι η Sales force. Η Sales force ξεκίνησε το 1999 την πορεία της ως εταιρεία που παροχής λογισμικού CRM (Customer Relationship Management) και αποτελεί μία από τις κορυφαίες εταιρείες λογισμικού σήμερα. Το 2007 η εταιρεία δημιούργησε την πλατφόρμα Force.com η οποία χρησιμοποίησε την πρωτοπορία της Sales force στην SaaS και την εισήγαγε στις υπηρεσίες cloud χαμηλών επιπέδων. Η συνεργασία των

δύο εταιρειών επέφερε την δημιουργία μίας υψηλού επιπέδου διαδικτυακής εφαρμογής η οποία δημιουργήθηκε για να τον επιχειρηματικό κόσμο φιλοξενούμενη στο cloud της Salesforce. (Γαρεφαλάκης, 2014)

1.5 Πλεονεκτήματα – Μειονεκτήματα App inventor

Όπως έχει ήδη αναφερθεί το app inventor προσφέρει μεγάλο εύρος υπηρεσιών και διευκολύνσεις στην επικοινωνία μεταξύ των διαφόρων τμημάτων ενός οργανισμού. Τα πλεονεκτήματα που απορρέουν από τη χρήση των υπηρεσιών αυτών είναι πολλά και ποικίλουν ανάλογα με την εκάστοτε πολιτική επικοινωνίας της κάθε επιχείρησης.

Τα βασικότερα πλεονεκτήματα του είναι:

(α) Εύκολο στη χρήση περιβάλλον με πολλές δυνατότητες

(β) Αντικειμενοστραφές μοντέλο οπτικού προγραμματισμού με δομές ελέγχου καθοδηγούμενες από γεγονότα (event-driven)

(γ) Μάθηση μέσω της λύσης προβλημάτων

(δ) Επιπλέον κίνητρα στους μαθητές σε σχέση με το Scratch και Alice εξαιτίας της φορητότητας και της πρακτικής χρήσης των εφαρμογών που δημιουργούνται

ε) ύπαρξη emulator που σημαίνει ότι δεν χρειάζονται πολλές συσκευές για την εισαγωγή στη σχολική τάξη (ζ) υποστήριξη από τη Google.

1.6 Μοντέλα υπηρεσίας του App inventor

Το App Inventor είναι ένα εργαλείο που βασίζεται στο διαδικτυακό μοντέλο αποθήκευσης «cloud storage», που σημαίνει ότι μπορείτε να δημιουργήσετε εφαρμογές απευθείας στο web browser σας, μέσω της υπηρεσίας που προσφέρεται στο δικτυακό τόπο http://ai2.appinventor.mit.edu. Τα αρχεία εφαρμογών αποθηκεύονται σε διαδικτυακά κέντρα αποθήκευσης data centers και δεν χρειάζεται να τ' αποθηκεύετε τοπικά στον υπολογιστή σας (μπορείτε όμως και να το κάνετε, αν θέλετε).

Απαιτήσεις συστήματος – Φυλλομετρητές

Ο Internet Explorer δεν υποστηρίζεται. Οι προτεινόμενοι φυλλομετρητές είναι Chrome 4.0 και νεότερες εκδόσεις, Firefox 3.6 και νεότερες εκδόσεις και Apple Safari 5.0 και νεότερες εκδόσεις. Ο Mozilla Firefox παρουσίασε παλαιότερα κάποιες φορές προβλήματα ανάκτησης των αποθηκευμένων αρχείων σε εφαρμογές με «μεγάλο κώδικα».

Ο Google Chrome είναι ο πιο ενδεδειγμένος για ασφαλή χρήση.

Λειτουργικά Συστήματα

Macintosh (with Intel processor): Mac OS X 10.5 και νεότερες εκδόσεις

Windows: Windows XP, Windows Vista, Windows 7

GNU/Linux: Ubuntu 8 και νεότερες εκδόσεις

Debian 5 και νεότερες εκδόσεις

Ρυθμίσεις δοκιμαστικής εκτέλεσης εφαρμογών με το App Inventor

Σύμφωνα με τις οδηγίες ρυθμίσεων υπάρχουν τρεις επιλογές δοκιμαστικής εκτέλεσης εφαρμογών με το App Inventor:

1) Android emulator: Χρήση του προγράμματος προσομοίωσης (emulator software) που τρέχει στον Η/Υ για να γίνει δοκιμή της εφαρμογής (Κάνε κλικ εδώ και κατέβασε τις οδηγίες)

2) USB: σύνδεση μιας κινητής συσκευής μέσω USB καλωδίου(Κάνε κλικ εδώ και δες τις οδηγίες)

3) Wifi: Σύνδεση μιας κινητής συσκευής μέσω WiFi (Κάνε κλικ εδώ και δες τις οδηγίες)

Βήμα 1ο: Κατεβάστε και εγκαταστήστε το MIT AI2 Companion App στο κινητό σας ή στο Tablet σας.

Βήμα 2ο: Συνδέστε το κινητό σας ή το Tablet σας και τον υπολογιστή σας στο ίδιο δίκτυο WiFi Internet.

Βήμα 3ο: Ανοίξτε την εφαρμογή που έχετε δημιουργήσει στο App Inventor και από το μενού επιλέξτε connect Al Companion.

Συνδέστε την εφαρμογή με το κινητό σας σκανάροντας τον QR code που εμφανίζεται. Προτείνουμε να ρυθμίσετε και τις τρεις επιλογές. Μερικές εφαρμογές δεν θα τρέχουν καλά με τον emulator αλλά πολλές φορές θα μας φανεί πολύ χρήσιμος. Για να ξεκινήσετε με τις ρυθμίσεις κάντε κλικ εδώ. Το περιβάλλον του App Inventor. Η επιλογή projects του μενού χρησιμοποιείται όταν θέλετε να δημιουργήσετε, να φορτώσετε, να αποθηκεύσετε, να διαγράψετε και γενικά να διαχειριστείτε τα έργα σας.

1.7 Μοντέλα Ανάπτυξης του App inventor

Προκειμένου κάποιος να δημιουργήσει ή να προσπελάσει μια δική του εφαρμογή στο AI, χρειάζεται απλά να επισκεφτεί το δικτυακό τόπο του AI, καθώς η δημιουργία και η διαχείριση των έργων (projects) γίνεται διαδικτυακά προσφέροντας μεγαλύτερη ευελιξία στον χρήστη απαλλάσσοντας τον από τοπικούς περιορισμούς αλλά προσφέροντας και ευελιξία αναφορικά με την επιλογή λειτουργικών συστημάτων και συσκευών. Σύμφωνα με το App Inventor Learning Portal (2012) το AI αποτελείται από 2 βασικά συστατικά μέρη (components) τα οποία επιτρέπουν στους χρήστες να χτίσουν τις εφαρμογές τους σειριακά (σχήμα 1): Σχεδιαστής (Designer): πρόκειται για μια ιστοσελίδα στην οποία ο χρήστης επιλέγει τα

- συστατικά μέρη για την εφαρμογή του και προσαρμόζει τις ιδιότητες του κάθε συστατικού. Συντάκτης (Blocks Editor): ουσιαστικά πρόκειται για ένα παράθυρο υλοποιήσιμο σε

- java στο οποίο ο χρήστης τοποθετεί τα κομμάτια κώδικα (program blocks) προκειμένου να «μεταφέρει» στα συστατικά μέρη του προγράμματος το πώς να «συμπεριφερθούν». Ο χρήστης πετυχαίνει τη συναρμολόγηση των δομικών στοιχείων του προγράμματος του (blocks) με οπτικό και το σημαντικότερο αρκετά απλό τρόπο. Στην πραγματικότητα πρόκειται για μια απλή τοποθέτηση κομματιών μαζί όπως όταν κάποιος συναρμολογεί ένα πάζλ. Το AI παρέχει σχεδόν σε πραγματικό χρόνο τη δυνατότητα προσαρμογής στις ενέργειες του χρήστη, με αποτέλεσμα ενώ ο χρήστης κάνει οποιαδήποτε τροποποίηση στην εφαρμογή του, να μπορεί να άμεσα παρατηρήσει την ενέργειά του στη συσκευή του ή στον προσομοιωτή του περιβάλλοντος. Η λειτουργία αυτή είναι αρκετά διαφορετική από το παραδοσιακό περιβάλλον προγραμματισμού, στο οποίο τα προγράμματα έπρεπε να μεταγλωττιστούν και να εκτελεστούν εκ νέου έπειτα από κάθε νέα τροποποίηση. Όταν ο χρήστης ολοκληρώσει την εφαρμογή του μπορεί είτε να την συσκευάσει για να παραγάγει το τελικό πρόγραμμα σε μορφή .apk (Android application package) προκειμένου να το εγκαταστήσει στην Android συσκευή του, να το αποθηκεύσει είτε ακόμη να το διανείμει δωρεάν ή εμπορικά στο δικτυακό κατάστημα της Google (Google Play). Εναλλακτικά, αν δεν υπάρχει διαθέσιμη κάποια συσκευή Android, ο χρήστης έχει τη δυνατότητα να δημιουργήσει και να ελέγξει τη λειτουργία της εφαρμογής του χρησιμοποιώντας τον προσομοιωτή Android (Android emulator)

(σχήμα 2), το οποίο αποτελεί ένα λογισμικό το οποίο τρέχει τοπικά στον υπολογιστή του χρήστη και συμπεριφέρεται ως ένα κινητό τηλέφωνο. Ουσιαστικά, αποτελεί μια πλήρη εικονική συσκευή με οθόνη αφής και επιπλέον κουμπιά τα οποία εμφανίζονται ως πλήκτρα κάτω από την «οθόνη». Το μοναδικό αρνητικό του στοιχείο είναι ότι ως προσομοιωτής είναι σχετικά αργός σε σύγκριση με μια πραγματική φορητή συσκευή. Το βασικό περιβάλλον διεπαφής (interface) του AI είναι χωρισμένο σε τέσσερα διαφορετικά πλαίσια: το Palette, που εμπεριέχει όλα τα στοιχεία που μπορεί κάποιος χρήστης να εισάγει στην εφαρμογή του χωρισμένα σε κατηγορίες, το Viewer, το οποίο ουσιαστικά αποτελεί την επιφάνεια σχεδιασμού τους, το Components, μια δενδροειδής δομή των στοιχείων που έχει χρησιμοποιήσει ο χρήστης, και το Properties, που είναι το πλαίσιο παραμετροποίησης του κάθε component. Η σχεδίαση γίνεται τμηματικά, μ' ένα απλό σύρσιμο (drag & drop) των συστατικών μερών (components) στη θέση που ο χρήστης επιθυμεί επί της οθόνης της συσκευής του. Μετά την εισαγωγή ενός στοιχείου προτείνεται η ρύθμιση των επιμέρους παραμέτρων του.

1.8 Εξυπηρέτηση Πελατών

Θέλετε να οργανώσετε την καθημερινότητά σας, ώστε να μην ξεχνάτε ραντεβού, προθεσμίες, υποχρεώσεις; Θέλετε να ταξινομήσετε και να αποθηκεύσετε τα αρχεία σας, να καταγράψετε τους πελάτες σας, να διαχειριστείτε τα project, να συνεργαστείτε και να έχετε πρόσβαση σε όλα τα δεδομένα σας από τον υπολογιστή ή το κινητό, οπουδήποτε και αν είστε; Σε όλους μας έχει συμβεί να ξεχάσουμε πού έχουμε αποθηκεύσει ένα χρήσιμο αρχείο, να χάσουμε τηλέφωνα, επαφές, αρχεία, φωτογραφίες, να ξεχάσουμε γενέθλια φίλων, να χάσουμε το κινητό μας, να χαλάσει ο υπολογιστής στο γραφείο, να ξεχάσουμε τι έχουμε υποσχεθεί σε έναν πελάτη… Όχι πια! Στις μέρες μας υπάρχουν δωρεάν εργαλεία στο cloud που θα αλλάξουν τον τρόπο που κάνετε τα πράγματα μέχρι σήμερα. Οι εφαρμογές (apps) είναι προσβάσιμες από οπουδήποτε και μέσω οποιασδήποτε συσκευής έχει πρόσβαση στο Ίντερνετ. Τα στοιχεία που ανεβάζετε είναι ασφαλή, μπορείτε να τα μοιραστείτε με όποιον θέλετε ή να τα κρατήσετε ιδιωτικά. Έχω επιλέξει τα 18 κορυφαία online εργαλεία που έχω δοκιμάσει και με έχουν βοηθήσει να καταργήσω την αποθήκευση στο σκληρό δίσκο του υπολογιστή μου ή στο flash drive, να πετάξω τις παραδοσιακές ατζέντες και ημερολόγια, καθώς και τους χειρόγραφους φακέλους των project με τα οποία ασχολούμαι. Όλες οι εφαρμογές έχουν iPhone/iPad και Android Apps, είναι δωρεάν και καλύπτουν τις ανάγκες ενός ιδιώτη, επαγγελματία ή μικρομεσαίας επιχείρησης που θέλει να οργανωθεί, να αυξήσει την παραγωγικότητα και να αποθηκεύσει όλες τις σημαντικές πληροφορίες. Ξεχάστε λοιπόν τα Post It και τα χαρτάκια που κατακλύζουν το γραφείο σας, μπείτε στο cloud!

