

Thesis Dissertation

SMART HOME AND SMART LOCK TECHNOLOGY

Andreas Makris

UNIVERSITY OF CYPRUS



DEPARTMENT OF COMPUTER SCIENCE

January 2021

UNIVERSITY OF CYPRUS
DEPARTMENT OF COMPUTER SCIENCE

Smart Home and Smart Lock Technology

Andreas Makris

Advisor:
Dr. Andreas Pitsillides

Thesis submitted in partial fulfilment of the requirements for the award of
degree of Bachelor in Computer Science at University of Cyprus.

January 2021

Ευχαριστίες

Πρώτα απ' όλα θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου της Διπλωματικής Εργασίας Δρ. Ανδρέα Πιτσιλλίδη για την βοήθεια του και την καθοδήγηση του σε όλα τα στάδια της εργασίας μου.

Επιπλέον, θα ήθελα να ευχαριστήσω τον πατέρα μου οποίος με την γνώσεις του και την εμπειρία του στο θέμα, με βοήθησε στα αρχικά στάδια της εργασίας.

Τέλος θα ήθελα να ευχαριστήσω την οικογένεια μου, τους συγγενείς και τους φίλους μου για την στήριξη και την πίστη τους που είχαν σε εμένα για την ολοκλήρωση της εργασίας.

Περίληψη

Οι έννοιες του διαδικτύου και του Internet of Things (IoT) έχουν εδραιωθεί για τα καλά στην καθημερινότητα μας. Οι απλές ηλεκτρικές συσκευές ολοένα και λιγοστεύουν και στην θέση τους μπαίνουν οι λεγόμενες «Έξυπνες» συσκευές. Τα απλά παραδοσιακά σπίτια μετατρέπονται σε «Έξυπνα» σπίτια απλοποιώντας και αυτοματοποιώντας λειτουργίες όπως ο φωτισμός και η κηπουρική. Μεγάλες εταιρείες όπως η Google και η Amazon έχουν μπει δυναμικά στον χώρο των smart συσκευών και smarthome συστημάτων κάτι που υποδηλώνει ότι η τεχνολογία αυτή είναι επίκαιρη και επικερδής, τόσο στους κατασκευαστές όσο και στους καταναλωτές.

Η Διπλωματική Εργασία επικεντρώνεται σε αυτή τη Smart Home τεχνολογία και πιο συγκεκριμένα στο Smart Lock. Η τεχνολογία του Smart Lock είναι σχετικά καινούργια καθιστώντας την υλοποίηση του ενδιαφέρον και γεμάτη προκλήσεις. Η κύρια πρόκληση που έπρεπε να επιτευχθεί ήταν η υλοποίηση ενός ασφαλούς συστήματος το οποίο όμως να έχει απλό και φιλικό προς τον χρήστη περιβάλλον.

Για την υλοποίηση της εργασίας λήφθηκαν υπόψη οι υπάρχουσες τεχνολογίες και εργαλεία που χρησιμοποιούνται στο smarthome industry. Επιπλέον έγινε μελέτη στους κινδύνους που αντιμετωπίζουν τέτοια συστήματα και στους τρόπους αντιμετώπισης τους και με βάση αυτούς έγινε και η υλοποίηση. Τέλος, έγινε η αξιολόγηση του συστήματος και καταγράφηκαν τα τελικά συμπεράσματα.

Περιεχόμενα

Κεφάλαιο 1	1
1.1 Γενική Εισαγωγή.....	1
1.2 Περιγραφή Διπλωματικής Εργασίας.....	2
1.3 Δομή Διπλωματικής Εργασίας.....	3
Κεφάλαιο 2	5
2.1 Smart Home.....	5
2.2 Smart Lock	8
2.3 Smart Home Κίνδυνοι και Μέτρα Προστασίας	9
Κεφάλαιο 3	12
3.1 Hardware	12
3.1.1 Raspberry Pi.....	12
3.1.2 PN532 NFC Module.....	16
3.1.3 Adafruit 16x2 LCD Pi Plate	17
3.1.4 3x4 Matrix Keypad	19
3.2 Τεχνολογίες - Software	19
3.2.1 Python	20
3.2.2 Node.js.....	21
3.2.3 MariaDB	22
3.2.4 Expo React Native.....	23
Κεφάλαιο 4	24
4.1 Προδιαγραφές συστήματος	24
4.2 Υλοποίηση συστήματος	25
4.2.1 Εγκατάσταση συστήματος	27
4.2.2 Διεπαφή φυσικής παρουσίας.....	28
4.2.3 Διεπαφή smartphone εφαρμογής.....	32
Κεφάλαιο 5	38
5.1 Εισαγωγή.....	38
5.2 Αξιολόγηση	39
5.3 Αδυναμίες συστήματος	41
Κεφάλαιο 6	43
6.1 Συμπεράσματα.....	43
6.2 Μελλοντικά Σχέδια	44
Βιβλιογραφία	45
Χρήσιμα links	45

Κεφάλαιο 1

Εισαγωγή

1.1	Γενική Εισαγωγή.	1
1.2	Περιγραφή Διπλωματικής Εργασίας.	2
1.3	Δομή Διπλωματικής Εργασίας.	3

1.1 Γενική Εισαγωγή

Αναμφισβήτητα η ραγδαία αύξηση της τεχνολογίας έχει επηρεάσει τη ζωή του μέσου ανθρώπου. Η ανάπτυξη των microcontrollers και της ασύρματης τεχνολογίας οδήγησαν στην κατασκευή «έξυπνων συσκευών». Έξυπνες συσκευές αποκαλούνται κυρίως οι συσκευές που ενώνονται στο διαδίκτυο και επιτρέπουν την χρήση τους, την παρακολούθηση τους ή την ανταλλαγή δεδομένων μέσω του διαδικτύου. Τέτοιες συσκευές χρησιμοποιούνται κυρίως στην ιατρική, στην γεωργία, στην παραγωγή ενέργειας και γενικά στην παραγωγή αγαθών.

Ο άνθρωπος εκ φύσεως πάντα ψάχνει τρόπους για να βελτιώσει την ζωή του. Έτσι δεν άργησε να εντάξει τις «έξυπνες» αυτές συσκευές στη ζωή του. Το μεγάλο μπαμ έγινε με την εφεύρεση των smartphone. Το smartphone επιτρέπει την πλοήγηση στον διαδίκτυο και είναι γενικά ένας υπολογιστής στην τσέπη του κάθε ανθρώπου. Τα smartphone σε συνδυασμό με τα εκατομμύρια applications που υπάρχουν επιτρέπουν στον άνθρωπο να κάνει αμέτρητες λειτουργίες με το πάτημα ενός κουμπιού.

Η τεχνολογία των έξυπνων συσκευών δεν σταμάτησε εκεί, αντιθέτως ήρθε πιο κοντά στην καθημερινότητα του ανθρώπου με την ανάπτυξη των έξυπνων οικιακών συσκευών. Συσκευές όπως φούρνοι, ψυγεία, τοστιέρες καφετιέρες μπορούν πλέον να ενωθούν στο διαδίκτυο διευρύνοντας έτσι την έννοια του Internet of Things (IoT). Το σύστημα ελέγχου όλων αυτών των έξυπνων οικιακών συσκευών ονομάζεται σύστημα Smart Home.

Μια άλλη συσκευή σχετικά καινούργια στον τομέα των Smart Home είναι το Smart Lock ή αλλιώς έξυπνη κλειδαριά. Με το Smart Lock ο χρήστης μπορεί πλέον να ξεκλειδώσει την πόρτα του σπιτιού του χωρίς την χρήση του παραδοσιακού κλειδιού. Μερικοί από τους τρόπους ξεκλειδώματος ενός Smart Lock είναι με την χρήση PIN, δακτυλικού αποτυπώματος, smartphone application NFC κλπ. Επιπλέον με την χρήση Smart Lock ο χρήστης μπορεί να ανοίξει την πόρτα remotely δηλαδή χωρίς να βρίσκεται κοντά στην πόρτα. Ο κύριος λόγος για τον οποίο τα Smart Lock δεν είναι τόσο διαδεδομένα είναι λόγω του υψηλού ρίσκου όσον αφορά την ασφάλεια του συστήματος.

1.2 Περιγραφή Διπλωματικής Εργασίας

Η Διπλωματική Εργασία αφορά κυρίως την υλοποίηση ενός Smart Lock. Κίνητρο της Εργασίας ήταν το πως θα γίνει ο σχεδιασμός ενός ασφαλούς συστήματος ξεκλειδώματος μιας πόρτας σε συνδυασμό με ένα περιβάλλον το οποίο να είναι εύχρηστο και φιλικό προς τον χρήστη. Επιπλέον το τελικό σύστημα θα πρέπει να έχει διάφορες μεθόδους με τις οποίες ο χρήστης να μπορεί να ξεκλειδώσει την πόρτα είτε από κοντά είτε remotely, να μπορεί να παρακολουθήσει ποιος και πότε προσπάθησε να ανοίξει την πόρτα και να λαμβάνει ειδοποιήσεις σε περιπτώσεις τυχόν προσπάθειας για παραβίαση του συστήματος.

Η Διπλωματική Εργασία αποτελείται από δύο μέρη: Η υλοποίηση ενός συστήματος του οποίου ο χρήστης θα μπορεί να ξεκλειδώνει την πόρτα με φυσική παρουσία, δηλαδή θα βρίσκεται κοντά στην πόρτα και ενός συστήματος του οποίου θα μπορεί να την ξεκλειδώνει από απόσταση (remotely). Και για τις δύο προσεγγίσεις θα πρέπει να ληφθεί υπόψη τόσο η ασφάλεια τόσο και η εμπειρία του χρήστη.

Το σύστημα ξεκλειδώματος με φυσική παρουσία έχει μια κύρια διεπαφή η οποία προβάλλεται μέσω μιας οθόνης LCD και παρουσιάζει τις 3 μεθόδους ξεκλειδώματος: με την χρήση PIN, NFC και One Time Password (OTP). Η επιλογή για την μέθοδο ξεκλειδώματος γίνεται με την χρήση του numpad και την επιλογή των αριθμών 1-3 αντίστοιχα.

Η κύρια διεπαφή της smartphone εφαρμογής παρουσιάζει τις κύριες λειτουργίες της εφαρμογής: Ξεκλείδωμα από απόσταση χρησιμοποιώντας της μεθόδους PIN και fingerprint, μέθοδο ξεκλειδώματος με την χρήση του NFC του κινητού και παρακολούθηση των logs. Επιπρόσθετα με την χρήση της εφαρμογής ο χρήστης μπορεί

να λαμβάνει ειδοποιήσεις σε περίπτωση πολλαπλών αποτυχημένων προσπαθειών ξεκλειδώματος.

1.3 Δομή Διπλωματικής Εργασίας

Ξεκινώντας με το κεφάλαιο 1, έχουμε μια γενική εισαγωγή για τα Smart Home και τις εφαρμογές τους στην σύγχρονη εποχή και μια σύντομη περιγραφή των λειτουργιών του συστήματος που υλοποιήθηκε κατά την διάρκεια της Διπλωματικής εργασίας. Επίσης περιέχει και μια σύντομη περιγραφή για το τι έπεται να διαβάσει ο αναγνώστης σε κάθε κεφάλαιο της εργασίας.

Συνεχίζοντας στο κεφάλαιο 2, το «Background», ο αναγνώστης πρόκειται να εξοικειωθεί περαιτέρω στις έννοιες που αφορούν τα Smart Home και τα Smart Lock που είναι και το κυρίως θέμα της Διπλωματικής Εργασίας. Επιπλέον θα ενημερωθεί για τους κινδύνους που διατρέχουν τα συστήματα και τρόπους αντιμετώπισής τους.

Ακολούθως, το κεφάλαιο 3, αφορά το Hardware & Software που επιλέχθηκε για την υλοποίηση του συστήματος, καθώς και τους λόγους για τους οποίους έγινε η επιλογή τους.

Το κεφάλαιο 4, το οποίο είναι και το εκτενέστερο, περιγράφει την υλοποίηση του συστήματος. Αρχικά, ξεκινά με τον προσδιορισμό των προδιαγραφών του συστήματος βάση των οποίων έγινε και η υλοποίηση. Στην συνέχεια περιγράφεται με λεπτομέρεια τον τρόπο και την ιδεολογία με την οποία κτίστηκε το σύστημα. Τέλος, γίνεται επεξήγηση όλων των λειτουργιών του συστήματος με οδηγίες βήμα προς βήμα και φωτογραφίες/screenshots.

Προχωρώντας, έχουμε το κεφάλαιο 5 το οποίο αφορά την αξιολόγηση του συστήματος. Πρώτα γίνεται μια εισαγωγή για τον τρόπο και τους λόγους που γίνεται η αξιολόγηση του συστήματος. Στη συνέχεια γίνεται η αξιολόγηση του συστήματος σε συνάρτηση με τις προδιαγραφές του συστήματος που αναφέρθηκαν σε προηγούμενο κεφάλαιο. Τέλος γίνεται αναφορά στις αδυναμίες του συστήματος.

Το κεφάλαιο 6, το οποίο είναι και το τελευταίο, περιγράφει τα συμπεράσματα που καταγράφηκαν με το πέρας της επιτυχούς υλοποίησης του συστήματος και τα σχέδια για το μέλλον.

Κεφάλαιο 2

Background

2.1	Smart Home	5
2.2	Smart Lock	8
2.3	Smart Home Κίνδυνοι και Μέτρα Προστασίας	9

2.1 Smart Home

Η Smart Home τεχνολογία ή αλλιώς η τεχνολογία έξυπνου σπιτιού βασίζεται στην παρακολούθηση και τον έλεγχο οικιακών συσκευών μέσω μιας συσκευής, smartphone ή του διαδικτύου. Σκοπός της Smart home τεχνολογίας είναι η βελτίωση της ποιότητας της ζωής του ανθρώπου σε συνδυασμό με την ευκολία και την ασφάλεια που προσφέρει.

