ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σχεδιασμός, Υλοποίηση και Αξιοπιστία Ψηφιακού Συστήματος Συναγερμού Ασφαλείας με Τεχνητή Νοημοσύνη για Κινητές Συσκευές

Μερτ Αγά
711171001

Επιβλέπων:
Χρήστος Τρούσσας
Επίκουρος Καθηγητής

Αθήνα, 2024

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σχεδιασμός, Υλοποίηση και Αξιοπιστία Ψηφιακού Συστήματος Συναγερμού Ασφαλείας με Τεχνητή Νοημοσύνη για Κινητές Συσκευές

Μερτ Αγά

Α.Μ. 711171001

Επιβλέπων:

Χρήστος Τρούσσας, Επίκουρος Καθηγητής

Εξεταστική Επιτροπή:

Α/Α	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ	ΥΠΟΓΡΑΦΗ
1	Χρήστος Τρούσσας	Επ. Καθηγητής	Christos Troussas Digitally signed by Christos Troussas Date: 2024.07.17 14:53:33 +03'00'
2	Ακριβή Κρούσκα	Μέλος ΕΔΙΠ	Akrivi Krouska Digitally signed by Akrivi Krouska Date: 2024.07.18 17:00:07 +03'00'
3	Παναγιώτα Τσελέντη	Μέλος ΕΔΙΠ	Panagiota Tselenti Digitally signed by Panagiota Tselenti Date: 2024.07.17 16:30:44 +03'00'

Ημερομηνία εξέτασης: Ιούλιος 2024

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Μερτ Αγά του Ριτβάν με αριθμό μητρώου 711171001 φοιτητής του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Βεβαιώνω ότι είμαι συγγραφέας αυτής της Διπλωματικής εργασίας και κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

ΕΥΧΑΡΙΣΤΙΕΣ

Εκφράζω την ειλικρινή μου ευγνωμοσύνη στους καθηγητές μου στο πανεπιστήμιο και στον επιβλέποντα καθηγητή μου, Χρήστο Τρούσσα, του οποίου η καθοδήγηση και η υποστήριξη ήταν καθοριστική καθ' όλη τη διάρκεια της ερευνητικής διαδικασίας και της υλοποίησης αυτής της εργασίας.

Επιπλέον, είμαι βαθιά ευγνώμων στην αγαπημένη μου οικογένεια και τους φίλους μου για την υποστήριξη, την ενθάρρυνση και την κατανόησή τους. Η συνεχής υποστήριξή τους και η πίστη τους σε μένα ήταν το βασικό θεμέλιο της δύναμής μου, εμπνέοντάς με να ακολουθήσω το πάθος μου.

ΠΕΡΙΛΗΨΗ

Επί αιώνες, η διατήρηση του προσωπικού χώρου και η διασφάλιση της ατομικής ασφάλειας παρέμειναν επιτακτικές για την ανθρώπινη ύπαρξη. Με την εξέλιξη της τεχνολογίας, έχουν εμφανιστεί αμέτρητες λύσεις για την ενίσχυση των μέτρων ασφαλείας, οι οποίες ανταποκρίνονται στις διαφορετικές ανάγκες των ατόμων και του περιβάλλοντός τους. Η παρούσα διπλωματική εργασία εξετάζει το σύγχρονο πεδίο της ενίσχυσης της ασφάλειας, προτείνοντας την ανάπτυξη μιας σύνθετης εφαρμογής για κινητά τηλέφωνα. Αξιοποιώντας τις δυνατότητες της όρασης υπολογιστών και της μηχανικής μάθησης, αυτή η εφαρμογή αξιοποιεί την κάμερα του κινητού τηλεφώνου για την υλοποίηση τεχνολογιών ανίχνευσης προσώπου, αναγνώρισης προσώπου και ανίχνευσης κίνησης.