1.9 Πως εξυπηρετούν τους πελάτες

Εμφάνιση: Μοντέρνος σχεδιασμός με ευχάριστα χρώματα. Ανταπόκριση: Άμεση εμφάνιση αποτελεσμάτων αλλά και εύκολη διαχείριση. Ευκολία: Δόθηκε μεγάλη σημασία στην ευκολία χρήσης του προγράμματος. Με ευδιάκριτα πλήκτρα αλλά και contrast εκεί που χρειάζεται χωρίς κατάχρηση. Αξιοπιστία: Δαπανήθηκαν άπειρες ώρες δοκιμών και εξετάσεων του κώδικα προκειμένου να πάρετε στα χέρια σας ένα πρόγραμμα απαλλαγμένο από κατασκευαστικά προβλήματα.

Κεφάλαιο 2. Ιστορική Εξέλιξη

2.1 Το χρονικό του App inventor

Το λειτουργικό σύστημα Android είναι ένα σύνολο προγραμμάτων για την διαχείριση της λειτουργίας smart phones. Διαιρείται σε τρία επίπεδα:

• Τον πυρήνα του

• Το Ενδιάμεσο επίπεδο

• Τις εφαρμογές.

Έχει την δυνατότητα να ανταποκρίνεται στους περιορισμένους πόρους και ενέργειας των συσκευών στις οποίες είναι εγκατεστημένο. Είναι ανοιχτού κώδικα και παράλληλα δίνει την στους προγραμματιστές να τροποποιούν τις λειτουργίες τους προσαρμόζοντάς τις στις απαιτήσεις τους. Συνοδεύεται από το Software Development Kit (SDK) το οποίο περιλαμβάνει όλα τα εργαλεία και Application Programming Interfaces (APIs) για την σχεδίαση και ανάπτυξη εφαρμογών σε γλώσσα Java και τα στοιχεία που χρειάζονται για τη λειτουργία των συσκευών που διαχειρίζονται. Είναι σχεδιασμένο να δημιουργεί κατάλληλες διεπαφές για την επικοινωνία χρήστη και συσκευής. Αναπτύχθηκε από την Android η οποία έχει εξαγοραστεί από την Google. Σκοπός του είναι η αποδοτική λειτουργία των συσκευών. Η ονομασία του προέρχεται από την Ελληνική λέξη ανδροειδές. Το λογότυπο του android Από τις πρώτες περιόδους της εμφάνισης του παρουσίασε μεγάλη διεισδυτικότητα στην αγορά και σήμερα κατέχει μεγάλο μερίδιο στην αγορά με συνέπεια να υπάρχει μεγάλο ενδιαφέρον για τις αντίστοιχες εφαρμογές οι οποίες στις περισσότερες περιπτώσεις χρησιμοποιούν υπηρεσίες της Google που προσφέρουν APIs δωρεάν.

2.2 Εξέλιξη του App inventor

Η νέα έκδοση του Android, το Android 3.0 με κωδική ονομασία “Honeycomb”, κυκλοφόρησε στις 22 Φεβρουαρίου 2011 και ήταν το πρώτο Android update μόνο για tablets. Στις σημαντικές αλλαγές και αναβαθμίσεις περιλαμβάνονται η υποστήριξη γραφικών 3D, multitasking, video chat με υποστήριξη της υπηρεσίας GTalk, βελτιωμένα animations, εντελώς νέο περιβάλλον εργασίας, εύκολη διαχείριση των εφαρμογών από τα διάφορα widgets, μεταφορά αρχείων και φακέλων με drag & drop, προσθήκη συστήματος ειδοποιήσεων και νέα υποστήριξη για Bluetooth tethering. Ακολούθησαν οι εκδόσεις 3.1 και 3.2 και τον Οκτώβριο η Google αποκάλυψε το Android 4.0 με ονομασία Ice Cream Sandwich, νέα χαρακτηριστικά και εγκωμιαστικά σχόλια. Οι πιο σημαντικές αλλαγές και χαρακτηριστικά είναι το ανασχεδιασμένο πληκτρολόγιο με voice-to-text, νέα χαρακτηριστικά στις ειδοποιήσεις, ανανεωμένος browser, ξεκλείδωμα οθόνης με αναγνώριση προσώπου, αναβαθμισμένο Gmail, προσθήκη της χειρονομίας pinch to zoom στο ημερολόγιο, η προσθήκη της εφαρμογής Data Usage για την διαχείριση των δεδομένων από/προς το διαδίκτυο, αναβάθμιση στον τρόπο διαμοιρασμού των φωτογραφιών και των βίντεο, μετονομασία της εφαρμογής Contacts σε People με νέα στοιχεία και το νέο χαρακτηριστικό Android Beam, το οποίο μεταφέρει δεδομένα μεταξύ συσκευών με NFC δυνατότητα, με ένα απλό άγγιγμα. [38] 12 Τον Μάρτιο του 2011 έγινε διαθέσιμη η 2.1.0 έκδοση του WebOS στα Pre 2 smartphones της Palm μέσω OTA (Over The Air) ενημέρωσης και στα Pre Plus μέσω USB-tethered ενημέρωσης. Το επόμενο OTA update 2.2.3 πραγματοποιήθηκε στις 28 Σεπτεμβρίου 2011 για το Pre 3 της Hewlett Packard. Ακολούθησε η 2.2.4 τον Δεκέμβριο για το Pre 2 προσθέτοντας Skype, κρυπτογράφηση DataAt-Rest και TouchPad sharing χωρίς Touchstone. Την 1η Ιουλίου 2011 η Hewlett-Packard λάνσαρε το HP TouchPad με το webOS 3.0 το οποίο πρόσφερε video chat, ασύρματη εκτύπωση (μόνο για τους εκτυπωτές της HP), ολοκληρωμένο email, ebooks, περιήγηση στον Ιστό, επεξεργασία εγγράφων, multitasking και πρόσβαση στον "HP Catalog", όπου μπορούν να κατεβαστούν επιπρόσθετες εφαρμογές. Ένα μήνα μετά δόθηκε η 3.0.2 ενημέρωση για το HP TouchPad και τον Οκτώβριο η OTA update 3.0.4 με δυνατότητα σύνδεσης τηλεφώνων χωρίς WebOS με το HP TouchPad και νέο Camera app για φωτογραφίες και βίντεο. Επίσης έδωσε υποστήριξη για αναπαραγωγή Ogg Vorbis και FLAC αρχείων. [44] Τον Αύγουστο της ίδιας χρονιάς έγινε διαθέσιμο το BlackBerry 7 OS

με τεχνολογία liquid γραφικών, Augmented Reality, NFC επικοινωνία, εγγραφή HD video, προεγκατεστημένες εφαρμογές και υπηρεσίες, ταχύτερο browser, φωνητική αναζήτηση, απάντηση κλήσεων χωρίς επαφή, βελτιώσεις στο Bluetooth και στην παρουσίαση εικόνων και την υπηρεσία αναγνώρισης BlackBerry ID. [45] Τον ίδιο μήνα η Nokia παρουσίασε επίσημα το Symbian OS 10.1 ή αλλιώς Symbian Belle, για τα τρία νέα της smartphones, Nokia 600, Nokia 700, και Nokia 701, και αργότερα μετονόμασε το Symbian Belle σε Nokia Belle. Το λειτουργικό αυτό είχε μία ολοκαίνουργια εμφάνιση με περισσότερες αρχικές οθόνες και πιο ευκρινή μενού, νέα widget, αναπτυσσόμενες ειδοποιήσεις, νέα γραμμή κατάστασης και εργαλείων, νέα εφαρμογή Χάρτες Nokia, βελτιωμένη εγγραφή βίντεο, πρόγραμμα περιήγησης στο web και άλλα. [36] Η Microsoft ξεκίνησε την διάδοση του Windows Phone 7.5 στις διεθνείς αγορές στις 27 Σεπτεμβρίου 2011. Το ανανεωμένο OS με κωδική ονομασία "Mango" είχε εκατοντάδες βελτιώσεις και νέες δυνατότητες. Κάποιες από αυτές είναι ο βελτιωμένος Mobile Internet Explorer 9 με υποστήριξη των ίδιων web standards και ικανότητας γραφικών με την desktop version, multitasking στις εφαρμογές τρίτων, ενσωμάτωση του Twitter για το People Hub, πρόσβαση στο Windows Live SkyDrive, οπτικό voicemail, φωνητικές εντολές, ενσωμάτωση συνομιλιών sms και κοινωνικών δικτύων σε μία συζήτηση, «καρφίτσωμα» των σημαντικότερων ομάδων στην οθόνη έναρξης, βελτιωμένα Live Tile και συγχρονισμός με το SkyDrive. [43] Στις 12 Οκτωβρίου 2011 κυκλοφόρησε η πέμπτη μεγάλη έκδοση του iOS, το iOS 5 και οι βασικότερες προσθήκες του ήταν το Notification Center, το οποίο αντικαθιστά το push notification system με όλα τα notifications να είναι μαζεμένα στην lock screen, το Newsstand (Κιόσκι) που επιτρέπει στους χρήστες να αγοράζουν και να ανανεώνουν ψηφιακά περιοδικά και εφημερίδες, η ενσωμάτωση του twitter απ' ευθείας στο λειτουργικό της συσκευής και άμεση πρόσβαση για tweets από παντού (Safari, Photos, Maps, Youtube κτλ), η προσθήκη tabs και των δύο νέων λειτουργιών Reader και Reading List στον Mobile Safari, η νέα To-Do list εφαρμογή Reminders, shortcut για την κάμερα, για γρήγορη πρόσβαση από την Lock Screen, χρησιμοποιώντας το κουμπί έντασης της συσκευής για τη λήψη και νέα εφαρμογή Mail με δυνατότητες rich text formatting, Indentation (tabbed text), αναζήτηση στο περιεχόμενο (και όχι μόνο στους τίτλους), Flag/unflag. Επίσης το χαρακτηριστικό PC Free που επιτρέπει ενεργοποίηση των συσκευών χωρίς σύνδεση με υπολογιστή, OTA αναβαθμίσεις λογισμικού, αναβαθμίσεις στο Game Center με προσθήκη φωτογραφιών στα προφίλ των χρηστών, προτάσεις παιχνιδιών και νέα Turn-based

games, το νέο σύστημα μηνυμάτων Message με βίντεο, φωτογραφίες, κείμενα και επαφές και η νέα υπηρεσία iCloud για αποθήκευση δεδομένων και ασύρματο συγχρονισμό αυτόματα σε όλες τις iOS και Mac συσκευές.

Κεφάλαιο 3. Ασφάλεια Δικτύων

3.1 Γενικά Στοιχεία

Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα δίκτυα υπολογιστών. Η χρήση προχωρημένων τεχνικών και τεχνολογιών, όπως οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αρκετά πλεονεκτήματα και αυξάνει τις δυνατότητες επίλυσης προβλημάτων σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Η ασφάλεια δικτύων αποτελεί αναγκαία συνθήκη και είναι απολύτως απαραίτητη συνδυαστικά με άλλες βασικές προϋποθέσεις λειτουργίας όπως η ποιότητα και η απόδοση, οι οποίες εξασφαλίζουν την εύρυθμη λειτουργία μιας επιχείρησης ή γενικότερα ενός οργανισμού. Ο λόγος της διαδεδομένης αυτής χρήσης προήλθε από τη ραγδαία εξέλιξη της τεχνολογίας και της αύξησης της χρησιμότητας της πληροφορικής με στόχο την συγκέντρωση μεγαλύτερου όγκου πληροφοριών σε λιγότερο χρονικό διάστημα.

Η έννοια τα ασφάλειας ενός δικτύου υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Επίσης, προσδιορίζεται από την ικανότητα του οργανισμού να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή βασίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων καθώς και την αδιάλειπτη λειτουργία του δικτύου.