Η εφεύρεση του microcontroller το 1971 είχε ως αποτέλεσμα τη μείωση των τιμών των ηλεκτρονικών συσκευών καθιστώντας τις τεχνολογίες αυτές πιο προσιτές. Ο microcontroller μπορεί να περιέχει ένα ή περισσότερα CPUs και σε συνδυασμό με την memory μπορεί να ελέγχει διάφορες συσκευές εισόδου εξόδου. Το 1975 αναπτύχθηκε η πρώτη τεχνολογία δικτύου οικιακού αυτοματισμού γενικής χρήσης με όνομα X10. Οι συσκευές X10 χρησιμοποιούσαν ηλεκτρικό ρεύμα για τον έλεγχο των συσκευών μέσω bursts ραδιοκυμάτων που περιείχαν ψηφιακά δεδομένα. Μέχρι το 1978, τα προϊόντα X10 περιλάμβαναν μια κονσόλα εντολών 16 καναλιών, μια μονάδα λαμπτήρα και μια μονάδα συσκευής. Αργότερα ήρθε και η μονάδα διακόπτη τοίχου η οποία περιλάμβανε και το πρώτο X10 timer.

Αναμφισβήτητα η τεχνολογία του Smart Home είναι από τις πιο υποσχόμενες και κερδοφόρες στην σύγχρονη εποχή. Σύμφωνα με έρευνα του MarketWatch το 2016, όταν ακόμα η τεχνολογία αυτή ήταν σχετικά καινούργια, η διεθνής αγορά smart home

υπηρεσιών υπολογίστηκε γύρω στα 55.6 δισεκατομμύρια δολάρια. Επιπλέον, σύμφωνα με έρευνα του Rochester Real Estate, 47% των Αμερικανών ηλικίας 23-38 έχουν τουλάχιστον μία συσκευή smart home στο σπίτι τους ποσοστό το οποίο είναι υψηλότερο όλο των εποχών φανερώνοντας το αυξανόμενο ενδιαφέρον του κόσμου στον τομέα αυτό.

Οι Smart Home εφαρμογές σήμερα είναι πολλές και ποικίλουν. Μερικές από αυτές αναφέρονται πιο κάτω:

- Voice Assistant: Η πιο δημοφιλής συσκευή smart home είναι το Voice Assistant. Το Voice Assistant είναι ένα speaker με μικρόφωνο το οποίο ακούει στις εντολές του χρήστη και της εκτελεί. Οι εντολές αυτές μπορεί να είναι απλές ερωτήσεις της οποίες ο Assistant θα ψάξει στο διαδίκτυο και θα απαντήσει μέσω του speaker ή μέχρι και τον έλεγχο άλλων έξυπνων συσκευών. Μερικά έχουν οθόνη και κάμερα για περισσότερες λειτουργίες όπως βιντεοκλήσεις και έλεγχο καμερών. Ο λόγος για τον οποίο είναι το πιο διαδεδομένο είναι κυρίως στην ευκολία εγκατάστασης και χρήσης του αφού το μόνο που χρειάζεται είναι σύνδεση στο διαδίκτυο. Υπάρχουν διάφορα Voice Assistant συσκευές με πιο διαδεδομένα το Amazon Alexa και το Google Home.
- Σύστημα ελέγχου φωτισμού: Το σύστημα ελέγχου φωτισμού είναι το σύστημα που είναι υπεύθυνο για την διαχείριση όλων φώτων σε ένα σπίτι μέσω ενός application ή πλατφόρμας. Το σύστημα αυτό μπορεί να υλοποιηθεί με διάφορους τρόπους είτε με την χρήση έξυπνων λαμπών είτε με την χρήση έξυπνων switches. Το πλεονέκτημα χρήσης λαμπών είναι ότι είναι ευκολότερο στην εγκατάσταση τους αλλά έχουν το μειονέκτημα ότι είναι αναλώσιμες και κάποτε θα πρέπει να αντικατασταθούν. Η Amazon προωθεί τις δικές τις έξυπνες λάμπες με κίνητρο την ευκολία χρήσης τους (Plug & Play) σε συνδυασμό με την Amazon Alexa.
- Σύστημα ελέγχου θερμοκρασίας: Το σύστημα αυτό επιτυγχάνεται με την χρήση έξυπνων θερμοστατών οι οποίοι είναι υπεύθυνοι για την live καταμέτρηση της θερμοκρασίας κάθε δωματίου. Όταν παρατηρηθεί αλλαγή στην θερμοκρασία το σύστημα θα προσπαθήσει να την προσαρμόσει ανάλογα ανάβοντας ή κλείνοντας το κλιματιστικό ή την θέρμανση. Με τον τρόπο αυτό ο χρήστης όχι μόνο κερδίζει χρόνο αλλά και χρήμα αφού δεν σπαταλά άσκοπα ενέργεια.

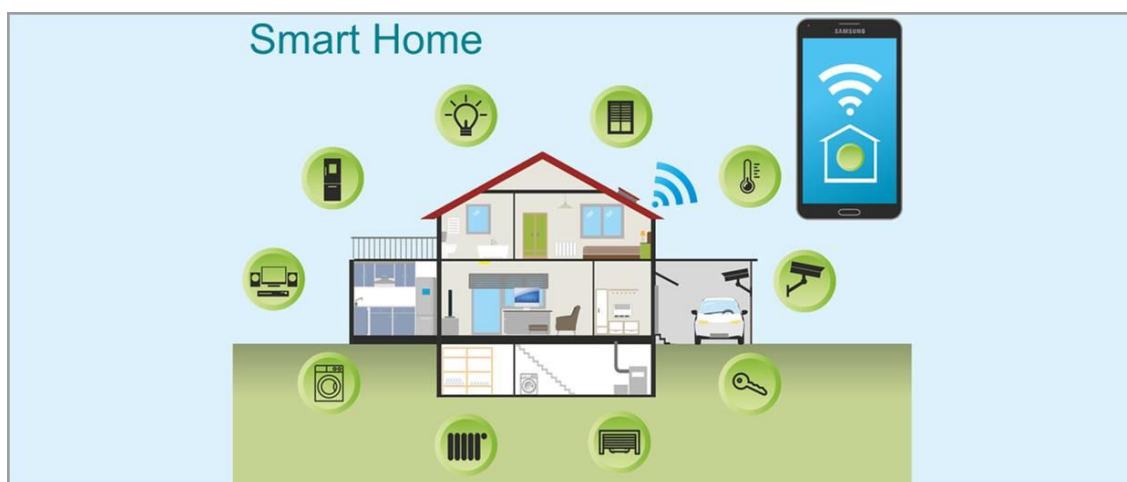
- Συστήματα ανίχνευσης ατόμων: Το σύστημα ανίχνευσης λειτουργεί με την χρήση διαφόρων αισθητήρων με σκοπό να καταλάβει αν κάποιος βρίσκεται στο συγκεκριμένο δωμάτιο. Οι αισθητήρες που χρησιμοποιούνται μπορεί να είναι infrared, ακουστικοί, κάμερες με image recognition ή ακόμα και αισθητήρες που ανιχνεύουν την ύπαρξη κινητού τηλεφώνου μέσω Bluetooth ή Wi-Fi. Με την ανίχνευση ατόμων και σε συνδυασμό με άλλες έξυπνες συσκευές μπορεί να ανάβουν και να σβήνουν αυτόματα φώτα, κλιματιστικά, κουρτίνες κλπ. γλυτώνοντας και πάλι χρόνο και χρήμα στους χρήστες.
- Έξυπνες τηλεοράσεις: Οι τηλεοράσεις σήμερα χρησιμοποιούνται όλο και λιγότερο για την παρακολούθηση των τυπικών καναλιών. Με την ύπαρξη έξυπνων τηλεοράσεων και συσκευών όπως το Google Chromecast και Amazon Firestick οι τηλεοράσεις έχουν μετατραπεί σε πλήρης υπολογιστές που επιτρέπουν πρόσβαση στο διαδίκτυο, streaming ταινιών και μουσικής προσφέροντας άνεση και ψυχαγωγία στους χρήστες.
- Συστήματα Συναγερμού: Παρόμοια με το σύστημα ανίχνευσης ατόμων το σύστημα συναγερμού με την χρήση αισθητήρων και καμερών μπορεί να ανιχνεύσει ανεπιθύμητη κίνηση εντός ή εκτός του σπιτιού και να ενημερώσει άμεσα τον χρήστη. Τέτοια συστήματα είναι πολύ ευαίσθητα γιατί αφορούν την ασφάλεια του σπιτιού και γι' αυτό πρέπει να τηρούν τα απαραίτητα πρωτόκολλα ασφαλείας.
- Smart Lock: Τα Smart Lock είναι υπεύθυνα για το ασφαλές άνοιγμα πορτών του σπιτιού είτε remotely είτε με κάποια άλλη μέθοδο όπως PIN, fingerprint, face recognition, NFC και άλλα. Όμοια με τα συστήματα συναγερμού είναι και αυτά πολύ ευαίσθητα και επειδή το project αφορά τα smart lock τα security concerns θα αναλυθούν παρακάτω.
- Smart Garden: Συστήματα έξυπνου κήπου μπορούν να περιλαμβάνουν αυτόματο πότισμα, αυτόματη ρύθμιση του φωτός, αυτόματη πρόσθεση θρεπτικών ουσιών στα φυτά.
- Έξυπνες ηλεκτρικές συσκευές: Πλέον στις μέρες μας, λόγω του internet of things, σχεδόν όλες οι οικιακές συσκευές μπορούν να ενωθούν στο διαδίκτυο. Αυτό σημαίνει ότι όλες οι συσκευές μπορούν να προγραμματιστούν μέσω ενός application για να ικανοποιήσουν τις ανάγκες του χρήστη. Τέτοιες συσκευές

είναι το έξυπνο ψυγείο, η έξυπνη καφετιέρα, ο έξυπνος φούρνος, οι έξυπνες ηλεκτρικές σκούπες και πολλά άλλα.

Αυτές είναι μόνο κάποιες από τις εφαρμογές που μπορούν να υπάρξουν σε ένα έξυπνο σπίτι. Σίγουρα ακόμα δεν υπάρχουν σε όλα τα σπίτια αφού οι τεχνολογίες αυτές είναι σχετικά καινούργιες αλλά όλα δείχνουν ότι στο μέλλον πολλές από αυτές τις εφαρμογές βρίσκονται σε κάθε σπίτι.

Figure 1

Παράδειγμα Smarthome συστήματος



Source: <https://carbontrack.com.au/blog/future-smart-homes-functional-feature-integration>

Σχήμα 2.1: Παράδειγμα Smarthome συστήματος

2.2 Smart Lock

Το Smart Lock ή αλλιώς η έξυπνη κλειδαριά είναι μια ηλεκτρομηχανική κλειδαριά που έχει σχεδιαστεί για να εκτελεί λειτουργίες κλειδώματος και ξεκλειδώματος μιας πόρτας όταν λαμβάνει τέτοιες οδηγίες από μια εξουσιοδοτημένη συσκευή χρησιμοποιώντας ένα ασύρματο πρωτόκολλο και ένα κρυπτογραφικό κλειδί για την εκτέλεση της διαδικασίας εξουσιοδότησης. Παρακολουθεί επίσης την πρόσβαση και στέλνει ειδοποιήσεις για τα διάφορα συμβάντα που παρακολουθεί και ορισμένα άλλα κρίσιμα γεγονότα που σχετίζονται με την κατάσταση της συσκευής. Οι έξυπνες κλειδαριές μπορούν να θεωρηθούν μέρος ενός έξυπνου σπιτιού.

Οι έξυπνες κλειδαριές, όπως και οι παραδοσιακές κλειδαριές, χρειάζονται δύο κύρια μέρη για να λειτουργήσουν: την κλειδαριά και το κλειδί. Στην περίπτωση των ηλεκτρονικών κλειδαριών, το κλειδί δεν είναι φυσικό κλειδί, αλλά ένα smartphone μία κάρτα ή ένα NFC tag διαμορφωμένο ρητά για το σκοπό αυτό, το οποίο εκτελεί ασύρματα τον έλεγχο ταυτότητας που απαιτείται για να ξεκλειδώσει αυτόματα την πόρτα.

Επιπλέον οι έξυπνες κλειδαριές επιτρέπουν στους χρήστες να παραχωρήσουν πρόσβαση σε τρίτο μέρος μέσω εικονικού κλειδιού. Αυτό το κλειδί μπορεί να σταλεί στο smartphone του παραλήπτη μέσω τυπικών πρωτοκόλλων ανταλλαγής μηνυμάτων όπως email ή SMS. Μόλις ληφθεί αυτό το κλειδί, ο παραλήπτης θα μπορεί να ξεκλειδώσει το έξυπνο κλείδωμα κατά το χρονικό διάστημα που είχε ορίσει ο αποστολέας. Ορισμένες έξυπνες κλειδαριές λειτουργούν με ένα έξυπνο κουδούνι και κάμερες για να επιτρέπουν στον χρήστη να δει ποιος και πότε κάποιος βρίσκεται στην πόρτα.