Ο βασικός στόχος της παρούσας εργασίας είναι να διερευνήσει τις περίπλοκες διαδικασίες σχεδιασμού, υλοποίησης και αξιολόγησης της προτεινόμενης εφαρμογής. Επιπλέον, αναλαμβάνει την αξιολόγηση παλαιότερων μοντέλων κινητών, λαμβάνοντας υπόψη την επικρατούσα τάση της ετήσιας αντικατάστασης κινητών τηλεφώνων. Η εργασία αυτή χρησιμεύει ως μια συναρπαστική απόδειξη της δυναμικής αλληλεπίδρασης μεταξύ καινοτομίας και αναγκαιότητας στη σύγχρονη κοινωνία.

Λέξεις κλειδιά: αναγνώριση προσώπου, ανίχνευση κίνησης, όραση υπολογιστών, μηχανική μάθηση, τεχνητή νοημοσύνη, συστήματα συναγερμού, ανάπτυξη κινητών εφαρμογών, android, kotlin

ABSTRACT

For centuries, having our own space and feeling safe has been extremely important to humans. As technology has sprung up tons of solutions to make security better for everyone's different needs and environments. This study dives into today's security world by proposing a fancy new app for mobile phones. Leveraging the capabilities of computer vision and machine learning, this application leverages the mobile phone camera to implement face detection, face recognition and motion detection technologies.

The main objective of this thesis is to explore the complex processes of design, implementation and evaluation of the proposed application. In addition, it undertakes the evaluation of older phone models, considering the prevailing trend of annual replacement of mobile phones. This work serves as a compelling demonstration of the dynamic interplay between innovation and necessity in contemporary society.

Keywords: face recognition, motion detection, computer vision, machine learning, artificial intelligence, alarm systems, mobile application development, android, kotlin

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΓΡΑΦΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

AI	Artificial Intelligence	Τεχνητή Νοημοσύνη
ML	Machine Learning	Μηχανική Μάθηση
DB	Database	Βάση Δεδομένων
UI	User Interface	Διεπαφή Χρήστη
API	Application Programming Interface	Διεπαφή Προγραμματισμού Εφαρμογών
CCTV	Closed Circuit Television	Κλειστό Κύκλωμα Τηλεόρασης
VR	Virtual Reality	Εικονική Πραγματικότητα
AR	Augmented Reality	Επαυξημένη Πραγματικότητα
PIR	Passive Infrared Sensor	Παθητικός Αισθητήρας Υπέρυθρων
IDE	Integrated Development Environment	Ολοκληρωμένο Περιβάλλον Ανάπτυξης
CNN	Convolutional Neural Networks	Συνελικτικά Νευρωνικά Δίκτυα
RNN	Recurrent Neural Networks	Επαναλαμβανόμενα Νευρωνικά Δίκτυα
SDK	Software Development Kit	Κιτ Ανάπτυξης Λογισμικού
AES	Advanced Encryption Standard	Προηγμένο Πρότυπο Κρυπτογράφησης

1. Εισαγωγή

Το κεφάλαιο αυτό παρέχει μια επισκόπηση του βασικού πλαισίου της θεματικής περιοχής, περιγράφοντας τους βασικούς όρους που χρησιμοποιούνται σε όλη τη διατριβή, οριοθετώντας τον προβληματικό τομέα και τα επακόλουθα ερευνητικά ερωτήματα. Στη συνέχεια, διενεργεί λεπτομερή ανάλυση των ερευνητικών στόχων, του πεδίου εφαρμογής των κινητών συσκευών και της περιγραφής του έργου.

Η ασφάλεια των σπιτιών αποτελεί ένα ζήτημα εξαιρετικής σημασίας, καθώς επηρεάζει σημαντικά την ευημερία και τη συνολική ασφάλεια των ανθρώπων. Στον σημερινό κόσμο, αντιμετωπίζονται κλιμακούμενες προκλήσεις, όπως ο εγκληματικός εκφοβισμός και οι κλοπές, υπογραμμίζοντας την ανάγκη για ισχυρά μέτρα προστασίας. Μεταξύ των πιο αποτελεσματικών μεθόδων προστασίας των σπιτιών είναι η εφαρμογή ενός καλά σχεδιασμένου συστήματος συναγερμού [1].