Η ασφάλεια στα δίκτυα υπολογιστών έχει να κάνει ουσιαστικά με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου καθώς και την λήψη μέτρων. Συγκεκριμένα, η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με τα παρακάτω βήματα:

- Πρόληψη (prevention): Την λήψη δηλαδή μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών,
- Ανίχνευση (detection): Τη λήψη μέτρων για την ανίχνευση του πότε, πως και από ποιον προκλήθηκε φθορά σε μια από τις παραπάνω μονάδες και

- Αντίδραση (reaction): Τη λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου.

Η ασφάλεια δικτύων και πληροφοριών μπορεί ακόμη να οριστεί ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται και είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών.

Το πρόβλημα όμως με την ασφάλεια των δικτύων δεν σταματά εκεί. Η προστασία ενός δικτύου το οποίο συνδέεται με το Internet είναι ένα θέμα που καλούνται να αντιμετωπίσουν οι σύγχρονες επιχειρήσεις και οργανισμοί. Είναι γενικά αποδεκτό σήμερα ότι η έννοια της ασφάλειας των δικτύων υπολογιστών αλλά και των πληροφοριακών συστημάτων γενικότερα συνδέεται στενά με τρεις στενά συνδεδεμένες έννοιες:

- Διαθεσιμότητα (Availability),
- Εμπιστευτικότητα (Confidentiality) και
- Ακεραιότητα (Integrity).

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες, χωρίς αδικαιολόγητη καθυστέρηση, οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Με τον όρο διαθεσιμότητα εννοούμε ότι τα δεδομένα είναι προσβάσιμα και οι υπηρεσίες λειτουργούν παρά τις όποιες διαταραχές όπως διακοπή τροφοδοσίας, φυσικές καταστροφές, ατυχήματα ή επιθέσεις. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των υπολογιστών του δικτύου δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης όταν επιθυμούν να προσπελάσουν τους πόρους του δικτύου.

Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την αντίδραση των χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών. Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση

καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο. Η αντιμετώπιση τους αποσκοπεί στο να υπερνικήσει την σκόπιμη, που προκαλείται από κακόβουλα μέρη, παρά την τυχαία απώλεια της διαθεσιμότητας.

Παρόλο που η διαθεσιμότητα συχνά αναδεικνύεται στο πλέον σημαντικό χαρακτηριστικό της ασφάλειας, εντούτοις λίγοι μηχανισμοί υπάρχουν για να βοηθήσουν στην υποστήριξη της.

Από την άλλη, σε πολλές περιπτώσεις της καθημερινής μας ζωής οι έννοιες της ασφάλειας και της εμπιστευτικότητας σχεδόν ταυτίζονται, όπως για παράδειγμα στα στρατιωτικά περιβάλλοντα όπου η ασφάλεια έχει τη σημασία του να κρατούνται μυστικές οι πληροφορίες.

Εμπιστευτικότητα σημαίνει η πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, ο όρος αυτός δηλώνει ότι τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αλλά ακόμη και από το γεγονός ότι τα δεδομένα αυτά απλώς υπάρχουν.

Τέλος, η έννοια της ακεραιότητας αφορά την επιβεβαίωση ότι τα δεδομένα που έχουν αποσταλεί, παραληφθεί ή αποθηκευτεί είναι πλήρη και δεν έχουν υποστεί αλλοίωση. Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απάντηση ότι τα πράγματα είναι όπως πρέπει να είναι. Στην πληροφορική, η λέξη ακεραιότητα χαρακτηρίζεται ως η πρόληψη μη εξουσιοδοτημένης δημιουργίας δεδομένων. Επομένως, η μετατροπή, η διαγραφή και η δημιουργία δεδομένων ενός υπολογιστικού συστήματος, επιτρέπεται να γίνεται μόνο από εξουσιοδοτημένα μέρη. (http://utopia.duth.gr/-kdrakato/thesis/chapter.doc)

3.2 Τομείς Ασφάλειας του App inventor

Η εφαρμογές μπορεί να χρειάζεται να εκτελούν κάποιες διαδικασίες υποστήριξης στο παρασκήνιο με ή χωρίς γραφικό περιβάλλον. Το Android παρέχει δύο κλάσεις τέτοιου σκοπού (Broadcast Receiver και Service). Εάν η διαδικασία που πρέπει να εκτελεστεί είναι μικρή τότε είναι καταλληλότερη η κλάση Broadcast Receiver εάν είναι μεγάλη τότε προτιμάται η κλάση Service. Προκειμένου να μην παγώνει η εκτελούμενη εφαρμογή και οι δύο αυτές κλάσεις τρέχουν το δικό τους thread. Η κλάση Broadcast Receiver ενεργοποιείται μέσω της μεθόδου onReceive() και απενεργοποιείται μέσω της επιστροφής αυτής της μεθόδου. Το γεγονός αυτό καθιστά απαραίτητη τη χρήση σύγχρονων μεθόδων στον δέκτη. Η διαδικασία παροχής πληροφοριών συνήθως δεν είναι περιορισμένη και έτσι στέλνει δεδομένα σε όλους τους δέκτες που ταιριάζουν, μπορεί όμως να οριοθετηθεί και να παρέχει πληροφορίες σε μόνο έναν δέκτη τη φορά. Ο δέκτης μπορεί να προωθήσει το αποτέλεσμα σε έναν άλλο δέκτη ή να σταματήσει την διαδικασία παροχής πληροφοριών. Μια υπηρεσία (Service) επιτρέπει στην εφαρμογή να εκτελεί σύνθετες εργασίες στο παρασκήνιο και παρέχει μεγαλύτερη ευελιξία σε άλλες εφαρμογές του συστήματος. Μία υπηρεσία μπορεί να χρησιμοποιηθεί με δύο τρόπους, είτε να ξεκινάει με μία εντολή είτε να ξεκινάει και να ελέγχεται από μία εσωτερική σύνδεση μέσω της χρήσης της μεθόδου Remote Procedure Call. Και οι δέκτες και οι υπηρεσίες πρέπει να δηλώνονται στο αρχείο manifest της εφαρμογής ώστε να επιτρέπεται στο Android να καθορίζει τις κλάσεις Service και Receiver ακόμα και όταν δεν εκτελείτε η εφαρμογή.

3.3 Οφέλη – Κρίσιμα Σημεία Ασφαλείας

Η ασφάλεια πληροφοριακών συστημάτων, ασφάλεια υπολογιστικών συστημάτων ή ασφάλεια υπολογιστών, είναι ένα γνωστικό πεδίο της επιστήμης της πληροφορικής, και ειδικότερα του κλάδου των υπολογιστικών συστημάτων, που ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων σε αυτά τα συστήματα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση ή χρήση τους. Συγγενικά γνωστικά πεδία είναι η ψηφιακή εγκληματολογία και η εφαρμοσμένη κρυπτογραφία. Ο σχεδιασμός ασφαλών πολιτικών στα πληροφοριακά συστήματα, συνδέεται άμεσα τόσο με τεχνικές, διαδικασίες και διοικητικά μέτρα όσο και με ηθικό-κοινωνικές αντιλήψεις, αρχές και παραδοχές, προφυλάσσοντας από κάθε είδους απειλή τυχαία ή σκόπιμη. Οι διαδικασίες σχεδιασμού πολιτικών ασφαλείας, δεν θα πρέπει να παρεμβαίνουν στην απρόσκοπτη λειτουργία των πληροφοριακών συστημάτων, ενώ οφείλουν να τηρούν την αρχή της αποκέντρωσης, της ύπαρξης αντικατάστασης και την αρχή της άμυνας σε βάθος. Ως βάση μπορεί να οριστεί ο εντοπισμός, η αξιολόγηση και στη συνεχεία η διαμόρφωση ενός θεωρητικού πλαισίου για το σχεδιασμό πολιτικών σχεδιασμού ασφάλειας. Το πιο βασικό σημείο στη διαδικασία σχεδιασμού ασφαλών πολιτικών, είναι ο εντοπισμός και χαρακτηρισμός ως εμπιστευτικών των πληροφοριών που πρόκειται να χρησιμοποιηθούν και να προστατευθούν. Εκτός από τις αρχές της Ακεραιότητας Πληροφοριών, την Εμπιστευτικότητα και τη Διαθεσιμότητα Πληροφοριών οι πολιτικές ασφάλειας θα πρέπει να εμπεριέχουν και τους όρους αυθεντικότητα, εγκυρότητα, μοναδικότητα και μη αποποίηση. Ωστόσο, οι πολιτικές ασφάλειας προϋποθέτουν την ύπαρξη μίας δέσμης βασικών αρχών, εκφρασμένων με σαφήνεια η οποία να περιλαμβάνει τους σχεδιαστικούς στόχους των λειτουργικών συστημάτων. Κάθε αντικείμενο του συστήματος θα πρέπει να μπορεί να αναγνωρισθεί μονοσήμαντα και να συνοδεύεται από μία ένδειξη του βαθμού εμπιστευτικότητας. Επιπλέον, η ισχύς των ασφαλιστικών μηχανισμών δεν θα πρέπει να βασίζονται στην άγνοια των χρηστών, σχετικά με τις τεχνικές ασφαλείας οι οποίες χρησιμοποιούνται. Αλλά στην αποτελεσματική τους σχεδίαση. Στόχος ενός συστήματος πολιτικής ασφάλειας είναι ο περιορισμός επικινδυνότητας σε αποδεκτό επίπεδο. Το σύστημα περιλαμβάνει αξιολόγηση της επικινδυνότητας και περιορισμό του αποδεκτού επιπέδου ασφαλείας, ανάπτυξη και εφαρμογή μιας πολιτικής ασφαλείας καθώς και δημιουργία κατάλληλου οργανωτικού πλαισίου και εξασφάλιση των απαιτούμενων πόρων για την εφαρμογή της πολιτικής

ασφάλειας. Η πολιτική ασφάλεια μαζί με το σύνολο των μέτρων προστασίας αποτελούν το σχέδιο ασφαλείας (security plan) για τα πληροφοριακά συστήματα ενός οργανισμού διότι χρειαζόμαστε ένα ολοκληρωμένο πλαίσιο με την καθοδήγηση των μέτρων ασφαλείας να λειτουργεί ως μέσο επικοινωνίας των εμπλεκομένων στα ζητήματα ασφαλείας. Επιπλέον θεμελιώνεται η σημασία της ασφάλειας του πληροφοριακού συστήματος για τα μέλη του οργανισμού, δημιουργείται μια κουλτούρα ασφαλείας καθώς πολλές φορές αποτελεί νομική υποχρέωση και αποτελεί παράγοντα εμπιστοσύνης μεταξύ οργανισμού και πελατών. Τα είδη των πολιτικών ασφαλείας είναι α)τα τεχνικά (computer oriented) συστήματα πληροφοριών, λειτουργικά συστήματα και δίκτυα υπολογιστών β)τα οργανωτικά (human oriented) και γ)τα ατομικά (individual security policies). Περιλαμβάνει αποσπασματική διαχείριση της ασφάλειας πληροφοριακών συστημάτων και μεγάλη πολυπλοκότητα στη συντήρηση ενώ αποτελεσματική σε αυτόνομες εφαρμογές κ υπολογιστικά συστήματα που δεν συνδέονται μεταξύ τους. Σε ένα ενιαίο έγγραφο μη εύχρηστο λόγω όγκου και με πληροφορίες γενικού επιπέδου αναφέρονται όλα τα υπολογιστικά συστήματα, οι εφαρμογές και η διαδικασία του πληροφοριακού συστήματος. Τις απαιτήσεις για την ασφάλεια του πληροφοριακού συστήματος πρέπει να την ικανοποιεί η πολιτική ασφάλεια που προέρχονται από όλους τους εμπλεκόμενους στη χρήση κ στη λειτουργία του πληροφοριακού συστήματος ενός οργανισμού που είναι οι χρήστες κ οι διαχειριστές του πληροφοριακού συστήματος, η διοίκηση του οργανισμού, οι πελάτες του οργανισμού, οι νομικές και κανονιστικές διατάξεις που διέπουν την λειτουργία τους.