2.3 Smart Home Κίνδυνοι και Μέτρα Προστασίας

Για την υλοποίηση ενός συστήματος Smart Home και ειδικά ενός Smart Lock, το οποίο είναι ένα πολύ ευαίσθητο σύστημα, πρέπει να ληφθούν υπόψη οι διάφοροι κίνδυνοι που υπάρχουν έτσι ώστε να εφαρμοστούν τα κατάλληλα μέτρα προστασίας. Μερικές από τις σημαντικότερες επιθέσεις τις οποίες δέχονται τα σύγχρονα συστήματα Smart Home είναι οι εξής:

- Eavesdropping: Eavesdropping είναι όταν ο κάποιος παρακολουθεί παράνομα το traffic των δεδομένων που παράγονται ή χρησιμοποιούνται από τις συσκευές του έξυπνου σπιτιού. Τα δεδομένα αυτά ενδέχεται να περιέχουν πληροφορίες οι οποίες οι χρήστες να μην θέλουν να εκτίθενται σε μη εξουσιοδοτημένους χρήστες. Το eavesdropping είναι από τις πιο συνηθισμένες επιθέσεις σε συστήματα smart home.
- Masquerading: Masquerading ή αλλιώς μεταμφίεση είναι όταν ο attacker υποδύεται κάποιο άλλο άτομο το οποίο έχει εξουσιοδότηση σε οφέλη του συστήματος στα οποία κανονικά δεν θα είχε άδεια. Με τον τρόπο αυτό ο εισβολέας μπορεί να αποκτήσει πρόσβαση στο smart home network και μέσω αυτού να υποκλέψει μυστικά δεδομένα.

- Replay attack: Στο Replay Attack ο attacker αρχικά θα παρακολουθήσει την επικοινωνία των διάφορων συσκευών του smart home και θα αποθηκεύσει τα δεδομένα που μεταφέρονται. Στην συνέχεια θα ξαναστείλει τα δεδομένα αυτά στις διάφορες συσκευές σαν μια εξουσιοδοτημένη συσκευή με σκοπό να υποκλέψει εμπιστευτικές πληροφορίες είναι να χρησιμοποιήσει τις λειτουργίες κάποιας συσκευής.
- Message modification: Η τροποποίηση μηνυμάτων μπορεί να προκύψει όταν ένας εισβολέας στοχεύει να παραβιάσει την επικοινωνία μεταξύ δύο εξουσιοδοτημένων συσκευών με πρόθεση την κακόβουλης λειτουργίας κάποιας συσκευής ή αλλαγή τις τιμές σε μια πληροφορία.
- Denial of service (DoS): Με την επίθεση DoS ο attacker στοχεύει στο να κάνει ένα δίκτυο μη διαθέσιμο στους νόμιμους χρήστες του, να διακόψει την εσωτερική επικοινωνία των smart home συσκευών με το σύστημα και γενικότερα να μειώσει την προσβασιμότητα της υπηρεσίας του δικτύου. Αυτό επιτυγχάνεται με αποστολή μεγάλου όγκου μηνυμάτων από τον εισβολέα στο σύστημα Smart Home ώστε να επιβαρύνει υπερβολικά τις υπηρεσίες του.
- Injection attack: Το injection attack επιτυγχάνεται όταν υπάρχει κάποιο bug ή vulnerability στον κώδικα και ο attacker το εκμεταλλεύεται προσθέτοντας κακόβουλο κώδικα στο Smart Home σύστημα με αποτέλεσμα την δυσλειτουργία του ή την διαρροή εμπιστευτικών δεδομένων.

Όπως φαίνεται και πιο πάνω οι κίνδυνοι σε ένα Smart Home σύστημα είναι πολλοί. Οι κατασκευαστές Smart Home υπηρεσιών οφείλουν όμως να αναπτύσσουν συστήματα τα οποία να είναι ασφαλές και να μην διατρέχουν κανένα κίνδυνο. Μερικές από τις μεθόδους καταπολέμησης των κινδύνων είναι οι παρακάτω:

- Authentication: Πρέπει να γίνεται η ταυτοποίηση του χρήστη κάθε φορά που θα χρησιμοποιεί το σύστημα. Ο καλύτερος τρόπος για να γίνει αυτό είναι χρησιμοποιώντας τις 3 αρχές τις ταυτοποίησης:
 - Something you know: Κάτι που γνωρίζει ο χρήστης π.χ. ένα password.
 - Something you have: Κάτι που έχει στην κατοχή του ο χρήστης π.χ. μία smart card ή ένα smartphone.
 - Something you are: Κάτι που φανερώνει ποιος είναι ο χρήστης π.χ. fingerprint, face recognition.

- Authorization: Η μέθοδος αυτή υποδηλώνει ότι ο κάθε χρήστης θα έχει διαφορετικά δικαιώματα ανάλογα με την χρήση την οποία κάνει μέσα στο σύστημα. Για παράδειγμα ένας απλός χρήστης του smart home δεν θα έχει το δικαίωμα να αλλάζει το PIN της κεντρικής εισόδου, κάτι που ο administrator θα μπορεί. Με το τρόπο αυτό, σε περίπτωση που ο attacker καταφέρει να εισχωρήσει στο σύστημα να μην μπορεί να έχει διοικητικές λειτουργίες στο smart home.
- Secure communication (Encryption): Με την ασφαλή επικοινωνία και την κρυπτογράφηση εννοούμε ότι τα δεδομένα που μεταφέρονται μεταξύ των συσκευών πρέπει να είναι προστατευμένα έτσι ώστε μόνο ο σωστός παραλήπτης να μπορεί να τα διαβάσει χρησιμοποιώντας ένα μυστικό κλειδί. Κρυπτογράφηση πρέπει επίσης να υπάρχει και στις βάσεις δεδομένων όπου αποθηκεύονται ευαίσθητα στοιχεία όπως οι κωδικοί των χρηστών.
- Security monitoring and analysis: Με την παρακολούθηση και την ανάλυση ασφαλείας το σύστημα μπορεί να αναγνωρίσει κακόβουλες ή ακόμα και ύποπτες κινήσεις μέσα στο σύστημα. Το σύστημα τότε μπορεί αυτόματα να μπλοκάρει τους ύποπτους χρήστες ή να ενημερώσει τον διαχειριστή του συστήματος και με την σειρά του να αξιολογήσει την κατάσταση και να κάνει τις απαραίτητες ενέργειες.

Κεφάλαιο 3

Hardware & Software

3.1	Hardware	12
3.1.1	Raspberry Pi	12
3.1.2	PN532 NFC Module	16
3.1.3	Adafruit 16x2 LCD Pi Plate	17
3.1.4	3x4 Matrix Keypad	19
3.2	Software	19
3.2.1	Python	20
3.2.2	Node.js	21
3.2.3	MariaDB	22
3.2.4	Expo React Native	23

3.1 Hardware

Για την υλοποίηση του SmartLock έπρεπε πρώτα απ' όλα να επιλεγεί το Hardware που θα χρησιμοποιηθεί. Σε μια εποχή όπου η τεχνολογία έχει προχωρήσει και οι επιλογές είναι αμέτρητες έπρεπε να γίνει σωστή επιλογή με βάση των προδιαγραφών.

3.1.1 Raspberry Pi

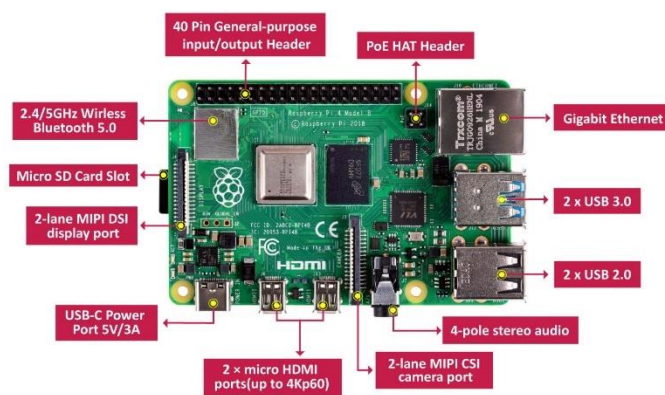
Για την κύρια μονάδα επεξεργασίας του συστήματος επιλέγηκε να χρησιμοποιηθεί το Raspberry Pi 4. Το Raspberry Pi είναι ένας μικρός υπολογιστής single-board ο οποίος κατασκευάζεται στο Ηνωμένο Βασίλειο από την Raspberry Pi Foundation σε συνεργασία με την Αμερικανική Broadcom. Αρχικός στόχος της Raspberry Pi Foundation ήταν να φτιάξει ένα φτηνό υπολογιστή για την εκμάθηση πληροφορικής στα

σχολεία. Πλέον το Raspberry Pi χρησιμοποιείται σε διάφορους τομείς λόγω της χαμηλής του τιμής σε σχέση με την υπολογιστική δύναμη που προσφέρει.

Η χαμηλή τιμή του Raspberry Pi, το μικρό μέγεθος σε σχέση με την υπολογιστική δύναμη που προσφέρει, η αυτονομία και η ευελιξία του ήταν οι κύριοι λόγοι επιλογής του. Τα κύρια χαρακτηριστικά του Raspberry Pi 4 (1GB RAM) φαίνονται στο παρακάτω σχεδιάγραμμα.

Figure 2

Τα μέρη του Raspberry Pi 4 Model B



Source: <https://www.seeedstudio.com/Raspberry-Pi-4-Computer-Model-B-4GB-p-4077.html>

Σχήμα 3.1: Τα μέρη του Raspberry Pi 4 Model B

Για την λειτουργία του Raspberry Pi έγινε εγκατάσταση του λειτουργικού συστήματος Raspbian OS που είναι και το official λογισμικό του Raspberry Pi και είναι βασισμένο πάνω στο Debian OS.

Στη συνέχεια περιγράφονται με λεπτομέρεια τα pins του Raspberry Pi που είναι υπεύθυνα για την επικοινωνία με τα υπόλοιπα εξαρτήματα του Smart Lock.

Figure 3
Τα pins του Raspberry Pi



Source: <https://www.open-electronics.org/raspberry-pi-gpio-pinout-learn-how-to-make-them-work/>

Σχήμα 3.2: Τα pins του Raspberry Pi

General Purpose Input Output (GPIO) Pins:

Τα GPIO pins είναι τα πιο βασικά και τα πιο ευκολά στη διαχείριση στο Raspberry Pi. Τα pins αυτά είναι digital δηλαδή έχουν δύο καταστάσεις on ή off. Η κατάσταση όσο και η κατεύθυνση, δηλαδή αν θα είναι input ή output μπορεί να καθοριστεί προγραμματιστικά με Python, JavaScript κλπ. Η τάση στα GPIO pins είναι 3,3v με μέγιστη ισχύ ρεύματος 16mA.

I2C - Inter-Integrated Circuit:

Το I2C είναι ένα σειριακό πρωτόκολλο δύο καλωδίων χαμηλής ταχύτητας για τη σύνδεση συσκευών χρησιμοποιώντας το πρότυπο I2C. Οι συσκευές που χρησιμοποιούν το πρότυπο I2C έχουν σχέση master-slave. Αυτό σημαίνει ότι μπορεί να υπάρχουν περισσότερα από ένα εξαρτήματα αλλά κάθε ένα από αυτά πρέπει να έχει μοναδική διεύθυνση, την οποία λαμβάνει ο κατασκευαστής από την NXP, παλαιότερα γνωστή ως Philips Semiconductors.

SPI - Serial Peripheral Interface:

Το SPI είναι ένα άλλο πρωτόκολλο για τη σύνδεση συμβατών συσκευών στο Raspberry Pi. Είναι παρόμοιο με το I2C στο ότι υπάρχει μια σχέση master-slave μεταξύ του Raspberry Pi και των συσκευών που είναι συνδεδεμένες σε αυτό. Η διάφορες του με το i2c είναι ότι είναι γρηγορότερο λόγω των start-stop bits του i2c αλλά για την χρήση περισσότερων εξαρτημάτων χρειάζεται περισσότερα pins και κώδικα.

UART - Universal Asynchronous Receiver / Transmitter:

Γνωστό και ως "Serial", τα pins UART (Transmit GPIO14, Receive GPIO15) παρέχουν μια σύνδεση στο console/terminal για headless setup, που σημαίνει σύνδεση στο Pi χωρίς πληκτρολόγιο ή mouse.

Ground (gnd):

Το GND είναι το σημείο από το οποίο μπορούν να μετρηθούν όλες οι τάσεις και συμπληρώνει επίσης ένα ηλεκτρικό κύκλωμα.

Pin 5v:

Τα pins 5v παρέχουν άμεση πρόσβαση στην τροφοδοσία 5v που προέρχεται από το power supply, λιγότερη ισχύ από ό, τι χρησιμοποιείται από το ίδιο το Raspberry Pi. Ένα Pi μπορεί να τροφοδοτείται απευθείας από αυτά τα pins και μπορεί επίσης να τροφοδοτεί άλλες συσκευές 5v.

Pin 3v3:

Το pin 3v υπάρχει για να προσφέρει σταθερή τροφοδοσία 3.3v στα εξαρτήματα τροφοδοσίας και για δοκιμή LED.

3.1.2 PN532 NFC Module

Η λειτουργική μονάδα Raspberry Pi PN532 NFC, όπως υποδηλώνει το όνομά της, βασίζεται στο chip PN532 και χρησιμοποιείται για επικοινωνία πεδίου 13,56 MHz. Αυτή η μονάδα είναι εξοπλισμένη με ενσωματωμένη κεραία, οπότε δεν υπάρχει εξωτερικό πηνίο κεραίας. Είναι συμβατό με διασυνδέσεις SPI, I2C για επικοινωνία. Με την υποστήριξη της βιβλιοθήκης NFC, το Raspberry Pi μπορεί να χρησιμοποιήσει εύκολα τις λειτουργίες του NFC.

Η διασύνδεση που χρησιμοποιήθηκε για την επικοινωνία του Raspberry Pi με το PN532 ήταν I2C επειδή χρησιμοποιούσε μόνο 4 pins στο Pi. Για να ρυθμιστεί η επικοινωνία σε i2c έπρεπε τα δύο switches SET0 και SET1 να ρυθμιστούν σε H και L αντίστοιχα. Τα pins που χρησιμοποιήθηκαν στο Pi ήταν 5V, GND, SDA, SCL τα οποία ενώθηκαν με τα αντίστοιχα πάνω στο NFC chip.

Η βιβλιοθήκη που χρειάστηκε να εγκατασταθεί στο Raspberry Pi για να μπορεί να προγραμματιστεί και να λειτουργήσει το chip ήταν η libnfc.