Η εξέλιξη των κινητών συσκευών και των εφαρμογών τους είναι μια συνεχής διαδικασία που χαρακτηρίζεται από συνεχή καινοτομία και βελτιωμένη φιλικότητα προς τον χρήστη. Κατά συνέπεια, η ενσωμάτωση των κινητών τηλεφώνων με συστήματα επιτήρησης έχει γίνει όλο και πιο διαδεδομένη, επιτρέποντας στους ιδιώτες να παρακολουθούν την ασφάλεια της περιουσίας τους οποτεδήποτε και οπουδήποτε [2]. Με την ευρεία υιοθέτηση και την αυξανόμενη πολυπλοκότητα των κινητών τηλεφώνων, δεν χρησιμεύουν μόνο ως συσκευές επικοινωνίας αλλά και ως κάμερες, προγράμματα περιήγησης στο διαδίκτυο, συσκευές αναπαραγωγής μουσικής, πλατφόρμες παιχνιδιών, ακόμη και ως ασύρματα τηλεχειριστήρια [3].

Με τις προηγμένες δυνατότητες και τη συνδεσιμότητά τους, τα κινητά τηλέφωνα προσφέρουν στους χρήστες πρωτοφανείς δυνατότητες ελέγχου και παρακολούθησης των συστημάτων ασφαλείας του σπιτιού τους. Μέσω ειδικών εφαρμογών και πλατφορμών, οι χρήστες μπορούν να έχουν απομακρυσμένη πρόσβαση σε ζωντανές τροφοδοσίες καμερών, να λαμβάνουν ειδοποιήσεις σε πραγματικό χρόνο και ακόμη και να ελέγχουν διάφορες πτυχές των συστημάτων ασφαλείας τους από οπουδήποτε υπάρχει πρόσβαση στο διαδίκτυο [4]. Αυτό το επίπεδο προσβασιμότητας και ευκολίας έχει φέρει επανάσταση στον τρόπο με τον οποίο οι άνθρωποι προσεγγίζουν την οικιακή ασφάλεια, καθιστώντας την πιο εξατομικευμένη και ανταποκρινόμενη στις ανάγκες τους.

Επιπλέον, η ενσωμάτωση τεχνολογιών αιχμής, όπως η αναγνώριση προσώπου και η ανίχνευση κίνησης, ενισχύει περαιτέρω την αποτελεσματικότητα των λύσεων οικιακής ασφάλειας μέσω κινητών τηλεφώνων [5]. Αυτές οι τεχνολογίες επιτρέπουν την ακριβέστερη και πιο αξιόπιστη ανίχνευση εισβολών ή ύποπτων δραστηριοτήτων, ελαχιστοποιώντας τους ψευδείς συναγερμούς και εξασφαλίζοντας άμεσες και κατάλληλες αντιδράσεις όταν συμβαίνουν παραβιάσεις της ασφάλειας. Αξιοποιώντας τη δύναμη της τεχνητής νοημοσύνης και της μηχανικής μάθησης, τα συστήματα ασφαλείας που βασίζονται σε κινητά μπορούν να προσαρμόζονται συνεχώς και να βελτιώνουν την απόδοσή τους με την πάροδο του χρόνου, παρέχοντας στους χρήστες μεγαλύτερη ψυχική ηρεμία και εμπιστοσύνη στα μέτρα ασφαλείας του σπιτιού τους [5].

Στο πλαίσιο αυτό, στην παρούσα διατριβή, ο «ψηφιακός συναγερμός ασφαλείας», αντιπροσωπεύει μια σημαντική πρόοδο στις λύσεις οικιακής ασφάλειας που βασίζονται σε κινητά. Συνδυάζοντας τις δυνατότητες της αναγνώρισης προσώπου και της ανίχνευσης κίνησης, ο ψηφιακός συναγερμός ασφαλείας προσφέρει στους χρήστες μια ιδιαίτερα εξελιγμένη και προληπτική προσέγγιση για την προστασία των σπιτιών και των ιδιοκτησιών τους. Το σύστημα χρησιμοποιεί την κάμερα ενός κινητού τηλεφώνου για την αναγνώριση ατόμων μέσω της τεχνολογίας αναγνώρισης προσώπου και την ανίχνευση τυχόν κινήσεων ή προσπαθειών μη εξουσιοδοτημένης πρόσβασης μέσω αλγορίθμων ανίχνευσης κίνησης. Κατά την ανίχνευση ύποπτων δραστηριοτήτων, το σύστημα συναγερμού στέλνει αμέσως ειδοποιήσεις στο κινητό τηλέφωνο του χρήστη, επιτρέποντας την ταχεία και αποφασιστική δράση για την αντιμετώπιση πιθανών απειλών ασφαλείας. Με την απρόσκοπτη ενσωμάτωση με τις κινητές συσκευές και τα προηγμένα χαρακτηριστικά ασφαλείας, ο ψηφιακός συναγερμός ασφαλείας θέτει νέα πρότυπα για τις λύσεις οικιακής ασφάλειας στην ψηφιακή εποχή.