Ο καθορισμός της πολιτικής ασφάλειας του πληροφοριακού συστήματος θα πρέπει να καλύπτουν οι ακόλουθες κατηγορίες

1. Ζητήματα προσωπικού
2. Φυσική ασφάλεια
3. Έλεγχος πρόσβασης στο πληροφοριακό σύστημα
4. Διαχείριση υλικών και λογισμικών
5. Νομικές υποχρεώσεις

6. Διαχείριση της πολιτικής ασφάλειας
7. Οργανωτική δομή
8. Σχέδιο συνέχισης λειτουργίας
9. Όταν εφαρμόζουμε μια πολιτική ασφαλείας επιδιώκουμε:

α)οι οδηγίες και τα μέτρα προστασίας οφείλουν να καλύπτουν το σύνολο των αγαθών και όλες τις λειτουργίες(πληρότητα)

β)να λάβουμε υπόψη τις τρέχουσες τεχνολογικές εξελίξεις (επικαιρότητα)

γ)με κάποιες τροποποιήσεις ή προσθήκες να μπορεί η πολιτική να καλύπτει μικρές αλλαγές ή επεκτάσεις στο πληροφοριακό σύστημα (γενικευσιμότητα). Επιπλέον πρέπει να υπάρχει σαφήνεια κ εύκολη κατανόηση, τεχνολογική ανεξαρτησία και καταλληλότητα ανάλογα με τον οργανισμό που απευθύνεται. Για να είναι επιτυχές ένα σύστημα πολιτικής ασφάλειας οφείλει να υποστηρίζει τους επιχειρηματικούς στόχους, να συμμετέχει η διοίκηση, να είναι κατάλληλη για το περιβάλλον που εφαρμόζεται, οι χρήστες να εκπαιδεύονται κατάλληλα, να υπάρχει αξιολόγηση και η πρόσβαση να είναι εύκολη και άμεση για όλους τους χρήστες του πληροφοριακού συστήματος. Τέλος το περιεχόμενο και οι εφαρμογές πρέπει να ανανεώνονται τακτικά.

Κεφάλαιο 4. Ανάλυση Κινδύνων

4.1 Γενικά

Όπως είναι φυσικό, μία διαδικτυακή εφαρμογή εκτός από τα πολλά θετικά αποτελέσματα που προσφέρει η χρήση της, κρύβει ορισμένους πολύ σοβαρούς κινδύνους τόσο για τους παρόχους, όσο και για τους ίδιους τους χρήστες της υπηρεσίας.

Στα επόμενα κεφάλαια παρουσιάζονται αναλυτικά οι κίνδυνοι αυτοί, με σαφή και ξεκάθαρο τρόπο, μέσα από συγκεκριμένα παραδείγματα.

4.2 Ανάλυση Κινδύνων Παροχών

Η πρόσβαση στο Διαδίκτυο με οποιοδήποτε τρόπο και εάν πραγματοποιείται αυτή (dial-up, ADSL, WLAN, Κινητή Τηλεφωνία) συνδέει τον υπολογιστή ή και άλλες συσκευές (π.χ. κινητά τηλέφωνα, PDA, smartphones, κα) με το παγκόσμιο Διαδίκτυο και ως εκ τούτου τον κάνουν προσβάσιμο από όλους τους άλλους υπολογιστές που είναι επίσης διασυνδεμένοι στο δίκτυο αυτό. Για το λόγο αυτό υπάρχει επιτακτική ανάγκη να γνωρίζουμε τους κινδύνους κατά την χρήση των υπηρεσιών πρόσβασης στο Διαδίκτυο και των άλλων τηλεπικοινωνιακών υπηρεσιών που προσφέρει η Εταιρεία, έτσι ώστε να χρησιμοποιήσουμε κατάλληλα μέτρα προφύλαξης για να αποκομίσουμε το μέγιστο από την τεχνολογία αυτή, διευκολύνοντας τη ζωή μας. Όπως και με την τηλεφωνία, οποιαδήποτε χρήση ηλεκτρονικής επικοινωνίας του Διαδικτύου πραγματοποιείται μέσω διάφορων τεχνολογιών επικοινωνίας που συνδέουν τον αποστολέα με τον παραλήπτη (και αντίστροφα), είτε αυτοί βρίσκονται κοντά είτε σε αντιδιαμετρικά σημεία του κόσμου. Είναι σαφές πως η επικοινωνία αυτή μεταφέρεται από διάφορα σημεία και διαμέσου πολλαπλών τηλεπικοινωνιακών παρόχων και παρόχων υπηρεσιών, πολλές φορές σε διαφορετικές χώρες και με διαφορετικά μέσα επικοινωνίας (καλώδια χαλκού, οπτικές ίνες, ασύρματη και δορυφορική σύνδεση, κα). Η χρήση των τηλεπικοινωνιακών υπηρεσιών αποσκοπούν στην πρόσβαση στο διαδίκτυο και των υπηρεσιών του διαδικτύου όπως και η επικοινωνία μεταξύ αποστολέα και παραλήπτη. Ο τρόπος χρήσης των υπηρεσιών αυτών θα πρέπει να είναι τέτοιος, ώστε το περιεχόμενο να γνωστοποιείται μόνο εκεί που απαιτείται για να διεκπεραιωθεί η συγκεκριμένη υπηρεσία και η πραγματοποίηση της επικοινωνίας αυτής να μην εμπεριέχει κινδύνους απώλειας δεδομένων, οικονομικών στοιχείων ή άλλων μέσων που χρησιμοποιούνται κατά τη διάρκειά της. Για το λόγο αυτό θα πρέπει να λαμβάνουμε μέτρα ασφάλειας στο σπίτι μας, στις συσκευές που χρησιμοποιούμε για την επικοινωνία αυτή και στα δεδομένα (συμπεριλαμβανομένου της τηλεφωνίας) που ανταλλάσουμε.

4.3 Ανάλυση Κινδύνων Χρηστών

Εκτός από τους παρόχους των υπηρεσιών νέφους, κινδύνους και ρίσκα ασφαλείας διατρέχουν και οι ίδιοι οι χρήστες της υπηρεσίας. Οι κίνδυνοι/ ρίσκα ασφαλείας αυτοί χωρίζονται σε τέσσερις βασικές κατηγορίες:

- τα συμβόλαια ασφαλείας-ρίσκα οργανισμού,
- τα τεχνικά ρίσκα,
- τα νομικά ρίσκα και
- τα ρίσκα που δεν αφορούν αποκλειστικά τις υπηρεσίες νέφους.

4.3 Οι προοπτικές για τη βελτίωση της αποδοτικότητας και ευελιξίας καθώς και την εξοικονόμηση κόστους που ανοίγονται με την υιοθέτηση της τεχνολογίας του cloud computing σε επιχειρήσεις και Οργανισμούς, είναι πολλές και σημαντικές. Τι γίνεται όμως με το θέμα της ασφάλειας; Το Cloud Computing στις μέρες μας θεωρείται μια εξελισσόμενη τεχνολογία, η οποία σταδιακά αρχίζει να γνωρίζει μεγάλη αποδοχή στο χώρο της πληροφορικής, μιας και υπόσχεται να προσφέρει μεγαλύτερη αποδοτικότητα στον τρόπο λειτουργίας μιας εταιρείας ή Οργανισμού. Στο προηγούμενο τεύχος παρουσιάσαμε την αρχιτεκτονική του «υπολογιστικού σύννεφου», όπως συνηθίζεται πλέον να αποδίδεται στα ελληνικά, καθώς επίσης και τις λειτουργίες και εφαρμογές του. Απαντήσαμε σε όλα σχεδόν τα ερωτήματα γύρω από αυτήν την τεχνολογία, εκτός από ένα: «Τι γίνεται με το θέμα της ασφάλειας»; Σε αυτό το άρθρο λοιπόν θα παρουσιάσουμε και θα αναλύσουμε την κρίσιμη πτυχή της ασφάλειας του Cloud Computing. Οι απόψεις γύρω από το θέμα είναι αρκετές και πολλές είναι και αντιφατικές μεταξύ τους - όπως άλλωστε και σε κάθε τεχνολογία - αλλά τελικά αυτό που μετράει είναι από ποια πλευρά το βλέπουμε. Ο Prof. Whitfield Diffie του Royal Holloway University of London και πρωτοπόρος σε θέματα κρυπτογραφίας, δίνει ένα πολύ εύστοχο παράδειγμα, λέγοντας: «Όλοι κατά γενική ομολογία εμπιστευόμαστε το Gmail ή την τηλεφωνική μας εταιρεία για να στείλουμε εμπιστευτικές πληροφορίες. Θεωρούμε πως υπάρχει η απαραίτητη ασφάλεια για να μεταδώσουμε μία εμπιστευτική πληροφορία τηλεφωνικά και εμπιστευόμαστε τον πάροχό μας. Υπάρχει όμως και μία μερίδα ανθρώπων που δεν μιλάνε στο τηλέφωνο αν δεν πάρουν περισσότερα μέτρα ασφαλείας - πέρα από αυτά που παρέχονται από τις εταιρείες τηλεφωνίας». Στο κείμενο που ακολουθεί θα εστιάσουμε στους

κινδύνους που συνοδεύουν την τεχνολογία και τις υπηρεσίες του cloud computing, θα παρουσιάσουμε τα πλεονεκτήματα που προκύπτουν και θα δούμε τι ρίσκα παίρνουμε υιοθετώντας αυτήν την τεχνολογία. Τέλος, θα κάνουμε μία αναφορά σε γεγονότα τα οποία έχουν λάβει χώρα, ώστε να κατανοήσουμε την αιτία κάποιων προβλημάτων και θα κλείσουμε με τον απολογισμό όλων των στοιχείων του άρθρου αυτού. Ποιοι κίνδυνοι ελλοχεύουν στο «σύννεφο» Μέσα στο «σύννεφο» λοιπόν, οι μεγαλύτεροι κίνδυνοι σε θέματα ασφάλειας εντοπίζονται στα εξής σημεία: Η παροχή υπηρεσίας του «σύννεφου» χρησιμοποιεί την υποδομή του πάροχου. Ουσιαστικά δηλαδή, ο χρήστης παραχωρεί κομμάτι του ελέγχου στον πάροχο. Την ίδια στιγμή, η συμφωνία σε επίπεδο υπηρεσιών μεταξύ πελάτη-πάροχου (SLA) δεν διασαφηνίζει αυτό το θέμα, αφήνοντας ερωτηματικά και κενά σε επίπεδα ασφάλειας. Τι θα μπορούσε αλήθεια να συμβεί αν χανόταν ο έλεγχος από τον πάροχο; Αυτή τη στιγμή τα εργαλεία που προσφέρονται, οι διαδικασίες, το πρότυπο τυποποιημένης μορφής και οι υπηρεσίες που μπορούν να παρέχουν ασφάλεια δεδομένων, φορητότητα και μετάβαση σε άλλο πάροχο, δεν μπορούν να θεωρηθούν ότι έχουν φτάσει σε ένα υψηλό επίπεδο. Με λίγα λόγια, αν θέλετε να αλλάξετε πάροχο υπηρεσιών «σύννεφου» έχετε δύο προβλήματα. Το ένα είναι ότι υπάρχει δυσκολία στη μεταφορά αρχείων και υπηρεσιών, ενώ ακόμα πιο δύσκολα γίνονται τα πράγματα αν θα θέλαμε να γυρίσουμε στην κλασική λύση με server και clients εντός της επιχείρησης. Εάν η φορητότητα των δεδομένων δεν είναι εφικτή, δεν γίνεται να γυρίσουμε πίσω στον παλιό κλασικό server. Σε αυτό το σημείο μάλιστα, τίθεται και θέμα εξάρτησης από τον πάροχο. Η κοινή διαχείριση αρχείων και πόρων που προσφέρει το «σύννεφο» έχει ένα μειονέκτημα σε σχέση με τη multi-tenant αρχιτεκτονική. Για να καταλάβουμε τον όρο multi-tenant, με απλά λόγια φανταστείτε το δίκτυο σαν μια πολυκατοικία. Όλοι μπορούν να έχουν κοινή χρήση του ανελκυστήρα και μόνο ο διαχειριστής έχει πρόσβαση στο μηχανοστάσιο. Το πρόβλημα στη συγκεκριμένη περίπτωση είναι πώς διασφαλίζεται το δίκτυο από τους ενοίκους, συνολικά και ατομικά. Για παράδειγμα, το διαμέρισμα Α του 2ου ορόφου με το Β συγκοινωνούν με κοινή - ας πούμε - εσωτερική πόρτα. Έρχεται ο κλέφτης να μπει στο Α, αλλά η πόρτα ασφαλείας του διαμερίσματος είναι αδιαπέραστη και θωρακισμένη. Πάει λοιπόν στο Β, στο οποίο η πόρτα είναι κλασική και ξεκλείδωτη. Με την ταυτότητα και μόνο ανοίγει, μπαίνει εύκολα και το χειρότερο είναι ότι αποκτάει πρόσβαση και στο διαμέρισμα Α. Θεωρητικά, μόλις καταλάβατε πώς θα μπορούσε να επιτευχθεί μία επίθεση τύπου guest-hopping. Βάλτε στο μυαλό σας εικονικές μηχανές (διαμερίσματα) και τον επόπτη τους (hypervisor ή virtual machine