Figure 4
PN532 NFC Module



Source: http://wiki.sunfounder.cc/index.php?title=PN532_NFC_Module_for_Raspberry_Pi

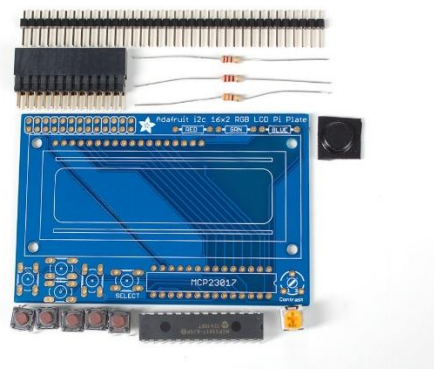
Σχήμα 3.3: Το PN532 NFC Module

3.1.3 Adafruit 16x2 LCD Pi Plate

Η πλακέτα αυτή υποστηρίζει μια οθόνη LCD 16x2 χαρακτήρων και 5 keypad κουμπιά. Για την ένωση του με το Raspberry Pi χρησιμοποιεί την επικοινωνία i2c και χρειάζεται 4 pins 5V, GND, SDA, SCL.

Η πλακέτα δεν έρχεται συναρμολογημένη out of the box. Αρχικά έπρεπε να γίνει η συναρμολόγηση και η συνένωση των διαφόρων εξαρτημάτων πάνω στην πλακέτα.

Figure 5
Εξαρτήματα LCD πλακέτας 16x2



Source: <https://learn.adafruit.com/adafruit-16x2-character-lcd-plus-keypad-for-raspberry-pi/parts-list>

Σχήμα 3.4: Τα Εξαρτήματα της LCD πλακέτας 16x2

Τα εξαρτήματα που έρχονται μαζί με την πλακέτα είναι: 3 αντιστάσεις 200ohm, ένα ποτενσιόμετρο για την ρύθμιση του contrast, 5 κουμπιά, το chip MCP23017, Male Header Pins για την ένωση της οθόνης LCD με την πλακέτα, Raspberry Pi Plate Header για την ένωση της πλακέτας με το Raspberry Pi και ένα rubber bumper.

Για την λειτουργία του μέσω της python χρειάζεται τις απαραίτητες βιβλιοθήκες από τον κατασκευαστή Adafruit.

Figure 6
Adafruit 16x2 LCD Pi Plate



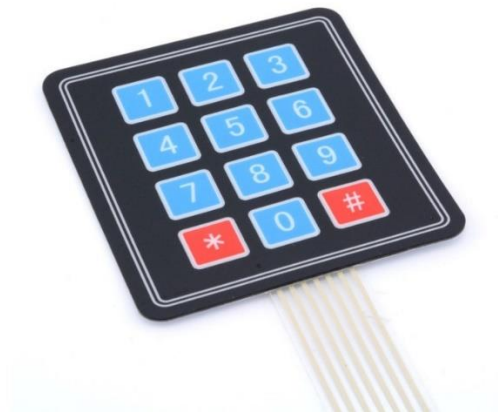
Source: <https://www.adafruit.com/product/1115>

Σχήμα 3.5: Η οθόνη Adafruit 16x2 LCD

3.1.4 3x4 Matrix Keypad

Το keypad έχει 12 πλήκτρα διαρρυθμισμένα σε 3 στήλες και 4 γραμμές. Για τον λόγο αυτό χρειάζεται 7 GPIO pins (1 GPIO pin για κάθε γραμμή ή στήλη). Για την λειτουργία του μέσω της python χρειάζεται τις απαραίτητες βιβλιοθήκες από τον κατασκευαστή Adafruit.

Figure 7
3x4 Matrix Keypad



Source: <https://www.kiwi-electronics.nl/adafruit/adafruit-components-parts/3x4-flexibel-matrix-keypad?lang=en>

Σχήμα 3.6: Το 3x4 Matrix Keypad

3.2 Τεχνολογίες - Software

Για την υλοποίηση του backend όσο και του frontend έπρεπε να γίνει σωστή επιλογή τεχνολογιών software που θα χρησιμοποιούνταν. Η επιλογή του παρακάτω software έγινε επειδή κυρίως εξυπηρετούσε τον σκοπό που θα χρησιμοποιούταν και επιπλέον είναι αξιόπιστο, ασφαλές, σύγχρονο και υπάρχει ευρεία υποστήριξη από διάφορα communities.

3.2.1 Python

Για τον κύριο προγραμματισμό του backend χρησιμοποιήθηκε η γλώσσα Python και πιο συγκεκριμένα η έκδοση 3.7.3. Η python είναι μια υψηλού επιπέδου γλώσσα γενικής χρήσης. Η φιλοσοφία σχεδιασμού της Python δίνει έμφαση στην αναγνωσιμότητα του κώδικα και η αντικειμενοστρεφής προσέγγιση της στοχεύει στο να βοηθήσει τους προγραμματιστές να γράψουν σαφή και λογικό κώδικα για μικρά και μεγάλα projects.

Η Python δημιουργήθηκε στα τέλη της δεκαετίας του 1980 και κυκλοφόρησε για πρώτη φορά το 1991 από τον Guido van Rossum ως διάδοχο της γλώσσας προγραμματισμού ABC. Η Python 2.0, που κυκλοφόρησε το 2000, εισήγαγε νέες δυνατότητες, όπως λίστες και garbage collector και διακόπηκε με την έκδοση 2.7 το 2020. Η Python 3.0, που κυκλοφόρησε το 2008, ήταν μια σημαντική αναθεώρηση της γλώσσας που δεν είναι backwards compatible με την Python 2.0, το ίδιο και με τον κώδικα της Python 2.0 ο οποίος δεν εκτελείται χωρίς τροποποίηση στην Python 3.0. Με το τέλος της ζωής της Python 2.0, μόνο η Python 3.6.x και αργότερα υποστηρίζονται, με παλαιότερες εκδόσεις να υποστηρίζουν π.χ. Windows 7 (και παλιά προγράμματα εγκατάστασης που δεν περιορίζονται σε Windows 64-bit).

Ένα από το μεγαλύτερα όπλα της Python είναι το τεράστιο εύρος βιβλιοθηκών που προσφέρει στους προγραμματιστές. Τον Νοέμβριο του 2019, το επίσημο repository third party Python software PyPI, περιείχε περισσότερα από 200.000 packages για διάφορες λειτουργίες όπως Automation, Data analytics, Databases και πολλά άλλα.

Figure 8
Python logo



Source: <https://www.python.org/community/logos/>

Σχήμα 3.7: Το Python logo

3.2.2 Node.js

Η node.js είναι μια γλώσσα προγραμματισμού ανοιχτού κώδικα που χρησιμοποιείται κυρίως για backend εφαρμογές αφού επιτρέπει την εκτέλεση κώδικα JavaScript εκτός Web Browser. Με τον τρόπο αυτό αντιπροσωπεύει ένα παράδειγμα του «JavaScript Everywhere» αφού για την ανάπτυξη εφαρμογών ιστού χρησιμοποιείται μόνο μια γλώσσα προγραμματισμού, η JavaScript, τόσο server-side όσο και client-side.

Η node.js δημιουργήθηκε από τον Ryan Dahl το 2009, 13 χρόνια μετά από το πρώτο server-side JavaScript environment, το Netscape's LiveWire Pro Web. Η πρώτη έκδοση της node.js υποστηριζόταν μόνο από Linux και MAC OS X, ενώ αργότερα σε συνεργασία με την Microsoft δημιουργήθηκε η node.js για Windows.

Τον Ιανουάριο του 2010 έγινε η εισαγωγή του package manager npm. Ο package manager επιτρέπει στους προγραμματιστές να δημοσιοποιούν και να μοιράζονται εύκολα κώδικα βιβλιοθηκών. Επιπλέον με την χρήση του npm απλοποιείται η εγκατάσταση, η αναβάθμιση και η απεγκατάσταση βιβλιοθηκών της node.js.

Η node.js χρησιμοποιείται κυρίως για την ανάπτυξη εφαρμογών διαδικτύου όπως για παράδειγμα Web Servers και networking tools με την χρήση διαφόρων modules τα οποία μπορούν να έχουν διάφορες λειτουργίες. Μερικές από τις λειτουργίες που προσφέρουν τα modules είναι file system I/O, networking (DNS, HTTP, TCP, TLS/SSL, UDP), μεθόδους κρυπτογραφίες και πολλά άλλα. Τα modules αυτά χρησιμοποιούν API σχεδιασμένο έτσι ώστε να απλοποιεί την ανάπτυξη server application.

Figure 9
Node.js logo



Source: <https://nodejs.org/en/about/resources/>

Σχήμα 3.8: Το Node.js logo

3.2.3 MariaDB

Η MariaDB είναι ένα σύστημα σχεσιακής διαχείρισης βάσεων δεδομένων η οποία προέρχεται από την MySQL. Η MariaDB σε αντίθεση με την MySQL είναι ανοιχτού κώδικα και δωρεάν κάτω από το GNU General Public License. Η ανάπτυξη της γίνεται από τους αρχικούς προγραμματιστές της MySQL οι οποίοι την διέδωσαν λόγω ανησυχιών για την απόκτηση της από την Oracle Corporation το 2009.

Τα κύρια features που χαρακτηρίζουν την MariaDB σε σχέση με άλλους διαχειριστές βάσεων δεδομένων εκτός από το ότι είναι δωρεάν είναι ότι υποστηρίζεται από διάφορα λειτουργικά συστήματα και γλώσσες προγραμματισμού, είναι εύκολη στην δημιουργία των queries, χρησιμοποιεί την λογική του σχεσιακού μοντέλου και είναι γρήγορη στην λειτουργία της.

Figure 10
MariaDB logo



Source: <https://www.rootusers.com/how-to-install-and-configure-mariadb/mariadb-logo-2/>

Σχήμα 3.9: Το MariaDB logo

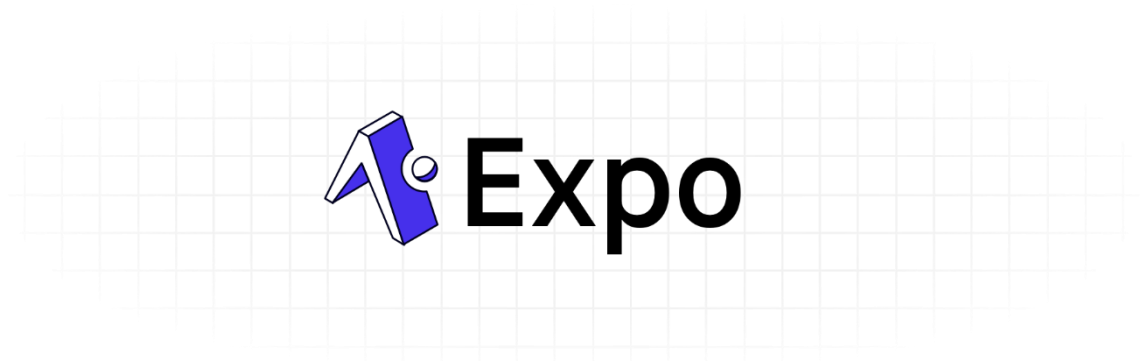
3.2.4 Expo React Native

Το Expo είναι ένα framework και μια πλατφόρμα ανάπτυξης για εφαρμογές React ανεξάρτητα από το λειτουργικό σύστημα. Αυτό σημαίνει ότι ο προγραμματιστής γράφει ένα κώδικα JavaScript / TypeScript και το expo είναι υπεύθυνο να μεταφράσει τον κώδικα αυτό έτσι ώστε να είναι compatible με οποιοδήποτε λειτουργικό σύστημα.

Το expo χρησιμοποιήθηκε για την ανάπτυξη του λογισμικού για android συσκευές. Οι λόγοι που προτιμήθηκε αντί του android studio και της plain react native είναι οι εξής:

- Η ανάπτυξη κώδικα React Native είναι γρηγορότερη και ευκολότερη σε σχέση με τον κώδικα Android.
- Ο ίδιος κώδικας σε React Native μπορεί να υποστηριχθεί σε Android, iOS ή ακόμα και σε ένα Web Browser.
- Οι αλλαγές στον κώδικα εμφανίζονται άμεσα στο application χωρίς να χρειάζεται rebuild κάθε φορά του application, κάτι που γλιτώνει πολλή χρόνο στον προγραμματιστή και επιτρέπει τον πειραματισμό στον κώδικα.
- Υπάρχουν υλοποιημένες διάφορες βιβλιοθήκες που βοηθούν τους προγραμματιστές σε διάφορες λειτουργίες όπως Camera, file system, location, push notifications και άλλα.

Figure 11
Expo React Native logo



Source: <https://yarnpkg.com/package/expo-splash-screen>

Σχήμα 3.10: Το Expo React Native logo

Κεφάλαιο 4

Προδιαγραφές και υλοποίηση

4.1	Προδιαγραφές συστήματος	24
4.2	Υλοποίηση συστήματος	25
4.2.1	Εγκατάσταση συστήματος.	27
4.2.2	Διεπαφή φυσικής παρουσίας.	28
4.2.3	Διεπαφή smartphone εφαρμογής.	32

4.1 Προδιαγραφές συστήματος

Η υλοποίηση ενός συστήματος Smart Home μπορεί αρχικά να φαίνεται απλή σαν ιδέα, αλλά στην πραγματικότητα κρύβει αρκετές δυσκολίες. Για τον λόγο αυτό έπρεπε αρχικά να καθοριστούν κάποιες προδιαγραφές βάση των οποίων να αναπτυχθεί το σύστημα, έτσι ώστε το τελικό προϊόν να μπορεί να συγκριθεί με υπάρχουσες εφαρμογές Smart Home.