2. Θεωρητικό Υπόβαθρο

2.1 Εισαγωγή στα Συστήματα Οικιακής Ασφαλείας

Στο επίκεντρο κάθε συστήματος ασφαλείας βρίσκεται μια μοναδική αποστολή να προστατεύει έναν χώρο χρησιμοποιώντας ένα δίκτυο διασυνδεδεμένων εξαρτημάτων και συσκευών. Στον τομέα της οικιακής ασφάλειας, το δίκτυο αυτό περιλαμβάνει μια σειρά ηλεκτρονικών συσκευών που εναρμονίζονται με έναν κεντρικό πίνακα ελέγχου. Ο συλλογικός τους σκοπός είναι να αποτρέψουν πιθανούς εισβολείς και να ειδοποιήσουν γρήγορα τους ιδιοκτήτες σπιτιού για τυχόν απειλές που διαφαίνονται.

Οι μηχανισμοί των συστημάτων συναγερμού ακολουθούν συνήθως ένα κυκλικό μοτίβο, ξεκινώντας με έναν αυτοματοποιημένο βρόχο κυκλώματος που καταλήγει στην ενεργοποίηση ενός συναγερμού ή στη μετάδοση ειδοποιήσεων στους ιδιοκτήτες σπιτιού. Ενεργώντας ως νευρικό κέντρο, μια κεντρική μονάδα ελέγχου οργανώνει αυτή τη διαδικασία, επιτηρώντας συνεχώς τη σειρά αισθητήρων και τις περιμετρικές αποθηκευμένες άμυνες [6].

Επιπλέον, η ενσωμάτωση της τηλεόρασης κλειστού κυκλώματος (CCTV) έχει αναδειχθεί ως εξέχον χαρακτηριστικό στα σύγχρονα συστήματα ασφαλείας, ενισχύοντας την ικανότητά τους να ανιχνεύουν και να παρακολουθούν μη εξουσιοδοτημένα άτομα. Στην εργασία, η ανίχνευση κίνησης χρησιμεύει ως κεντρικό στοιχείο, αξιοποιώντας τις δυνατότητες των κινητών καμερών τόσο για την ανίχνευση κίνησης όσο και για την αναγνώριση προσώπου, που τροφοδοτείται από μια σειρά μοντέλων μηχανικής μάθησης.

Οι εξελίξεις στην τεχνητή νοημοσύνη (AI) έχουν φέρει επανάσταση στις δυνατότητες των συστημάτων ασφαλείας, δίνοντάς τους τη δυνατότητα να προσαρμόζονται και να ανταποκρίνονται έξυπνα στις εξελισσόμενες απειλές [7]. Οι αλγόριθμοι μηχανικής μάθησης αναλύουν τεράστιες ποσότητες δεδομένων για τον εντοπισμό μοτίβων και ανωμαλιών, επιτρέποντας την προγνωστική ανάλυση και τον προληπτικό μετριασμό απειλών.