monitor). Στην πραγματικότητα βέβαια, ο βαθμός δυσκολίας μιας τέτοιας επίθεσης είναι μεγάλος σε σχέση με τις κλασικές επιθέσεις στο παραδοσιακό λειτουργικό. Επειδή ασφάλεια δεν είναι μόνο το τεχνικό επίπεδο και ο κώδικας ενός υπολογιστή, ένας κίνδυνος που αφορά στις επιχειρήσεις είναι και ο παρακάτω. Μία επένδυση που χρειάζεται απόλυτη συμμόρφωση με συγκεκριμένους όρους για την εκπόνησή της, ίσως να μην είναι καλή ιδέα να εμπλακεί με το «σύννεφο». Ειδικά στην περίπτωση όπου ο πάροχος δεν δίνει αποδεικτικό ότι η υπηρεσία θα δουλεύει σύμφωνα με τις απαιτήσεις. Μεγάλη προσοχή λοιπόν χρειάζεται σε θέματα που αφορούν σε κανονιστικά πλαίσια και πρότυπα λειτουργίας. Το «σύννεφο» προσφέρει πρόσβαση μέσω παγκόσμιου ιστού και κοινόχρηστων δικτύων. Είναι ευνόητο πως υπάρχει ένα αυξημένο ρίσκο στην ασφάλεια, ειδικά όταν συνδυάζεται και με απομακρυσμένη σύνδεση. Πόσο σίγουροι είμαστε ότι τα δεδομένα μας είναι ασφαλή; Πόσο κατοχυρωμένοι είμαστε ότι δεν θα χαθεί ένα σημαντικό αρχείο; Είναι γνωστό ότι τα αρχεία μας στο «σύννεφο» ταξιδεύουν μεταξύ δικτύων ανά τον κόσμο. Η ερώτηση είναι, ποιος τα ελέγχει; Και, αν κάποιος ελέγχει πού θα πάνε, τα διαχειρίζεται με σωστό και νόμιμο τρόπο; Γενικά, είναι απαραίτητο να γνωρίζουμε την πολιτική του πάροχου. Κάποιοι παρέχουν μάλιστα και πιστοποιητικά. Στο θέμα των αρχείων, ένας κίνδυνος εμφανίζεται κατά τη διαγραφή τους. Στην πραγματικότητα, αν θέλαμε να σβήσουμε τα πάντα από το δίσκο υπάρχουν άπειρες τεχνικές. Από ένα απλό delete έως και πιο σύνθετες, που κάνουν δυσκολότερη έως αδύνατη την ανάκτηση των δεδομένων. Στο «σύννεφο» όμως, δεν θα μπορούσαμε να κάνουμε κάτι τέτοιο. Μην ξεχνάτε ότι μοιραζόμαστε το δίσκο και με άλλους πελάτες και ότι στην πραγματικότητα το σβήσιμο δεν γίνεται πάντα σε πραγματικό χρόνο..1 Συμβόλαια Ασφαλείας – Ρίσκα Οργανισμού

4.3.2 Τεχνικά Ρίσκα

Η πολλαπλή-μίσθωση και οι μοιραζόμενοι πόροι είναι αυτά που ορίζουν τα χαρακτηριστικά του cloud computing. Αυτή η κατηγορία κινδύνου καλύπτει την αποτυχία των μηχανισμών να διαχωρίζει την αποθήκευση, τη μνήμη, τη δρομολόγηση και ακόμη και την φήμη μεταξύ των διαφόρων ενοικιαστών (π.χ., οι αποκαλούμενες quest- hopping επιθέσεις). Ωστόσο, θα πρέπει να ληφθεί υπόψη ότι οι επιθέσεις στους μηχανισμούς της απομόνωσης των πόρων(π.χ. ενάντια hypervisors) εξακολουθούν να είναι λιγότεροι σε αριθμό και πολύ πιο δύσκολο για έναν εισβολέα να θέσει σε εφαρμογή σε σχέση με τις επιθέσεις στα παραδοσιακά λειτουργικά συστήματα. Οι κακόβουλες δραστηριότητες εκ των έσω θα μπορούσε να έχει αντίκτυπο: στην εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα όλων των ειδών των δεδομένων, IP, όλα τα είδη των υπηρεσιών και ως εκ τούτου έμμεσα στη φήμη του οργανισμού και στην εμπιστοσύνη των πελατών. Αυτό μπορεί να θεωρηθεί ιδιαίτερα σημαντικό στην περίπτωση του cloud computing, λόγω του γεγονότος ότι οι αρχιτεκτονικές του cloud απαιτούν συγκεκριμένους ρόλους που είναι εξαιρετικά υψηλού κινδύνου. Παραδείγματα τέτοιων ρόλων περιλαμβάνουν τους Cloud Provider διαχειριστές του συστήματος και των ελεγκτών καθώς και τους διαχειριστές υπηρεσιών ασφαλείας που ασχολούνται με τις αναφορές ανίχνευσης εισβολής και την αντιμετώπιση τους. Καθώς αυξάνεται η χρήση του cloud, οι εργαζόμενοι των παροχών cloud γίνονται όλο και περισσότερο στόχοι από κακόβουλες ομάδες με σκοπό να υποκλέψουν πληροφορίες για τους πελάτες των παροχών cloud που εργάζονται.

4.3.3 Νομικά Ρίσκα

Προστασία των δεδομένων δημιουργεί πολλούς κινδύνους στην προστασία των δεδομένων για τους πελάτες του cloud και τους παρόχους του. Σε ορισμένες περιπτώσεις, μπορεί να είναι δύσκολο για τον πελάτη του cloud(στο ρόλο του ως υπεύθυνος της διαχείρισης των δεδομένων)να ελέγχει αποτελεσματικά τις πρακτικές διαχείρισης των δεδομένων που εφαρμόζει ο πάροχος του cloud και επομένως να μην είναι σίγουρος ότι τα δεδομένα διαχειρίζονται με νόμιμο τρόπο. Αυτό το πρόβλημα επιδεινώνεται σε περιπτώσεις πολλαπλής διαβιβάσεις δεδομένων π.χ. μεταξύ συνδεόμενων cloud. Από την άλλη πλευρά, ορισμένοι πάροχοι cloud παρέχουν πληροφορίες σχετικά με τις πρακτικές επεξεργασίας των δεδομένων τους. Κάποιοι επίσης προσφέρουν περιλήψεις σχετικά με την πιστοποίηση που ακολουθούν για την επεξεργασία των δεδομένων τους και τις δραστηριότητες ασφάλειας και τους ελέγχους των δεδομένων που διαθέτουν π.χ.SAS70 πιστοποίηση. Μπορεί να υπάρχουν στοιχεία παραβίασης της ασφάλειας τα οποία δεν κοινοποιούνται στον υπεύθυνο διαχείρισης από τον πάροχο του cloud. Ο πελάτης του cloud μπορεί να χάσει τον έλεγχο των δεδομένων του που υφίστανται επεξεργασία από τον πάροχο του cloud. Το πρόβλημα αυτό αυξάνεται σε περίπτωση που υπάρχει πολλαπλή μεταβίβαση δεδομένων (π.χ. μεταξύ συνενωμένων παρόχων cloud). Ο πάροχος του cloud (ο υπεύθυνος διαχείρισης) μπορεί να λάβει δεδομένα που δεν έχουν νομίμως συλλεχθεί από τους πελάτες τους.

4.3.4 Ρίσκα που δεν αφορούν τις υπηρεσίες App inventor(cloud)

Κατά τη διάρκεια της ανάλυσης των κινδύνων, εντοπίσαμε τις παρακάτω απειλές οι οποίες δεν αφορούν ειδικά το cloud computing, αλλά θα πρέπει ωστόσο να εξεταστούν προσεκτικά κατά την εκτίμηση του κινδύνου ενός τυπικού cloud-based συστήματος. Network breaks (διακοπές δικτυού):Ένας από τους υψηλότερους κινδύνους.¬ Δυνητικά επηρεάζονται χιλιάδες πελάτες ταυτόχρονα Network management(διαχείριση του δικτυού):Προβλήματα που μπορούν να¬ δημιουργηθούν κατά την διαχείριση του δικτυού είναι να υπάρχει συμφόρηση στο δίκτυο, έλλειψη σύνδεσης και μη βέλτιστη χρήση του. Modifying network traffic: τροποποίησης της κίνησης στο δίκτυο.¬ Social engineering attacks: Οι επιθέσεις τύπου social engineering¬ θεωρούνται συνήθως αυτές όπου υπάρχει χειρισμός των ανθρώπων που εκτελούν ενέργειες ή κατέχουν εμπιστευτικές πληροφορίες. Αν και είναι παρόμοιο με ένα τέχνασμα εμπιστοσύνης ή απλά μιας απάτης, ο όρος συνήθως απάτη ή εξαπάτηση ισχύει για το σκοπό της συλλογής πληροφοριών η' την πρόσβασης στο σύστημα και στις περισσότερες περιπτώσεις ο εισβολέας χρησιμοποιεί τα στοιχειά του νόμιμου διαχειριστή του συστήματος(πλαστοπροσωπία). Unauthorized access to premise: (περιλαμβάνει αναρμόδια πρόσβαση στις¬ εγκαταστάσεις, συμπεριλαμβανομένων τις φυσικής πρόσβασης στα μηχανήματα και σε άλλες περιοχές).Δεδομένου ότι οι πάροχοι cloud Ασφάλεια σε συστήματα cloud computing και υλοποίηση τεχνικών ασφαλείας 31 συγκεντρώνουν τους πόρους σε μεγάλα κέντρα δεδομένων, και δεδομένου ότι ο φυσικός περιμετρικός έλεγχος είναι πιθανόν πιο ισχυρός, ο αντίκτυπος της παραβίασης των ελέγχων αυτών είναι υψηλότερος. Να σημειωθεί ότι οι κίνδυνοι που αναφέρονται παραπάνω δεν ακολουθούν μια συγκεκριμένη σειρά της κρισιμότητας. Είναι από τους δώδεκα πιο σημαντικούς κινδύνους που αντιμετωπίζει το cloud computing κατά τη διάρκεια της αξιολόγησης του. Οι κίνδυνοι από τη χρήση του cloud computing θα πρέπει να συγκριθούν με τους κινδύνους της παραμονής σε παραδοσιακές λύσεις. Επίσης είναι συχνά δυνατό, και σε ορισμένες περιπτώσεις ενδείκνυται, για τον πελάτη cloud τη μεταφορά των κινδύνων στον πάροχο του cloud. Όμως δεν μπορούν όλοι οι κίνδυνοι να μεταφερθούν: Εάν υπάρξει κίνδυνος ο οποίος οδηγεί στην αποτυχία μιας επιχείρησης, σοβαρή ζημιά στη φήμη ή νομικές συνέπειες, είναι δύσκολο ή αδύνατο για την αποζημίωση για τη ζημία αυτή.

ΚΕΦΑΛΑΙΟ 5

ΑΝΑΠΤΥΞΗ ΕΦΑΡΜΟΓΗΣ GPS

5.1. Εισαγωγή

Η εφαρμογή χρησιμεύει στις επιχειρήσεις ξενοδοχείων όπου δέχονται τουρίστες και ζητούν την ακριβή ώρα που θα καταφθάνουν στο ξενοδοχείο τους από την ώρα που θα φτάσουν στο αεροδρόμιο ή στο λιμάνι να γνωρίζουν από την ώρα που φθάνουν σε πόση ώρα θα φτάσουν στο ξενοδοχείο τους.