Οι Προδιαγραφές του συστήματος Smart Home περιγράφονται παρακάτω:

- Απλό και εύκολο στην χρήση: Οι Smart Home συσκευές χρησιμοποιούνται για να κάνουν εύκολη τη ζωή των ανθρώπων. Αυτό πρέπει να ισχύει και στο σύστημα μας. Πρέπει οι οθόνες και οι λειτουργίες να είναι αυτοεπεξηγηματικές στον χρήστη χωρίς άσκοπες πληροφορίες και κουμπιά. Αφού το σύστημα θα αντικαταστήσει την λειτουργία ξεκλειδώματος της κύριας εισόδου πρέπει ο χρήστης με την εγκατάσταση του συστήματος να μπορεί να χρησιμοποιεί όλες τις βασικές λειτουργίες δηλαδή το άνοιγμα και το κλείσιμο της πόρτας.
- Γρήγορο: Το έξυπνο σύστημα ξεκλειδώματος της πόρτας πρέπει να βελτιώνει την παραδοσιακή μέθοδο του ξεκλειδώματος με κλειδί. Αυτό θα επιτευχθεί μόνο αν η νέα μέθοδος ξεκλειδώματος γίνεται όσο γρήγορα και seamless όσο αυτή του κλειδιού.

Με άλλα λόγια, με το νέο σύστημα θέλουμε ο χρήστης να μπορεί να ξεκλειδώσει την πόρτα σε χρόνο τουλάχιστον τον ίδιο με αυτό που χρειάζεται ένας μέσος άνθρωπος για να ψάξει να βρει το κλειδί του και να ξεκλειδώσει την πόρτα.

- Ασφάλεια και Προστασία Δεδομένων: Το σύστημα αφορά το ξεκλείδωμα πόρτας σπιτιού κάτι που καθιστά το σύστημα πολύ ευαίσθητο αφού το σπίτι είναι το πολυτιμότερο αγαθό του ανθρώπου και δεν πρέπει σε καμία περίπτωση κάποιος ανεπιθύμητος να μπορεί να έχει πρόσβαση σ' αυτό. Για τον λόγο αυτό, το τελικό προϊόν δεν πρέπει σε καμία περίπτωση να έχει θέματα όσον αφορά την ασφάλεια και θα πρέπει να ακολουθεί τα κατάλληλα πρωτόκολλα ασφαλείας διαδικτυακών εφαρμογών.
- Επιλογή των σωστών υλικών και εργαλείων: Το Hardware όσο και το Software που θα χρησιμοποιηθεί θα πρέπει να είναι σύγχρονο και να συμβαδίζει με τις τεχνολογίες που υπάρχουν ήδη στην αγορά και να είμαστε σίγουροι για την αξιοπιστία τους. Επιπλέον θα πρέπει να επιτρέπουν την αναβάθμιση, διόρθωση λαθών και επεκτασιμότητα έτσι ώστε το σύστημα να αντέχει στον χρόνο.

4.2 Υλοποίηση συστήματος

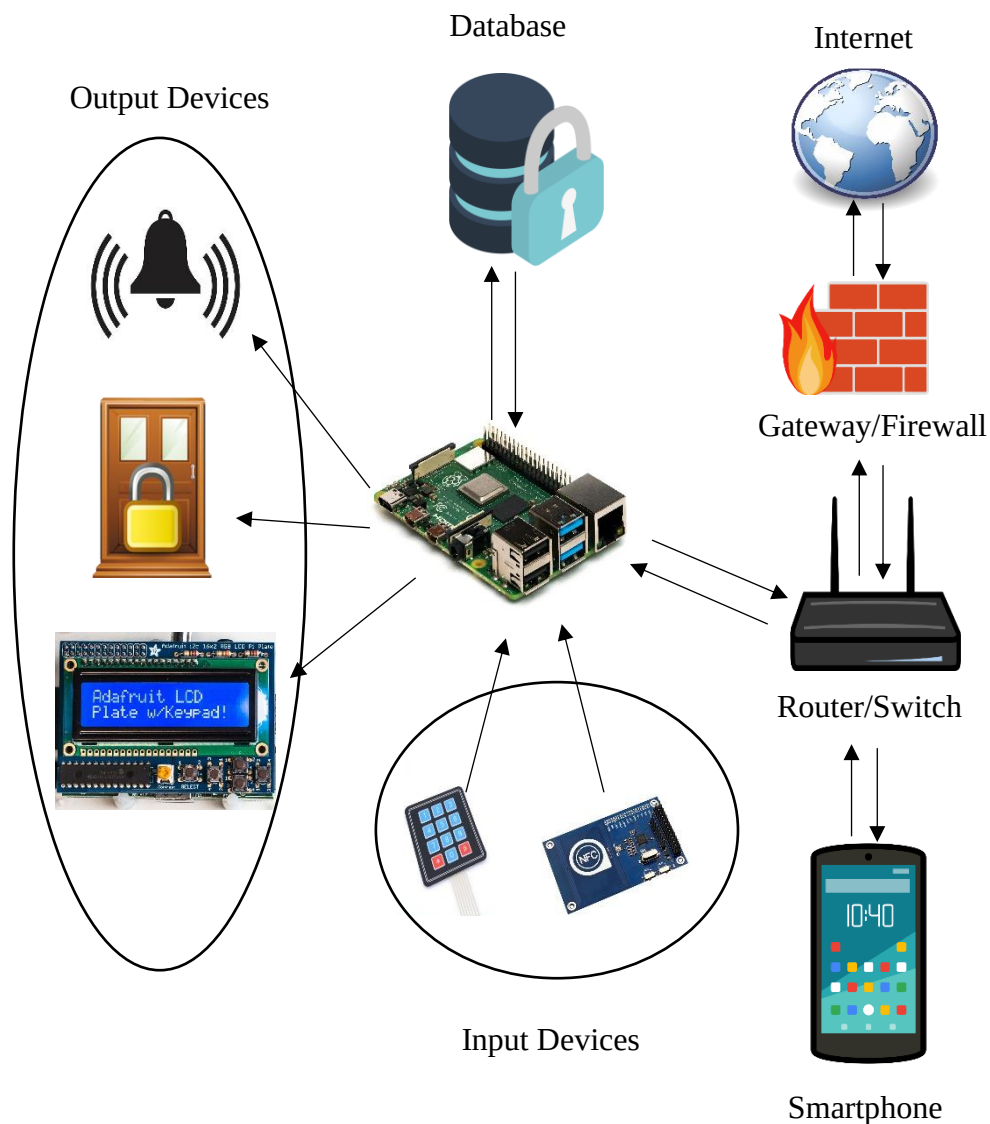
Στη συνέχεια θα ακολουθήσει λεπτομερής επεξήγηση των λειτουργιών και της υλοποίησης του συστήματος. Αρχικά πρέπει να γίνει αναφορά στα δύο μέρη του συστήματος τα οποία είναι το backend και το frontend. Το backend ουσιαστικά είναι ο εγκέφαλος και ο συντονιστής όλων των λειτουργιών του συστήματος. Το backend τρέχει πάνω στο Raspberry Pi και ο κώδικας είναι γραμμένος κυρίως σε Python 3.7.3 και node.js. Το frontend είναι η κύρια διεπαφή μέσω της οποίας ένα απλός χρήστης θα μπορεί να εκτελεί τις λειτουργίες του Smart Home. Ο κώδικας frontend είναι υλοποιημένος σε React Native χρησιμοποιώντας το expo framework και μπορεί να τρέξει σε Android και iOS εφαρμογές ή ακόμα και στον browser του υπολογιστή και επίσης σε Python για την διεπαφή χρησιμοποιώντας την LCD οθόνη και το numpad.

Η προσέγγιση με την οποία ολόκληρο το project υλοποιήθηκε είναι σχετικά απλή. Το Raspberry Pi είναι η κεντρική μονάδα επεξεργασίας του συστήματος και είναι ενωμένο με τις διάφορες συσκευές: LCD οθόνη, numpad, NFC receiver, κλειδαριά (LED) και ηχητικός συναγερμός (buzzer). Το Raspberry Pi επίσης είναι υπεύθυνο για την επικοινωνία με το database στο οποίο είναι αποθηκευμένα τα δεδομένα των χρηστών και

οι διάφοροι κωδικοί κρυπτογραφημένοι. Οι μέθοδοι κρυπτογραφίας που εφαρμόστηκαν ήταν AES-128 όπου χρειαζόταν συμμετρική κρυπτογραφία και SHA-512 για το hashing των κωδικών. Επιπλέον το Raspberry Pi είναι ενωμένο στο δίκτυο του σπιτιού μέσω ethernet ή Wi-Fi επιτρέποντας την επικοινωνία μαζί με το smartphone και το διαδίκτυο για επιπλέον λειτουργίες όπως το one time password χρησιμοποιώντας το Google Authenticator. Όλα τα validations των κωδικών γίνονται από το Raspberry Pi και όλες οι επικοινωνίες είναι κρυπτογραφημένες.

Figure 12

Σχεδιάγραμμα επικοινωνίας συσκευών



Σχήμα 4.1: Σχεδιάγραμμα επικοινωνίας συσκευών

4.2.1 Εγκατάσταση συστήματος

Η εγκατάσταση του συστήματος είναι σχετικά απλή αλλά είναι προτιμότερο να γίνει από κάποιο άτομο με βασική γνώση στα Linux και το command-line terminal. Αρχικά πρέπει να γίνει η συνδεσμολογία του Raspberry Pi με τις διάφορες συσκευές. Η συσκευές που έχουμε μέχρι στιγμής στο Smart Home σύστημα μας είναι η LCD οθόνη, το numpad, το NFC chip και ένα board με την κλειδαριά (LED) και ένα buzzer. Ο τρόπος με τον οποίο συνδέονται στο Raspberry επεξηγείτε αναλυτικά στο κεφάλαιο 3.1. Επιπλέον το Raspberry θα πρέπει να ενωθεί στο ρεύμα με τον μετασχηματιστή 5V και την θύρα usb type C. Τέλος το Raspberry Pi θα πρέπει να ενωθεί στο δίκτυο του σπιτιού μέσω ethernet ή Wi-Fi. Το σύστημα μπορεί να λειτουργήσει χωρίς σύνδεση στο διαδίκτυο (εκτός την λειτουργία one time password η οποία χρησιμοποιεί τον Google Authenticator αλλά μπορεί εύκολα να αντικατασταθεί με μια τοπική μέθοδο ελέγχου για one time password.). Για την επικοινωνία του συστήματος με smartphones εκτός του τοπικού δικτύου πρέπει να γίνουν οι απαραίτητες ρυθμίσεις στο gateway για άνοιγμα των απαραίτητων πορτών, το λεγόμενο port forwarding. Για λόγους ασφαλείας δεν προτείνεται το port forwarding και συνίσταται η χρήση VPN.

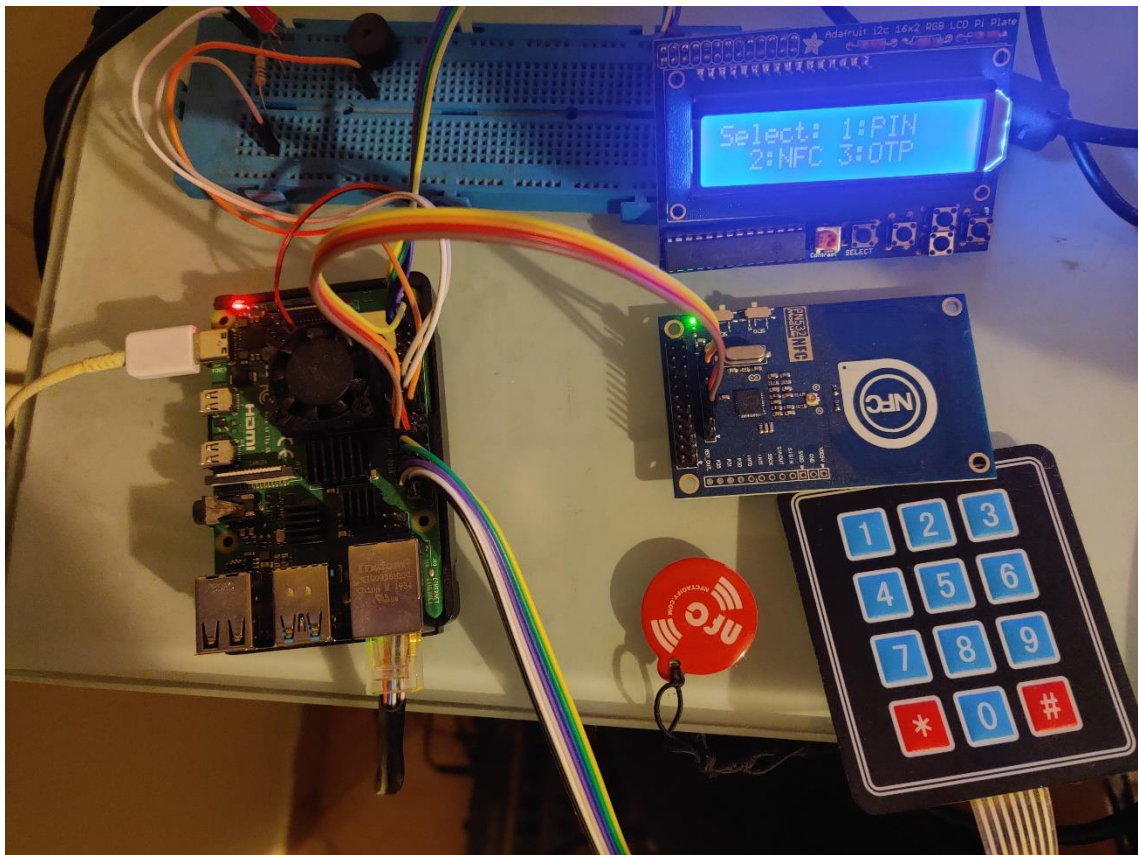
Υπάρχουν μικρά προγράμματα προεγκατεστημένα στο Raspberry Pi για τον έλεγχο της λειτουργίας της κάθε συσκευής τα οποία είναι προτιμότερο να τα τρέξει ο διαχειριστής πριν την εγκατάσταση ολόκληρου του συστήματος. Η χρήση του Raspberry Pi και των προγραμμάτων του μπορεί να γίνει με διάφορους τρόπους:

- Χρήση του command line terminal ενώνοντας μια οθόνη στο micro HDMI port και ένα keyboard στο USB port.
- Χρήση του GUI ενώνοντας μια οθόνη στο micro HDMI port και keyboard και mouse στα USB ports.
- Χρήση του SSH με την μόνη προϋπόθεση ότι το Raspberry Pi είναι συνδεδεμένο στο δίκτυο.

Αφού έγινε η εγκατάσταση του συστήματος και ο έλεγχος των εξαρτημάτων θα προχωρήσουμε στην ανάλυση των κυρίων λειτουργιών του συστήματος. Οι κύριες λειτουργίες του συστήματος χωρίζονται σε δύο διεπαφές:

- Διεπαφή φυσικής παρουσίας: Όπου ο χρήστης βρίσκεται έξω από την πόρτα και θα χρησιμοποιήσει το numpad την LCD οθόνη και το NFC receiver για να ξεκλειδώσει την πόρτα.
- Διεπαφή smartphone εφαρμογής: Όπου ο χρήστης δεν βρίσκεται απαραίτητα έξω από την πόρτα και μπορεί να την ξεκλειδώσει μέσω του κινητού τηλεφώνου.

Figure 13
Το σύστημα Smart Lock



Σχήμα 4.2: Σχεδιάγραμμα επικοινωνίας συσκευών

4.2.2 Διεπαφή φυσικής παρουσίας

Η διεπαφή φυσικής παρουσίας προϋποθέτει ότι ο χρήστης βρίσκεται έξω από την πόρτα και πρόκειται να χρησιμοποιήσει την LCD οθόνη, το numpad και το NFC receiver για να την ξεκλειδώσει. Οι τρόποι με τους οποίους μπορεί να ξεκλειδώσει την πόρτα είναι οι εξής:

Ξεκλείδωμα μέσω του κωδικού PIN:

Ο χρήστης από την κύρια διεπαφή θα πρέπει να επιλέξει τον αριθμό 1 χρησιμοποιώντας το numpad. Στην επόμενη διεπαφή που θα εμφανιστεί ο χρήστης καλείται χρησιμοποιώντας και πάλι το numpad να πληκτρολογήσει τον μυστικό κωδικό PIN.

Figure 14

Χρήση της μεθόδου ξεκλειδώματος μέσω κωδικού PIN



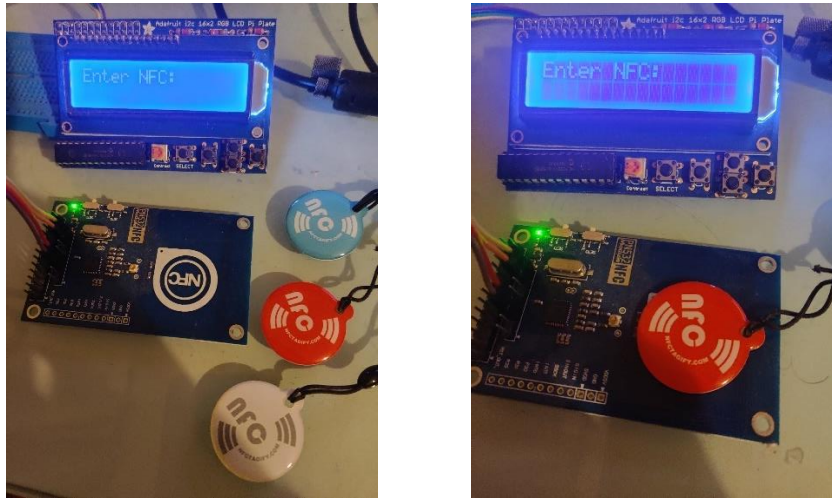
Σχήμα 4.3: Χρήση της μεθόδου ξεκλειδώματος μέσω κωδικού PIN

Ξεκλείδωμα μέσω του NFC receiver:

Ο χρήστης από την κύρια διεπαφή θα πρέπει να επιλέξει τον αριθμό 2 χρησιμοποιώντας το numpad. Στην επόμενη διεπαφή που θα εμφανιστεί ο χρήστης καλείται να τοποθετήσει ένα valid NFC tag ή το smartphone του κοντά στο NFC receiver.

Figure 15

Χρήση της μεθόδου ξεκλειδώματος μέσω NFC



Σχήμα 4.4: Χρήση της μεθόδου ξεκλειδώματος μέσω NFC

Ξεκλείδωμα μέσω του One Time Password (OTP):

Ο χρήστης από την κύρια διεπαφή θα πρέπει να επιλέξει τον αριθμό 3 χρησιμοποιώντας το numpad. Στην επόμενη διεπαφή που θα εμφανιστεί ο χρήστης καλείται χρησιμοποιώντας και πάλι το numpad να πληκτρολογήσει τον μυστικό κωδικό OTP.

Figure 16

Χρήση της μεθόδου ξεκλειδώματος μέσω του OTP

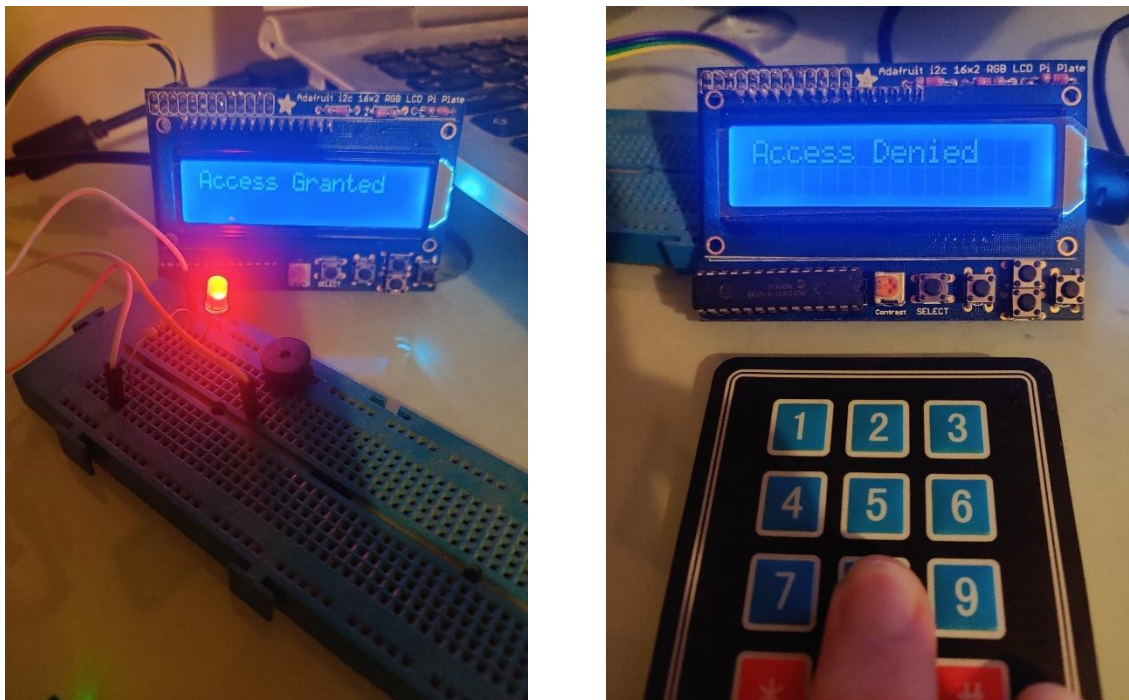


Σχήμα 4.5: Χρήση της μεθόδου ξεκλειδώματος μέσω του OTP

Μετά από κάθε επιτυχημένο ξεκλείδωμα εμφανίζεται το μήνυμα “Access Granted” πάνω στην οθόνη, και ανάβει η LED η οποία αντιπροσωπεύει το ξεκλείδωμα της πόρτας. Στην αντίθετη περίπτωση που ο χρήστης πληκτρολογήσει λανθασμένο PIN ή OTP ή τοποθετήσει μη εξουσιοδοτημένο NFC tag τότε εμφανίζεται το μήνυμα “Access Denied” στην οθόνη και ακούγεται ένας χαρακτηριστικός ήχος από το buzzer.

Figure 17

Παράδειγμα επιτυχημένης και αποτυχημένης προσπάθειας ξεκλειδώματος



Σχήμα 4.6: Παράδειγμα επιτυχημένης και αποτυχημένης προσπάθειας ξεκλειδώματος

Τέλος σε περίπτωση πολλαπλών αποτυχημένων προσπαθειών ο χρήστης μπλοκάρεται για ένα μικρό χρονικό διάστημα και ειδοποιείται ο διαχειριστής του συστήματος μέσω notification στο smartphone του.

Figure 18
Παράδειγμα timeout



Σχήμα 4.7: Παράδειγμα timeout

4.2.3 Διεπαφή smartphone εφαρμογής

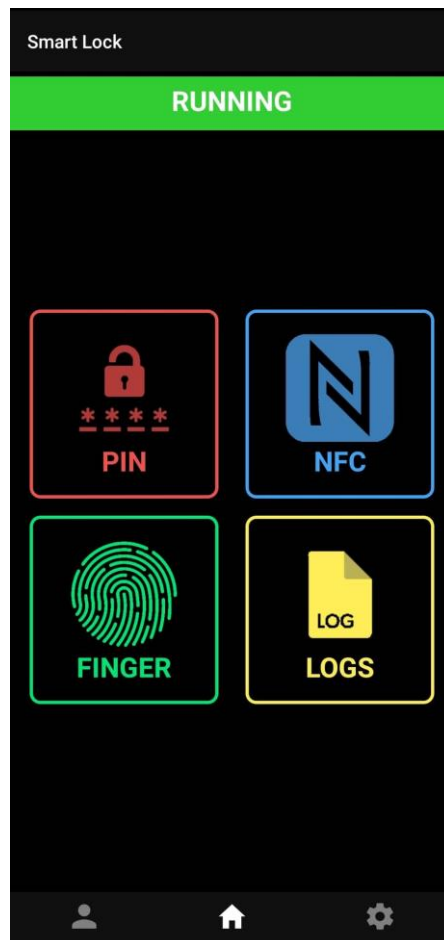
Η διεπαφή smartphone εφαρμογής επιτρέπει στον χρήστη να ξεκλειδώσει την πόρτα από οπουδήποτε χωρίς να βρίσκεται κοντά στο numpad ή το NFC receiver. Επίσης επιτρέπει την χρήση του fingerprint του NFC του smartphone αντί NFC tag. Τέλος, επιτρέπει την παρακολούθηση προσπαθειών ξεκλειδώματος είτε επιτυχημένες είτε αποτυχημένες και μπορεί να λαμβάνει notifications μετά από πολλαπλές λανθασμένες προσπάθειες.

Για να μπορεί να γίνει η χρήση του application πρέπει πρώτα να εγγραφεί στη βάση δεδομένων χρησιμοποιώντας ένα username και ένα password. Τότε θα έχει το δικαίωμα χρήσης του application.

Η κύρια διεπαφή του Smart Home Application φαίνεται στο παρακάτω σχήμα:

Figure 19

Κύρια διεπαφή Smarthome Application



Σχήμα 4.8: Κύρια διεπαφή Smarthome Application

Στην κύρια διεπαφή όπως φαίνεται και από την εικόνα διακρίνουμε τις βασικές λειτουργίες του application οι οποίες είναι ή εισαγωγή του κωδικού PIN, η χρήση του NFC και του fingerprint για το ξεκλείδωμα της πόρτας και η προβολή των logs.

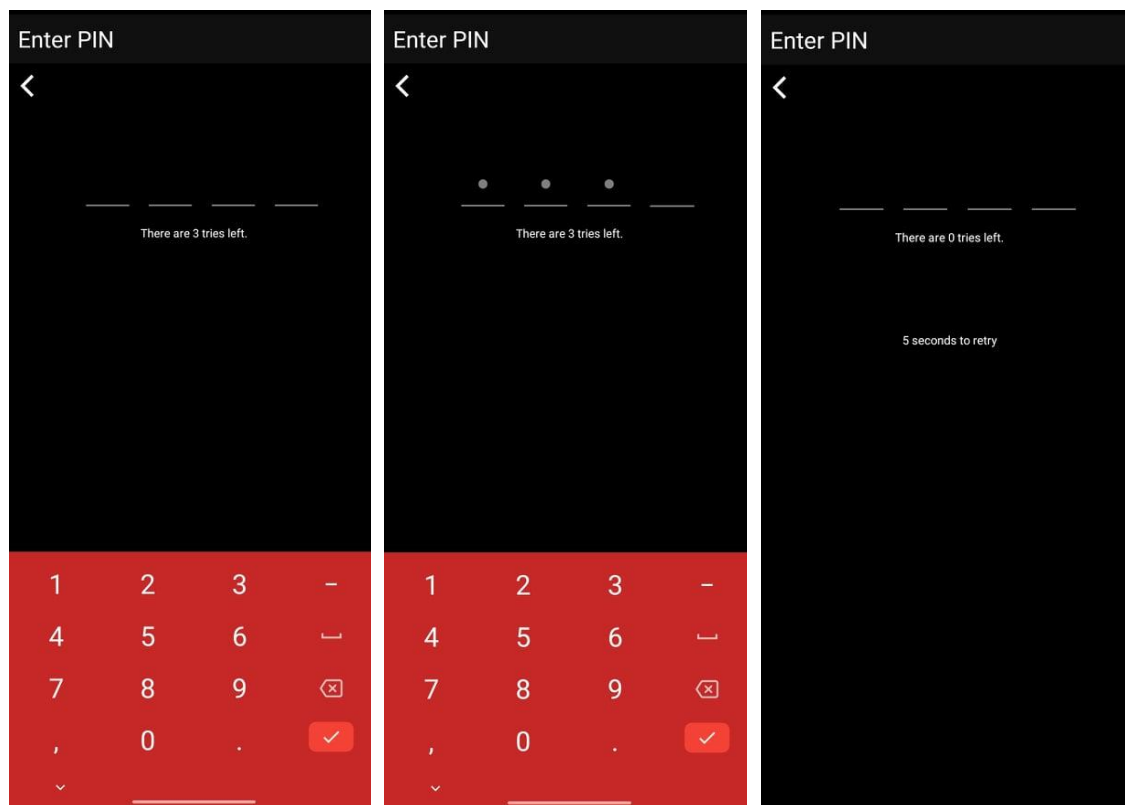
Ξεκλείδωμα με την εισαγωγή PIN:

Το ξεκλείδωμα με την εισαγωγή PIN γίνεται με όμοιο τρόπο όπως αυτόν με φυσική παρουσία. Επιλέγοντας το εικονίδιο PIN από την κύρια διεπαφή ο χρήστης στην επόμενη διεπαφή καλείται να πληκτρολογήσει τον κωδικό PIN. Όπως και με την μέθοδο της φυσικής παρουσίας μετά από 3 αποτυχημένες προσπάθειες ο χρήστης

μπλοκάρεται και πρέπει να περιμένει 30 δευτερόλεπτα για να ξαναπροσπαθήσει. Ταυτόχρονα ειδοποιείται και ο διαχειριστής του συστήματος.