5.2 Δημιουργία

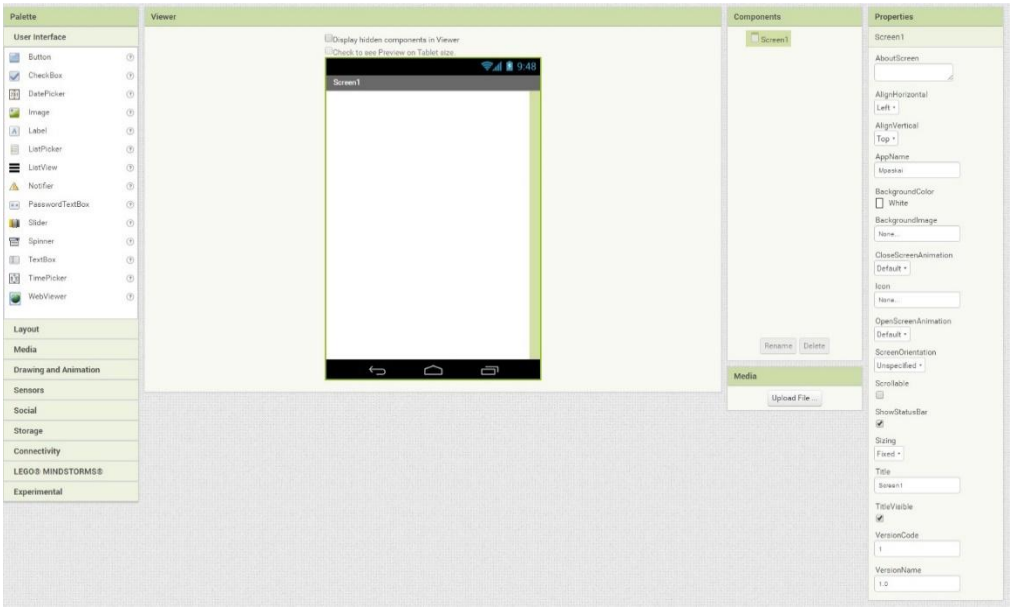
Για την δημιουργία της εφαρμογής θα χρειαστούμε την εφαρμογή MIT App Inventor 2. Την βρίσκει κάποιος εδώ. Το MIT App Inventor είναι ένα online πρόγραμμα δωρεάν και δουλεύει με Emulator ή με την συσκευή σας. Προσοχή μόνο Android.

5.3. Τι είναι το Android;

Τα τελευταία χρόνια το Android έχει μπει για τα καλά στη ζωή μας. Συχνά γινόμαστε μάρτυρες συζητήσεων ή και καυγάδων για το τι μπορεί να κάνει και τι όχι. Μόνο καφέ δεν μας έχουν πει ότι κάνει μέχρι τώρα. Τι είναι όμως το Android; Για να δούμε! Κινητές συσκευές με Android. Στην πραγματικότητα λοιπόν το Android είναι ένα λειτουργικό σύστημα που χρησιμοποιεί τον πυρήνα του Linux σχεδιασμένο για κινητές συσκευές με οθόνες αφής όπως smartphones και tablets. Ακριβώς δηλαδή ότι είναι τα Windows, τα Macintosh και τα Linux για τους ηλεκτρονικούς υπολογιστές. Το όνομα του είναι ελληνικής προέλευσης και σημαίνει Ανδροειδές, δηλαδή ανθρωπόμορφο ρομπότ. Άλλωστε και το λογότυπο του, το οποίο δημιουργήθηκε από την γραφίστρια Irina Blok, είναι ένα ρομποτάκι χρώματος ανοιχτού πράσινου. Ακριβώς επειδή αρχικά σχεδιάστηκε για να χρησιμοποιηθεί σε συσκευές με οθόνες αφής (touchscreen) περιλαμβάνει ένα μεγάλο αριθμό αντίστοιχων λειτουργιών συμπεριλαμβανομένου και εικονικού πληκτρολογίου. Επίσης υποστηρίζει υπηρεσίες φωνής, δηλαδή τηλεφωνικές κλήσεις, υπηρεσίες σύντομων μηνυμάτων SMS και αποστολή μηνυμάτων πολυμέσων MMS. Στην πορεία ωστόσο χρησιμοποιήθηκε και σε πλήθος άλλων συσκευών όπως έξυπνες τηλεοράσεις, κονσόλες, ψηφιακές μηχανές κλπ.

5.4 Τα βήματα για την δημιουργία της εφαρμογής.

Βήμα 1

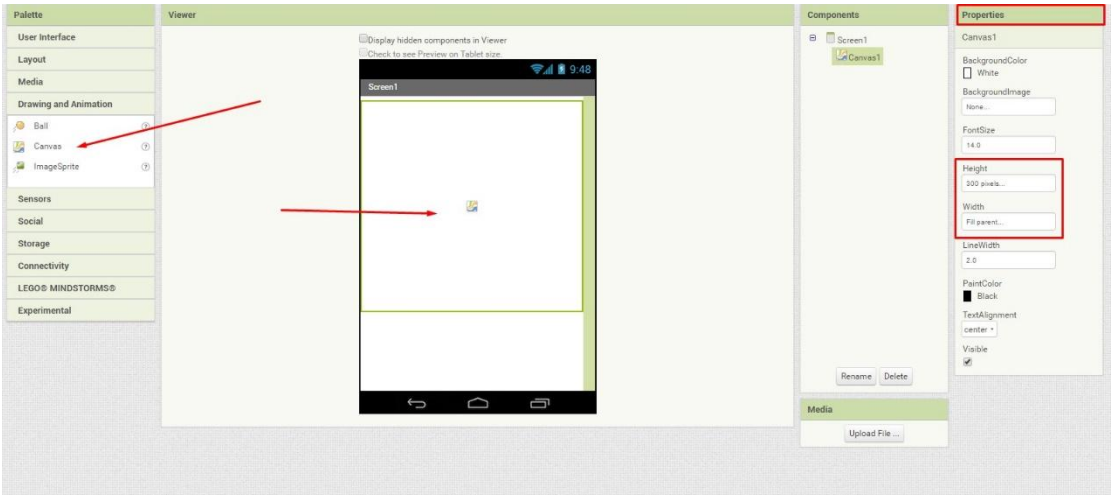


Εικόνα 1. Ξεκινώντας βλέπουμε το screen.

Βήμα 2

Στην συνέχεια θα πρέπει να πάμε στο "Drawing and Animation" και να επιλέξουμε το Canvas.

Το Canvas είναι αυτό που θα δώσει την κίνηση στην εικόνα μας όπως βλέπουμε στην εικόνα 2.



5.0 Δημιουργία της εφαρμογής Βήμα 2

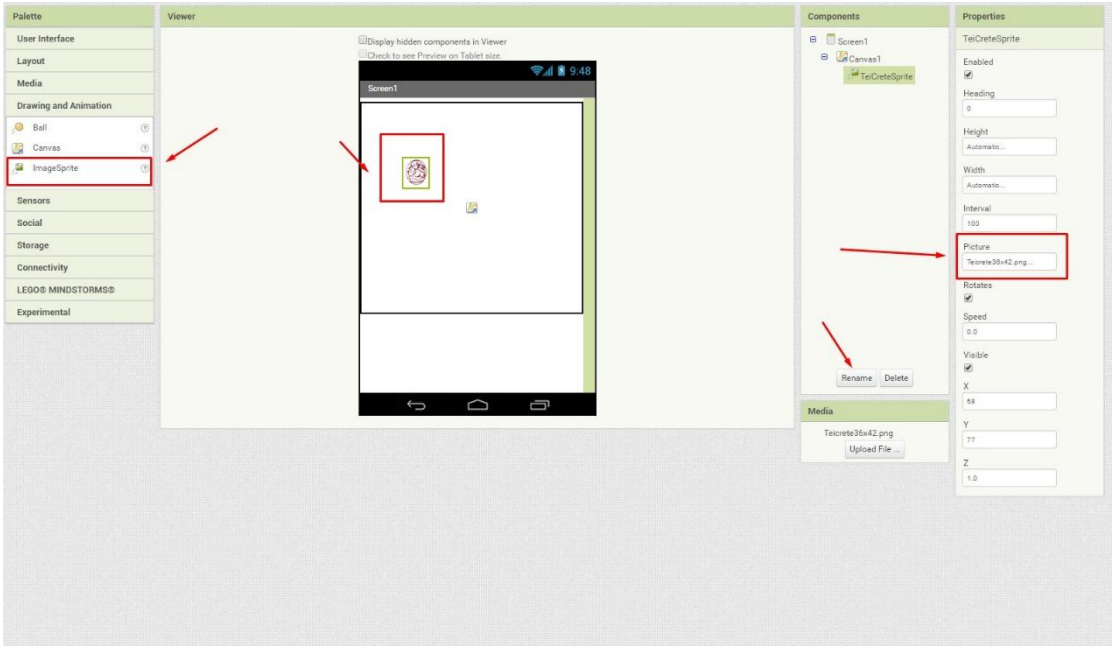
Εικόνα 2. Σχεδίαση εικόνας.

Δεξιά υπάρχουν τα Properties (Ιδιότητες) όπου βάζουμε στο Height (300 pixels) και το Width (Fill Parent).

Βήμα 3

Παραμένουμε στο "Drawing and Animation" όπως βλέπουμε στην εικόνα 3 και επιλέγουμε το ImageSprite και το τοποθετούμε μέσα στο Canvas (βήμα πρώτο). Στην συνέχεια πηγαίνουμε στα Properties > Image και ανεβάζουμε την φωτογραφία που εμείς θέλουμε.

Προσοχή η εικόνα θα πρέπει να είναι 36x42 και μορφή png για να πάρει το άσπρο.

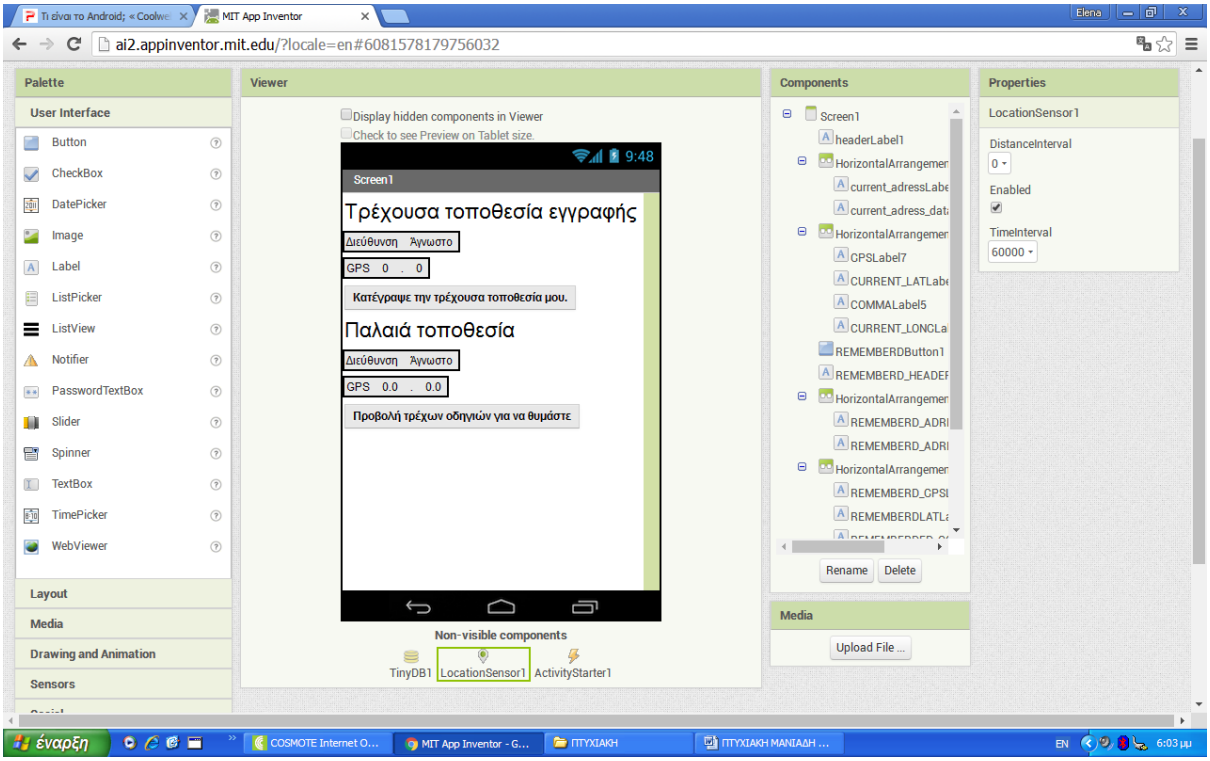


Βήμα 4

Εικόνα 3. Προσθέτοντας εικόνες στην εφαρμογή.

Για τη δημιουργία της εφαρμογής θα πρέπει να βάλουμε ορισμένες λειτουργίες ακόμη:

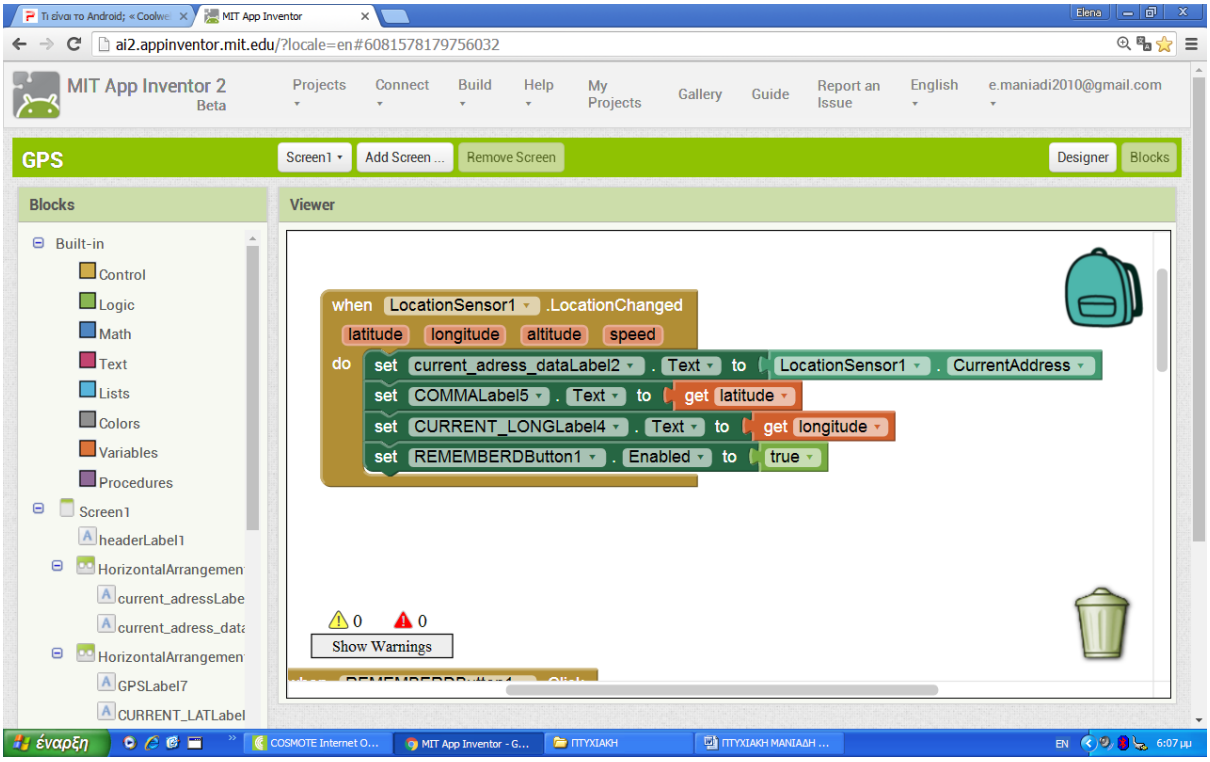
Την τρέχουσα τοποθεσία εγγραφής, ένα location sensor όπου θα καταγράφει και θα εξηγεί που ακριβώς βρίσκονται και που θέλουν να φτάσουν τέλος θα προσθέσουμε ένα email του ιδιοκτήτη του ξενοδοχείου για παράδειγμα όπου μόλις καταφθάσουν οι επισκέπτες να γνωρίζει ο επιχειρηματίας την ακριβή ώρα άφιξη τους όπως ακριβώς φαίνεται στην εικόνα 4 .



Εικόνα 4. Βάζοντας τις λειτουργίες της εφαρμογής.

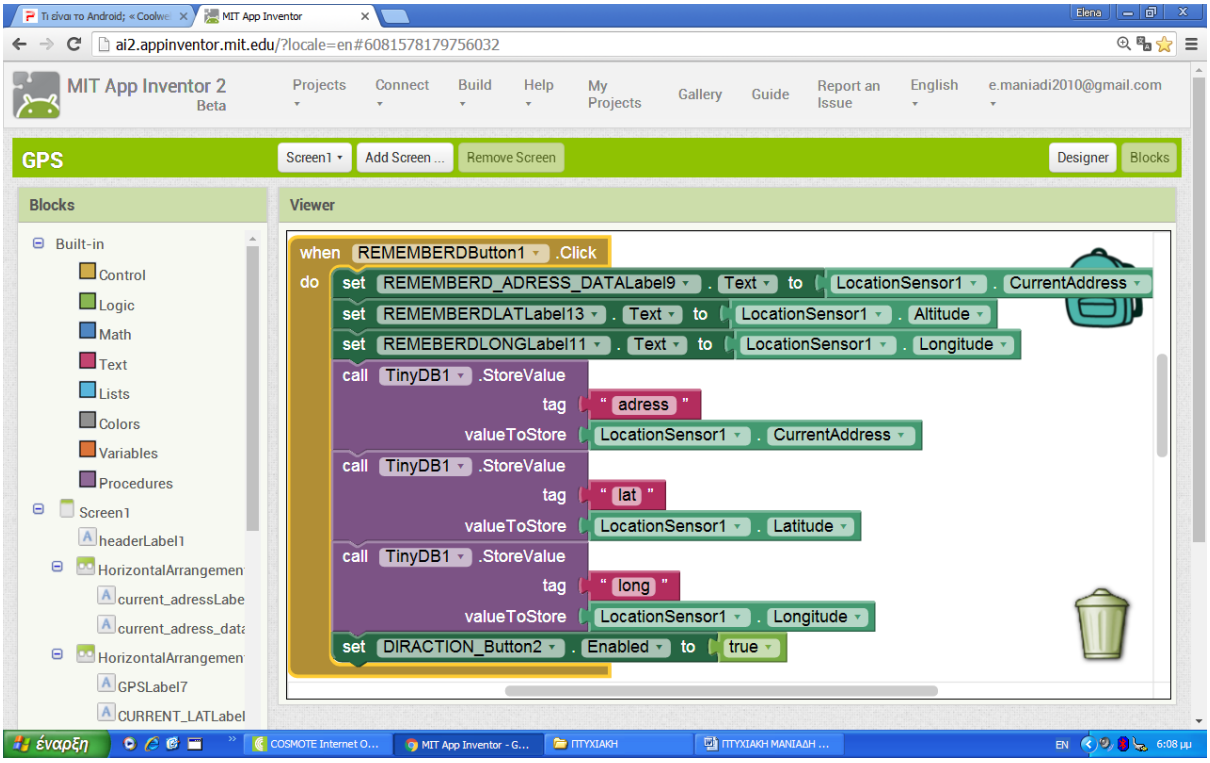
Βήμα 5

Θα πρέπει να φτιάξουμε τον κώδικα μας τώρα όπου θα συνδέεται η εφαρμογή όλη.



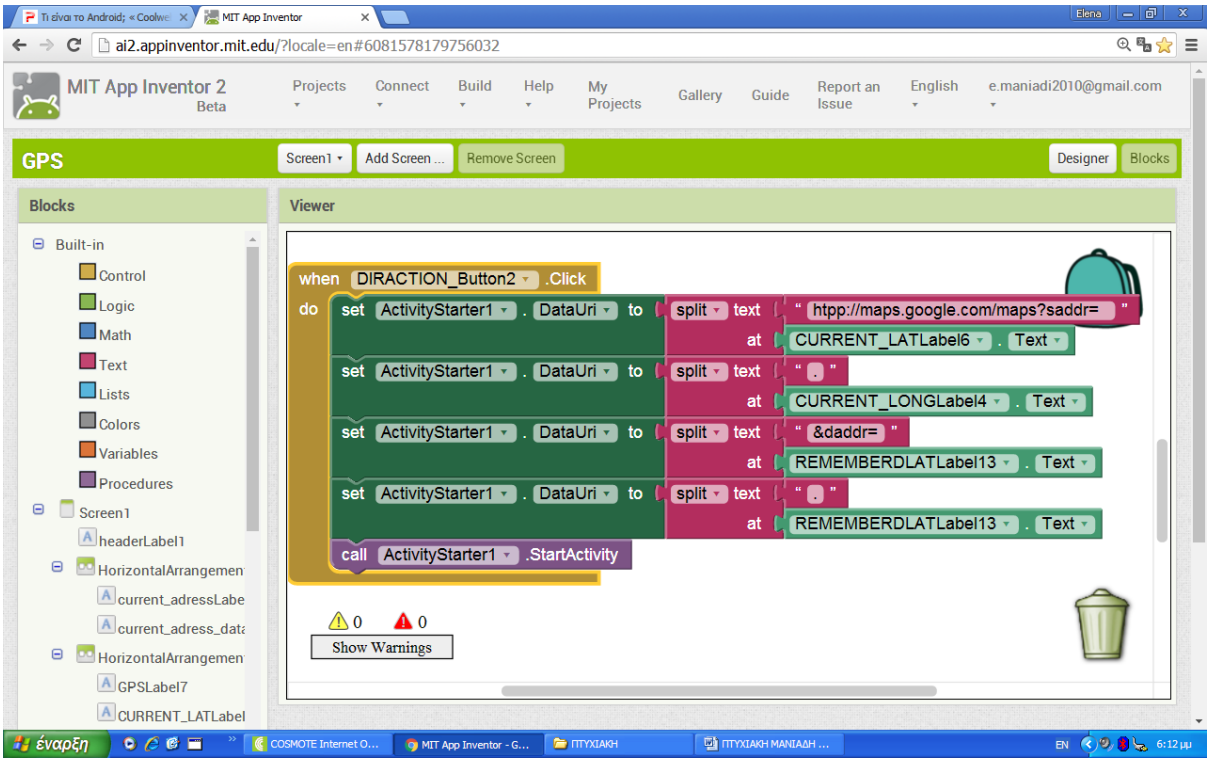
Εικόνα 5. Φτιάχνοντας των κώδικα.

Σε αυτό το κομμάτι του κώδικα μας λέει ότι αποθηκεύει την τοποθεσία όπου βρίσκεται ο επισκέπτης.



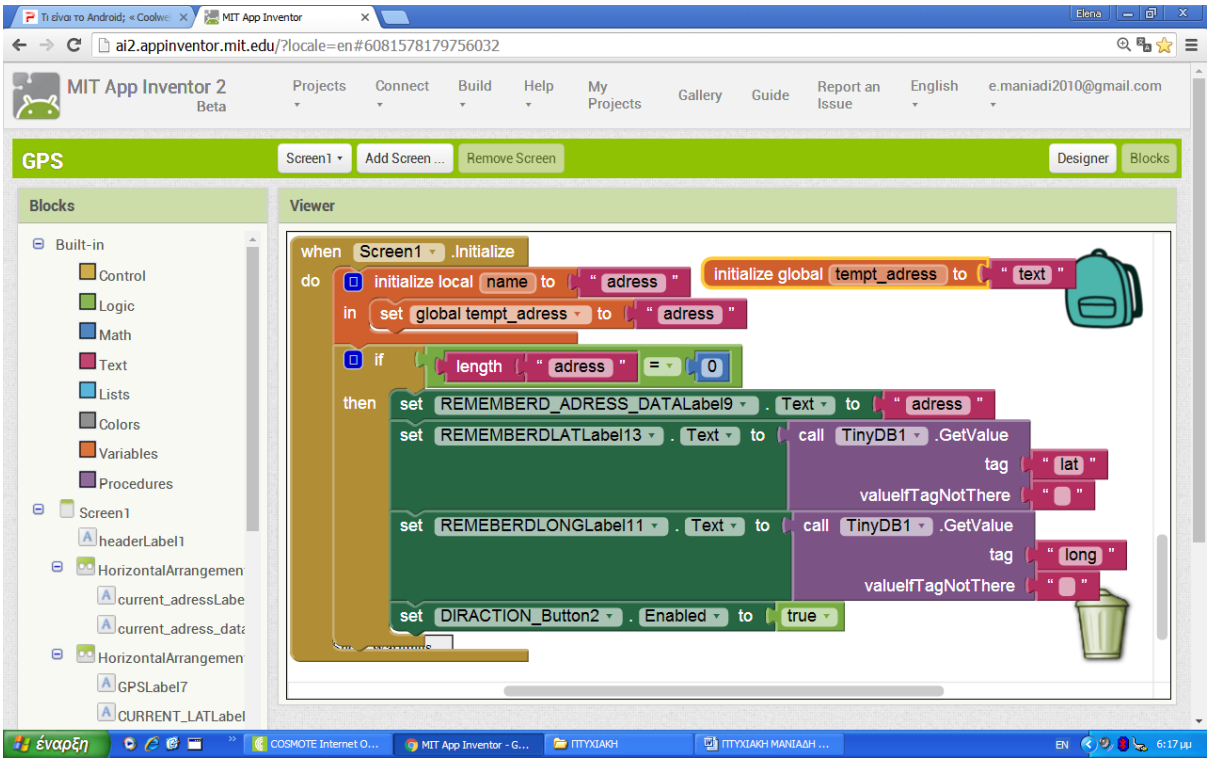
Εικόνα 6. Βάζοντας τα κουμπιά στον κώδικα.