Figure 20

Παράδειγμα ξεκλειδώματος με την εισαγωγή PIN μέσω του application



Σχήμα 4.9: Παράδειγμα ξεκλειδώματος με την εισαγωγή PIN μέσω του application

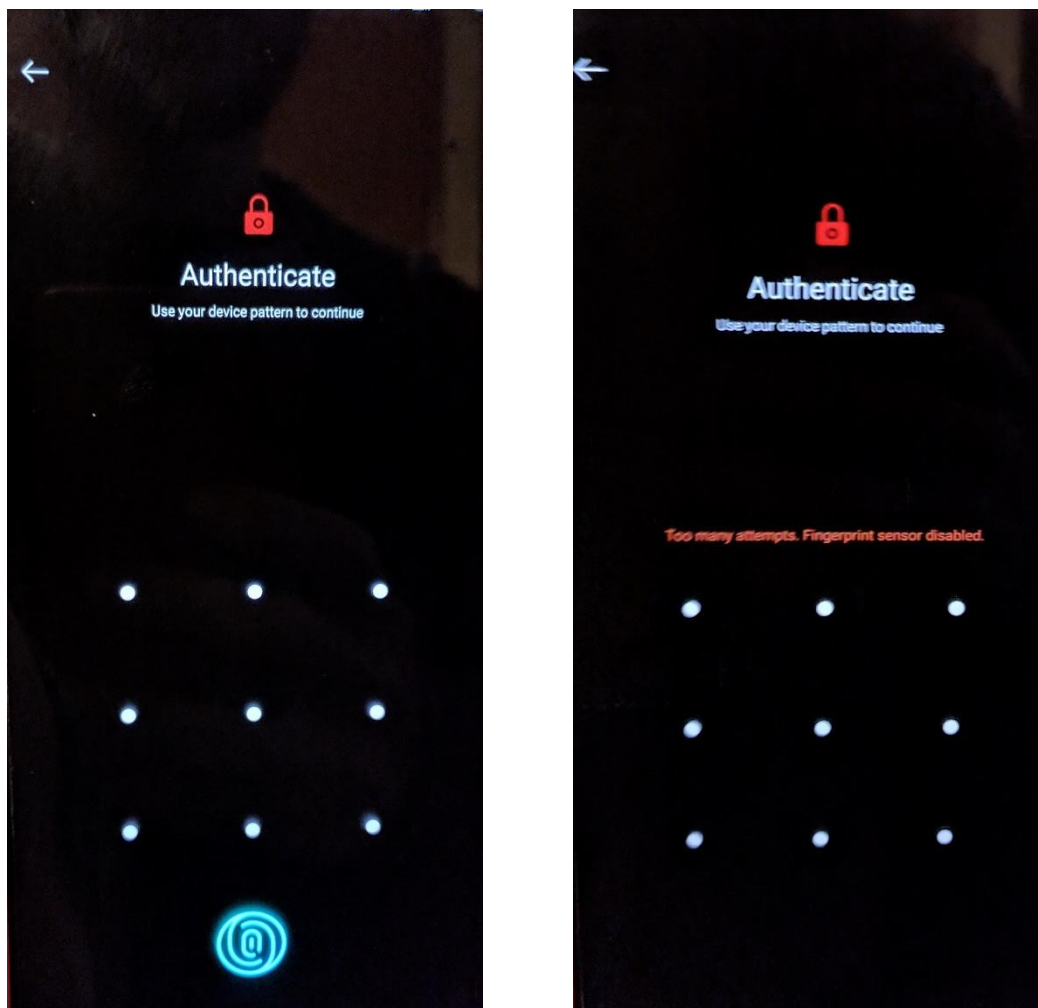
Ξεκλείδωμα μέσω δακτυλικού αποτυπώματος:

Με την επιλογή για ξεκλείδωμα με fingerprint το application χρησιμοποιεί την μέθοδο ταυτοποίησης με fingerprint όπως χρησιμοποιείται από το σύστημα του smartphone. Δηλαδή χρησιμοποιεί τα δεδομένα που έχουν γίνει στο setup του fingerprint μέσα από το λειτουργικό σύστημα. Η λειτουργία αυτή μπορεί να χρησιμοποιηθεί και σε συνδυασμό με μία από τις άλλες μεθόδους για περαιτέρω ασφάλεια ή ακόμα και για το άνοιγμα της εφαρμογής. Μετά από πολλαπλές λανθασμένες προσπάθειες το λειτουργικό σύστημα μπλοκάρει εντελώς την χρήση

fingerprint και επιτρέπει μόνο την χρήση του pattern ή pin που έγινε στο setup της συσκευής.

Figure 21

Παράδειγμα ξεκλειδώματος μέσω δακτυλικού αποτυπώματος



Σχήμα 4.10: Παράδειγμα ξεκλειδώματος μέσω δακτυλικού αποτυπώματος

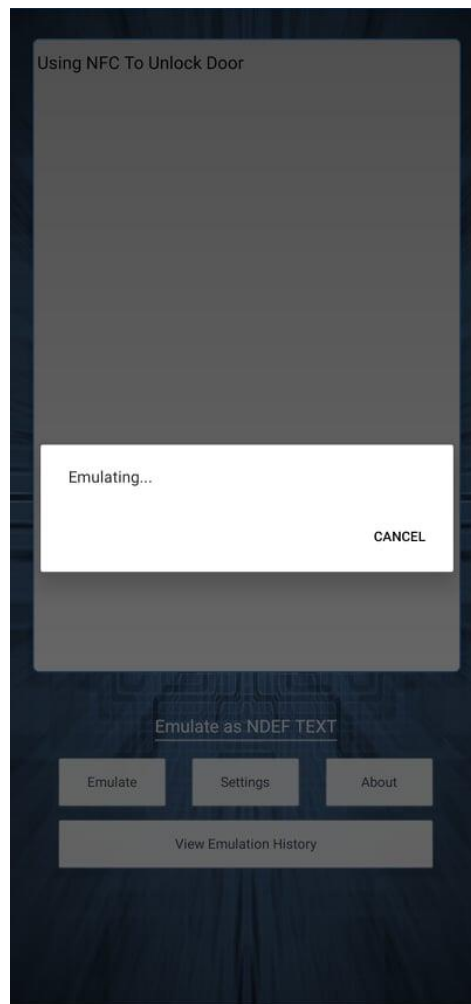
Ξεκλείδωμα με την χρήση του NFC:

Με την επιλογή για ξεκλείδωμα με NFC ο χρήστης έχει την δυνατότητα να ξεκλειδώσει την πόρτα χρησιμοποιώντας το NFC receiver αλλά αντί να χρησιμοποιήσει NFC tag μπορεί να χρησιμοποιήσει το smartphone του, δεδομένου ότι παρέχει την δυνατότητα αυτή. Λόγω της αδυναμίας το expo framework και του React Native για

υποστήριξη NFC, με την επιλογή NFC από την κύρια διεπαφή το application κάνει redirect σε άλλη εφαρμογή που απευθείας επιτρέπει την χρήση του NFC του κινητού.

Figure 22

Παράδειγμα ξεκλειδώματος με τη χρήση του NFC του smartphone



Σχήμα 4.11: Παράδειγμα ξεκλειδώματος με τη χρήση του NFC του smartphone

Παρακολούθηση των logs./ Notifications:

Με την επιλογή αυτή ο χρήστης έχει την δυνατότητα να παρατηρήσει προηγούμενες προσπάθειες επιτυχημένες και μη για το ξεκλείδωμα της πόρτας. Οι πληροφορίες που καταγράφονται είναι το όνομα χρήστη (doorbell σε περίπτωση χρήστη φυσικής παρουσίας) , η μέθοδος ξεκλειδώματος που χρησιμοποιήθηκε (PIN, NFC, Fingerprint, OTP), οι προσπάθειες που έμειναν στον χρήστη προτού να μπλοκαριστεί, ημερομηνία, ώρα και με χρώμα πράσινο ή κόκκινο ανάλογα με το αν έγινε επιταχυνόμενο ξεκλείδωμα.

Επιπλέον όπως αναφέρθηκε και προηγουμένως σε περίπτωση πολλαπλών αποτυχημένων προσπαθειών ο χρήστης λαμβάνει notification μέσω της εφαρμογής.

Figure 23

Παράδειγμα παρακολούθησης των logs



LOGS	
doorbell	13:48:53
NFC	07/12/2020
Tries Left: 2	
doorbell	13:48:42
NFC	07/12/2020
Tries Left: 3	
makris25	16:40:20
PIN	26/11/2020
Tries Left: 3	
makris25	19:07:12
PIN	25/11/2020
Tries Left: 2	
makris25	18:38:36
PIN	25/11/2020
Tries Left: 3	
makris25	18:38:03
PIN	25/11/2020
Tries Left: 3	
makris25	18:34:55

Σχήμα 4.12: Παράδειγμα ξεκλειδώματος με τη χρήση του NFC του smartphone

Κεφάλαιο 5

Αξιολόγηση Συστήματος

5.1	Εισαγωγή	38
5.2	Αξιολόγηση	39
5.3	Αδυναμίες συστήματος	41

5.1 Εισαγωγή

Μετά την υλοποίηση του συστήματος δεν θα μπορούσε να παραληφθεί η αξιολόγηση του συστήματος. Με την αξιολόγηση μπορούμε να διακρίνουμε αν έχουν υλοποιηθεί όλοι οι στόχοι που προσδιορίστηκαν στις προδιαγραφές του συστήματος και παράλληλα να βρούμε τυχόν αδυναμίες ή ατέλειες του συστήματος. Η αξιολόγηση ενός συστήματος μπορεί να γίνει με διάφορους τρόπους, είτε με την χρήση του συστήματος από άλλους χρήστες είτε με την αξιολόγηση από τον κατασκευαστή συγκρίνοντας τις προδιαγραφές του συστήματος με το τελικό προϊόν.

Ένα από τα κύρια χαρακτηριστικά του συστήματος είναι η απλότητα και η ευκολία του στην χρήση. Για τον λόγο αυτό η αξιολόγηση θα ήταν προτιμότερο να γίνει με την μέθοδο απάντησης ερωτηματολογίων από χρήστες που έχουν δοκιμάσει το σύστημα εξετάζοντας τόσο τις λειτουργίες, όσο και την ευχρηστία του συστήματος. Η διεκπεραίωση του project όμως, έγινε κατά την περίοδο της πανδημίας COVID-19 όπου η αλληλεπίδραση και η φυσική επικοινωνία μεταξύ των ανθρώπων είναι περιορισμένη. Αυτό είχε ως αποτέλεσμα να μην ήταν δυνατή η αξιολόγηση του συστήματος από τους χρήστες. Έτσι η μέθοδος που χρησιμοποιήθηκε για την αξιολόγηση του συστήματος ήταν η μέθοδος της αυτό-αξιολόγησης.

5.2 Αξιολόγηση

Στην συνέχεια θα ακολουθήσει η αξιολόγηση του συστήματος σε σχέση με τις προδιαγραφές που ορίστηκαν, όπως φαίνονται και στο κεφάλαιο 4.1.

- Απλό και εύκολο στην χρήση: Το σύστημα μας χαρακτηρίζεται από την απλότητα του και την ευχρηστία, όσο με την χρήση της φυσικής παρουσίας όσο και με την χρήση του smart home application. Και στις δύο περιπτώσεις ο χρήστης καλείται να χρησιμοποιήσει την κύρια διεπαφή για την επιλογή μεθόδου ξεκλειδώματος και αμέσως μετά να εισαγάγει έναν κωδικό ή να χρησιμοποιήσει το NFC ή το δακτυλικό αποτύπωμα για το ξεκλείδωμα. Επιπλέον, οι διάφορες επιλογές του χρήστη για το ξεκλείδωμα καθιστούν την χρήση του συστήματος ακόμα πιο εύκολη επειδή ο χρήστης δεν είναι αναγκασμένος να έχει πάνω του ένα κλειδί για να ξεκλειδώσει την πόρτα. Το μόνο που χρειάζεται είναι γνώση του PIN ή κατοχή smartphone με εγκατεστημένη την εφαρμογή του Smart Lock. Τέλος σε περίπτωση που ο χρήστης θέλει να δώσει προσωρινή άδεια σε κάποιον να μπει στο σπίτι δεν χρειάζεται να του δώσει το κλειδί του αλλά μπορεί να του δώσει έναν προσωρινό κωδικό μιας χρήσης OTP.
- Γρήγορο: Οι μέθοδοι ξεκλειδώματος είναι αρκετά γρήγοροι, αν όχι και γρηγορότεροι, από την παραδοσιακή μέθοδο του ξεκλειδώματος με κλειδί. Η λειτουργίες όσο με φυσική παρουσία όσο και μέσω της smartphone εφαρμογής χρειάζονται 2 με 4 δευτερόλεπτα για την ολοκλήρωση τους ανάλογα και με την ταχύτητα του χρήστη. Ο χρόνος αυτός είναι περίπου ο ίδιος με τον μέσο χρόνο που ένας άνθρωπος χρειάζεται για να ανοίξει την πόρτα με ένα κλειδί.
- Ασφάλεια και Προστασία Δεδομένων: Μεγάλη έμφαση δόθηκε στον τομέα της Ασφάλειας και της Προστασίας των Δεδομένων του συστήματος. Αρχικά οι μόνοι που μπορούν να χρησιμοποιήσουν το σύστημα είναι αυτοί που:
 - Γνωρίζουν τον κωδικό PIN
 - Κατέχουν ένα valid NFC tag
 - Γνωρίζουν το secret key για να λαμβάνουν το OTP μέσω του Google Authenticator
 - Είναι εγγεγραμμένοι στην βάση δεδομένων, κατέχουν την smartwatch εφαρμογή, χρησιμοποιούν το τοπικό δίκτυο ή VPN και είτε γνωρίζουν τον κωδικό PIN είτε χρησιμοποιούν συσκευή με authorized NFC ID.