Σε αυτό το κομμάτι κώδικα βλέπουμε ένα remember button το οποίο αποθηκεύει την τοποθεσία και καλεί μέσω του tiny την τοποθεσία που θα πρέπει να φτάσουν και τέλος ένα κουμπί το οποίο είναι διαθέσιμο να σε γυρίσει στην <αρχική σελίδα> της εφαρμογής.



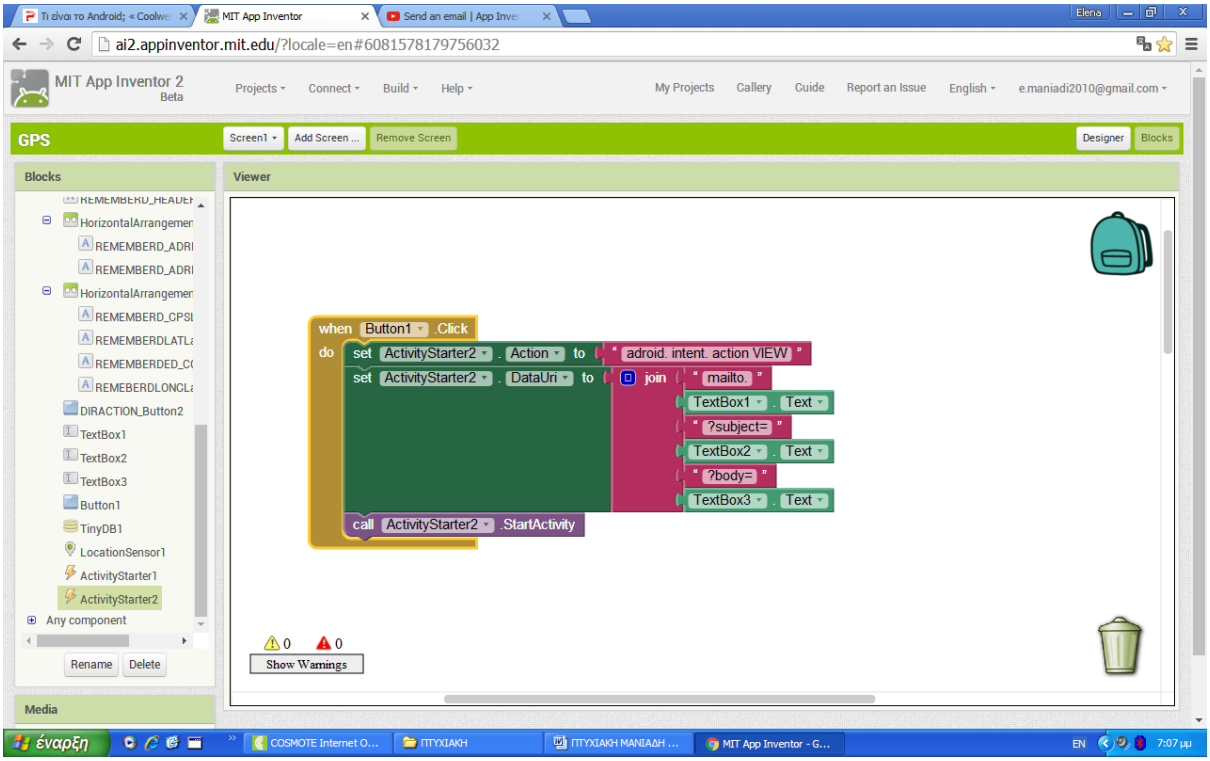
Εικόνα 7. Βάζοντας τα κουμπιά στον κώδικα.

Σε αυτό το σημείο βλέπουμε το κουμπί το οποίο συνδέεται με το Google maps για να μας δώσει τους χάρτες που χρειαζόμαστε και την εκκίνηση της διαδικασίας υπενθύμισης της τρέχουσας τοποθεσίας.



Εικόνα 8. Συνδέοντας την οθόνη με τα κουμπιά διεύθυνσης, τοποθεσίας.

Σε αυτό το κομμάτι ο κώδικας μας λέει ότι όταν ανοίγει η αρχική μας να εμφανίζει να γράψουμε το τρέχων όνομα και διεύθυνση όπου βρισκόμαστε και έπειτα την διεύθυνση που θέλουμε να πάμε. Μας λέει ακόμη να καταγραφεί η απόσταση που χρειάζεται να διανύσουμε για να φτάσουμε στο προορισμό μας . Τέλος αποθηκεύει την διεύθυνση με λέξεις.



Εικόνα 9. Το τελευταίο κουμπί της εφαρμογής συνδέεται με τον activity starter.

Τέλος είναι το κουμπί που συνδέει για να μπορούμε να στείλουμε email στον επιχειρηματία και να γνωρίζει την ακριβή ώρα άφιξης.

Barcode εφαρμογής.

ΚΕΦΑΛΑΙΟ 6

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα δύο λειτουργικά συστήματα κινητών τηλεφώνων κυριαρχούν στην αγορά εδώ και χρόνια. Σύμφωνα με στοιχεία του netmarketshare.com το λειτουργικό της Google είναι εγκατεστημένο στο **46%** των smartphones, ενώ της Apple στο **43%.** Ωστόσο, αν δούμε τα στοιχεία μόνο για το 2014 η κυριαρχία του Android είναι ολοκληρωτική καθώς, σύμφωνα με το idc.com, κατέχει το **84,4%** της αγοράς σε νέες συσκευές, ενώ το iOS μόλις το **11,7%** (και άλλο 3% το Windows Phone), γεγονός που εξηγείται από το ότι το Android χρησιμοποιείται από δεκάδες κατασκευαστές με συσκευές αξίας ακόμα και λίγων δεκάδων δολαρίων, ενώ το iOS «παίζει» αποκλειστικά στο premium κομμάτι**.**

Όμως ποιο λειτουργικό κερδίζει με βάση αντικειμενικά στοιχεία, ευκολία χρήσης, λειτουργίες και γενικότερη εντύπωση. Τα «έξυπνα» κινητά στην σημερινή εποχή είναι μία απαραίτητη συσκευή πληροφόρησης και επικοινωνίας. Είναι ένα εργαλείο με το οποίο οι χρήστες μπορούν να οργανώσουν την καθημερινή τους δραστηριότητα και μάλιστα από οπουδήποτε.

Είναι πλέον η πρώτη επιλογή των ανθρώπων διότι προσφέρει διασκέδαση, επικοινωνία, ενημέρωση αλλά και η χρήση των κινητών σαν φωτογραφική μηχανή. Ένας μέσος χρήστης κάνει την χρήση του «έξυπνου» κινητού του επί 3 ώρες την ημέρα , δηλαδή μια ολόκληρη ημέρα της εβδομάδας! Οι χρήστες παραδέχονται ότι χωρίς την κινητή τους συσκευή νιώθουν χαμένοι αυτό σε ποσοστό 4 στους 10! Η εξάρτηση των σύγχρονων ανθρώπων από τα κινητά μεγαλώνει διαρκώς, ο τυπικός χρήστης τα χρησιμοποιεί 221 διαφορετικές εργασίες στη διάρκεια της ημέρας, από το να δει το e-mail του, να δει ή τα στείλει μηνύματα, να κάνει έρευνα αγοράς μέχρι και τα ηλεκτρονικά ψώνια, τις διαδικτυακές τραπεζικές συναλλαγές του έως και «χάζεμα» στο διαδίκτυο ή παίξιμο παιγνιδιών για χαλάρωση. Τα προγράμματα ανταποδοτικής επιβράβευσης των πελατών από τις εταιρείες, τείνουν να έχουν αυξητική τάση το τελευταίο διάστημα. Σύμφωνα με έρευνες που έχουν γίνει, αυτό συμβαίνει επειδή το 82% του κοινού συνηθίζει να αγοράζει από επιχειρήσεις με προγράμματα ανταποδοτικής πίστης (loyalty programs) και το 46% συνηθίζει να ξοδεύει περισσότερο σε επιχειρήσεις με loyalty programs. Επίσης, η ολοένα αυξανόμενη χρήση κινητών συσκευών (smartphones και tablets) εξηγεί γιατί το 59% του καταναλωτικού κοινού συνηθίζει να κατεβάζει και να εγγράφεται σε mobile loyalty application. Τέλος, δεν είναι καθόλου αμελητέο το γεγονός ότι σε μια

επιχείρηση κοστίζει 6-7 φορές περισσότερο να προσελκύσει νέους πελάτες από ότι να διατηρήσει τους ήδη υπάρχοντες.

Προτίμηση της επιχείρησης από κάποια αντίστοιχη του ανταγωνισμού

Διατήρηση / επαναληψιμότητα του υπάρχοντος πελατολογίου (Customer Lifetime Value)

Επαναπροσέλκυση παλιών πελατών
Προσέλκυση νέων πελατών
«Χτίσιμο» δεσμών με τους πελάτες
Αλληλεπίδραση πελατών με την επιχείρηση
Αύξηση της αναγνωρισιμότητας της επιχείρησης
Μετρήσιμα αποτελέσματα σε ενέργειες του τμήματος marketing
Απόκτηση και ανάλυση δεδομένων πελατών
Αξιοποίηση δεδομένων πελατών για εμπορικούς και διαφημιστικούς σκοπούς
Εισαγωγή σε mobile εφαρμογές και αξιοποίηση των δυνατοτήτων που προσφέρουν
Ακολουθείτε το κοινό σας στα σύγχρονα κανάλια επικοινωνίας
Επιπλέον "εργαλείο" marketing

Βιβλιογραφία

Ελληνόφωνη:

- Δούκας, Χαράλαμπος, Θωμάς Πλιάκας, και Ηλίας Μαγκλογιάννης. "Mobile διαχείρισης πληροφοριών υγειονομικής περίθαλψης που χρησιμοποιούν το Cloud Computing και το Android OS."

- Ένα αυτο-ρύθμισης νέα παιδιά γενιάς σύστημα παρακολούθησης βασίζεται σε κινητά ad hoc δίκτυα που αποτελούνται από Android κινητά τερματικά." Συστήματα Αυτόνομης Αποκεντρωμένη (ISADS), 2011 10ο Διεθνές Συμπόσιο . IEEE 2011.

- Δίκτυα Υπολογιστών 57,9 (2013): 2093-2115.

- Έρευνες IEEE Communications & Tutorials 17.1 (2015): 358-380.

- International Journal of katanemhm;ena d;iktya aisuht;hrvn 9.2 (2013)Q 917.923. 23.

- Ασύρματων επικοινωνιών και mobile computing 13,18 (2013): 1587-1611.

- Έρευνες IEEE Communications & Tutorials 16.1 (2014): 393-413.

- Συστήματα μελλοντικής γενιάς ηλεκτρονικών υπολογιστών 29.1 (2013): 84-106.

Ξενόγλωσση:

- Abolfazli S., Sanaei Z., Hadi Sanaei M., Shojafar M., Gani A. (2015). Mobile Cloud Computing: the state-of-the-art, challenges, and future research.

- (2009). Cloud Computing Benefits, risks and recommendations for information security European Network and Information Security Agency (ENISA).

- Mather T. , Kumaraswamy S., Shahed L. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice), O'Reilly Media, Inc.

- Neidecker-Lutz B., Jeffery K., Schubert L. (2010). "The Future of Cloud Computing Opportunities for European Cloud Computing Beyond 2010", Expert Group Report Public Version 1.0, European Comission, Information Society and Media.

- Rehan S. (2011). Cloud computing effect on enterprises.

- Rittinghouse J., Ransome J. (2010). Cloud Computing Implementation, Management, and Security.

- Betcher J. T., Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners.

- Turner-McGrievy, Gabrielle M., et al. "Comparison of traditional versus mobile app self-monitoring of physical activity and dietary intake among overweight adults participating in an mHealth weight loss program." *Journal of the American Medical Informatics Association* 20.3 (2013): 513-518.

- Lin, Jialiu, et al. "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing." *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM, 2012.

- Khalid, Hammad, et al. "What do mobile app users complain about?." *IEEE Software* 32.3 (2015): 70-77.

- Joorabchi, Mona Erfani, Ali Mesbah, and Philippe Kruchten. "Real challenges in mobile app development." *2013 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*. IEEE, 2013.

- Felt, Adrienne Porter, et al. "Android permissions: User attention, comprehension, and behavior." *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012.

- Chin, Erika, et al. "Measuring user confidence in smartphone security and privacy." *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012.

- Felt, Adrienne Porter, et al. "Android permissions demystified." *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011.

- Enck, William, et al. "A Study of Android Application Security." *USENIX security symposium*. Vol. 2. 2011.

- Barrera, David, et al. "A methodology for empirical analysis of permission-based security models and its application to android." *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010.

- Felt, Adrienne Porter, et al. "Android permissions: User attention, comprehension, and behavior." *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012.