Όλοι οι κωδικοί των χρηστών, τα PINs, τα IDs των valid NFC tags και συσκευών και των κλειδι για το OTP είναι κρυπτογραφημένοι μέσα στην βάση δεδομένων. Στην συνέχεια θα αναλύσουμε την ασφάλεια που παρέχει η κάθε μέθοδος ξεκλειδώματος, τις αδυναμίες τους και τρόπους αντιμετώπισης:

- PIN με φυσική παρουσία: Ο μόνος τρόπος να παραβιαστεί το PIN με φυσική παρουσία είναι κάποιος να γνωρίζει το PIN ή να προσπαθήσει να το μαντέψει. Στην περίπτωση ενός τετραψήφιου PIN η πιθανότητα είναι 0.01%, αλλά αφού έχουμε 3 προσπάθειες προτού μπλοκαριστεί ο χρήστης και ειδοποιηθεί ο διαχειριστής, η πιθανότητα γίνεται 0.03%. Για μεγαλύτερη ασφάλεια ο διαχειριστής μπορεί να αυξήσει τα ψηφία του PIN και να αλλάζει το PIN συχνά.
- NFC tag: Όσον αφορά την μέθοδο του NFC tag μπορεί να υπάρξει NFC spoofing ή η φυσική κλοπή του tag. Με το NFC spoofing εννοούμε ότι κάποιος μπορεί να τοποθετήσει κοντά στο tag μια συσκευή η οποία να κλέβει τα δεδομένα του tag και μετά να τα χρησιμοποιήσει για να εισχωρήσει στο σύστημα. Ο τρόπος για να αντιμετωπιστεί αυτό είναι τα tags να φυλάγονται σε NFC protected θήκες έτσι ώστε να μην μπορεί κάποιος να κλέψει τα στοιχεία τους ενώ βρίσκονται στις τσέπες των χρηστών. Αν τυχόν κλαπεί ένα NFC tag ο διαχειριστής μπορεί να το απενεργοποιήσει από την βάση δεδομένων.
- OTP Google Authenticator: Το OTP είναι ένας 6-ψήφιος αριθμός ο οποίος αλλάζει κάθε 30 δευτερόλεπτα γι' αυτό και είναι δύσκολο να παραβιαστεί με την τυπική μέθοδο brute-force. Η αδυναμία του κυρίως βρίσκεται στην πρόσβαση εξουσιοδοτημένης συσκευής με το Google Authenticator. Για τον λόγο αυτό τα smartphone των εξουσιοδοτημένων χρηστών πρέπει να ζητούν κάποιο είδος authentication για να ξεκλειδωθούν.
- Μέθοδοι μέσω smartphone: Πρόσβαση στο smarthome application έχουν μόνο οι χρήστες του τοπικού δικτύου και είναι εγγεγραμμένοι στο τοπικό δίκτυο. Επιπλέον πρέπει να γνωρίζουν το PIN ή να έχουν εγγεγραμμένο NFC ID στην βάση δεδομένων ή να επιβεβαιώσουν ότι είναι οι πραγματικοί χρήστες της συσκευής μέσω του system Fingerprint authentication.

Ο διαχειριστής του συστήματος μπορεί να απενεργοποιήσει ή να ενεργοποιήσει κάποιες από τις λειτουργίες αν θεωρεί ότι δεν είναι αρκετά ασφαλής. Επιπλέον για

περισσότερη ασφάλεια, μοντέρνα συστήματα ταυτοποίησης χρησιμοποιούν την μέθοδο του 2FA (2-Factor Authentication). Αυτό σημαίνει ότι για το authentication του χρήστη χρειάζονται δύο στάδια ταυτοποίησης. Το 2FA πρέπει συνήθως να επαληθεύει δύο από τις τρεις αρχές ταυτοποίησης (something you have, something you know, something you are). Συνήθως για το 2FA χρησιμοποιείται ένα password (something you know) και ένας κωδικός μέσω SMS (something you have). Στην δική μας εφαρμογή μπορεί να εφαρμοστεί το 2FA με κάποιες τροποποιήσεις στον κώδικα. Ένα παράδειγμα 2FA στο παρών σύστημα είναι η χρήση του PIN (something you know) και μετά η χρήση του OTP με το Google Authenticator (something you have) επαληθεύοντας έτσι ότι η εισαγωγή του κωδικού PIN έγινε από κάποιον που έχει πρόσβαση σε εξουσιοδοτημένη συσκευή με το Google Authenticator. Με την χρήση 2FA αυξάνεται η ασφάλεια του συστήματος αλλά ταυτόχρονα αυξάνεται και ο χρόνος και η πολυπλοκότητα στο ξεκλείδωμα της πόρτας.

- Επιλογή των σωστών υλικών και εργαλείων: Το υλικό που χρησιμοποιήθηκε για το σύστημα μέχρι στιγμής μπορεί να κριθεί αξιόπιστο αφού δεν έχουν παρατηρηθεί μεγάλα προβλήματα όσον αφορά τα εξαρτήματα. Επιπλέον τα εργαλεία που χρησιμοποιήθηκαν για την διαχείριση του συστήματος ήταν αρκετά καλά και επέτρεπαν την εύκολη χρήση των συσκευών χωρίς bugs. Αδυναμίες του συστήματος παρατηρήθηκαν στην χρήση των εργαλείων για την δημιουργία του front end σε smartphone συσκευές και θα επεξηγηθεί στην συνέχεια.

5.3 Αδυναμίες συστήματος

Η υλοποίηση ενός τέτοιου πολύπλοκου συστήματος δεν θα μπορούσε να επιτευχθεί χωρίς την επίλυση των διαφόρων προβλημάτων που εμφανίζονταν κατά την ανάπτυξη του συστήματος. Τα περισσότερα προβλήματα επιλύονταν μετά από έρευνα στο διαδίκτυο και με την χρήση διαφορετικών μεθόδων και βιβλιοθηκών. Κάποια προβλήματα όμως δεν μπορούσαν να επιλυθούν λόγω αδυναμιών του λογισμικού που χρησιμοποιήθηκε. Πιο συγκεκριμένα, για την ανάπτυξη του front end για smartphone εφαρμογές, επιλέχθηκε το expo framework για την ευκολία χρήσης του, υποστήριξης του από διαφορετικά λειτουργικά συστήματα και βιβλιοθήκες.

Οι αδυναμίες του expo framework που παρατηρήθηκαν κατά την υλοποίηση της android εφαρμογής ήταν:

- Υποστήριξη του Login με Google Account.
- Ενεργοποίηση του NFC μέσα από την εφαρμογή.
- Εξαγωγή του κώδικα React Native σε Android Studio.

Οι αδυναμίες του framework δεν επηρέασαν σε μεγάλο βαθμό την αξιοπιστία και τις λειτουργίες του συστήματος αλλά θα έδιναν περισσότερες δυνατότητες στον προγραμματιστή για εισαγωγή περαιτέρω features.

Κεφάλαιο 6

Συμπεράσματα και Μελλοντικά Σχέδια

6.1	Συμπεράσματα	43
6.2	Μελλοντικά Σχέδια	44

6.1 Συμπεράσματα

Η υλοποίηση ενός τέτοιου συστήματος δεν ήταν εύκολη. Οι προκλήσεις για την δημιουργία ενός συστήματος τόσο ευαίσθητου αλλά και τόσο απλού στην χρήση ήταν πολλές. Μετά από αρκετή έρευνα και μελέτη στο διαδίκτυο αλλά και εφαρμογή της θεωρίας που μαθαίνεται μέσα από το πανεπιστήμιο η υλοποίηση ολοκληρώθηκε με επιτυχία. Ξεκινώντας από την συνδεσμολογία των συσκευών στο Raspberry Pi και την υλοποίηση του κώδικα, χρειάστηκε βαθύτερη κατανόηση στις αρχές επικοινωνίας με τα διάφορα input/output devices και της αρχιτεκτονικής τόσο του Raspberry Pi όσο και των διαφόρων συσκευών. Στη συνέχεια έπρεπε να γίνει η υλοποίηση των διαφόρων πρωτοκόλλων ασφάλειας για την αποθήκευση και την αποστολή ευαίσθητων δεδομένων. Τέλος, να ληφθούν υπόψη οι διάφορες ανάγκες των χρηστών για να μπορούν να εφαρμοστούν σε ένα ευκολόχρηστο σύστημα που στο τέλος της ημέρας να βελτιώνει την εμπειρία του χρήστη.

Η ανάπτυξη του συστήματος αγγίζει διάφορες πτυχές της τεχνολογίας των Ηλεκτρονικών Υπολογιστών. Μερικές από αυτές είναι:

- Κρυπτογραφία και Ασφάλεια Δικτύου
- Προγραμματισμός συσκευών
- Ανάπτυξη front end application φιλικό προς τον χρήστη
- Προγραμματισμός βάσεων δεδομένων
- Smarthome technology

Η μελέτη των παραπάνω τεχνολογιών και η εφαρμογή τους σε real life application αποτέλεσε την επιτυχή υλοποίηση του συστήματος.

6.2 Μελλοντικά Σχέδια

Κανένας δεν μπορεί να αρνηθεί ότι η Smart Home τεχνολογία είναι η επιστήμη του μέλλοντος. Ο άνθρωπος πάντα θα ψάχνει τρόπους για να βελτιώσει την ζωή του και ένας από αυτούς είναι η αξιοποίηση των έξυπνων σπιτιών. Από την στιγμή που η τεχνολογία αυτή δεν εδραιώθηκε σε ολόκληρο τον κόσμο, είτε λόγω του κόστους, είτε λόγω της πολυπλοκότητας είτε λόγω των περιορισμένων λειτουργιών, πάει να πει πως υπάρχει περιθώριο για βελτίωση.

Το ίδιο ισχύει και για το δικό μας σύστημα. Πιστεύω πως οι τεχνολογίες που χρησιμοποιήθηκαν είναι σύγχρονες αλλά όσο η τεχνολογία προχωρά θα πρέπει και τα συστήματα να αναβαθμίζονται ανάλογα. Μερικές τεχνολογίες που θα μπορούσαν να ενσωματωθούν στο μέλλον για να προσφέρουν περισσότερες επιλογές ξεκλειδώματος στους χρήστες είναι:

- Face recognition
- QR-code
- Voice commands

Επιπλέον, για περισσότερη ασφάλεια όπως αναφέρθηκε και στην αξιολόγηση του συστήματος, καλό θα ήταν να εφαρμοστεί η μέθοδος του Two Factor Authentication (2FA). Με την μέθοδο 2FA μπορούν να χρησιμοποιηθούν 2 από τις μεθόδους που υλοποιήθηκαν στο σύστημα για την ταυτοποίηση του χρήστη. Αρχική σκέψη υλοποίησης του 2FA είναι να απενεργοποιηθεί η μέθοδος του OTP από τις κύριες μεθόδους ξεκλειδώματος και να χρησιμοποιείται μόνο στην δεύτερη φάση ταυτοποίησης.

Τέλος, το Smart Lock σύστημα σε συνδυασμό με προηγούμενες εργασίες ή υπάρχουσες εφαρμογές smarthome οι οποίες υλοποιούν συστήματα φωτισμού, ελέγχου θερμοκρασίας κλπ. με τις κατάλληλες τροποποιήσεις μπορούν να αποτελέσουν το απόλυτο σύστημα smarthome, τόσο σε ασφάλεια, όσο και σε λειτουργίες.

Βιβλιογραφία

- [1] Robles, Rosslin John, and Tai-hoon Kim. "Applications, systems and methods in smart home technology: A." Int. Journal of Advanced Science And Technology 15 (2010): 37-48.
- [2] Sripan, Meensika, et al. "Research and thinking of smart home technology." International Conference on Systems and Electronic Engineering (ICSEE'2012). 2012.
- [3] Rahman, Md Maksudur, Mohammed Sowket Ali, and Md Shoaib Akther. "Password Protected Electronic Lock System for Smart Home Security." International Journal Of Engineering Research & Technology 7.4 (2018): 541-544.
- [4] Ur, Blase, Jaeyeon Jung, and Stuart Schechter. "The current state of access control for smart devices in homes." Workshop on Home Usable Privacy and Security (HUPS). Vol. 29. HUPS 2014, 2013.
- [5] Robles, Rosslin John, et al. "A review on security in smart home development." International Journal of Advanced Science and Technology 15 (2010).

Χρήσιμα links

- <https://www.tomshardware.com/>
- <http://wiki.sunfounder.cc/>
- <https://cryptography.io/>
- <https://learn.adafruit.com/>
- <https://en.wikipedia.org/>