2.2 Ο Ρόλος της Τεχνητής Νοημοσύνης στα Συστήματα Ασφαλείας

Από την προέλευσή της ως μια απλή ιδέα στην επιστήμη των υπολογιστών, η Τεχνητή Νοημοσύνη (AI) έχει εξελιχθεί σε μια συναρπαστική τεχνολογία που αγγίζει σχεδόν κάθε άλλο κλάδο, όπως τα μέτρα ασφαλείας. Η έννοια της τεχνητής νοημοσύνης που θα επέτρεπε στις μηχανές να αντιγράφουν την ανθρώπινη νόηση έχει τις ρίζες της ήδη από την αρχαιότητα και εκφράστηκε σε μύθους και θρύλους για αυτόματα και τεχνητούς ανθρώπους. Αλλά το πότε ξεκίνησε επίσημα η τεχνητή νοημοσύνη ως πεδίο μελέτης μπορεί να εντοπιστεί στα μέσα της δεκαετίας του 1900. Αξίζει να αναφέρουμε ότι το 1950 ο Alan Turing, ο οποίος ήταν Άγγλος μαθηματικός, καθηγητής της λογικής, κρυπτογράφος και θεωρητικός βιολόγος, δημοσίευσε την έρευνα με τίτλο «Computing Machinery and Intelligence» στην οποία πρότεινε το τεστ για την αξιολόγηση της ικανότητας της μηχανής να εκτελεί τις ίδιες ενέργειες με τον άνθρωπο [8].

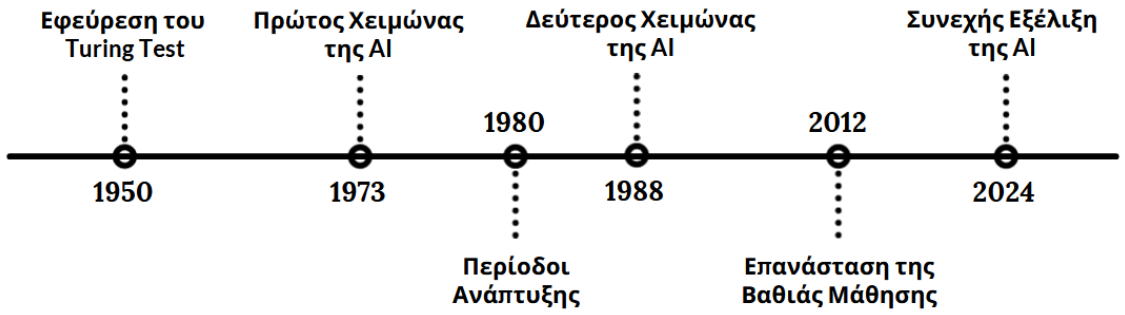
Ο όρος Τεχνητή Νοημοσύνη χρησιμοποιήθηκε για πρώτη φορά σε μια ετήσια συνάντηση με την ονομασία Dartmouth Conference το 1956 στο Dartmouth College από τους John McCarthy, Marvin Minsky, Nathaniel Rochester και Claude Shannon [9]. Το συνέδριο αυτό σηματοδότησε την επίσημη γέννηση της Τεχνητής Νοημοσύνης ως ακαδημαϊκού κλάδου. Η πρώιμη έρευνα για την AI επικεντρώθηκε ως συμβολική, η οποία αφορούσε τον χειρισμό συμβόλων και τη δημιουργία συστημάτων βασισμένων σε κανόνες για την επίλυση προβλημάτων. Η έρευνα για την AI ξεκίνησε ενθαρρυντικά, αλλά σύντομα κατέστη σαφές ότι ο τομέας ήταν γεμάτος παγίδες. Τα πρώτα συστήματα AI αποδείχθηκαν εξαιρετικά αναποτελεσματικά και μη παραγωγικά και αργότερα οδήγησαν σε μια περίοδο μειωμένης χρηματοδότησης και ενδιαφέροντος για τον τομέα που ονομάστηκε «Winter AI». Η πρόοδος έμεινε στάσιμη κατά τη διάρκεια αυτής της περιόδου λόγω των υπολογιστικών περιορισμών και της αδυναμίας κλιμάκωσης των πρώιμων αλγορίθμων AI [10].

Οι δεκαετίες του 1990 και του 2000 ήταν περίοδοι του τρίτου χειμώνα της AI και της τρίτης ανόδου της AI αντίστοιχα, ως αποτέλεσμα της αυξημένης υπολογιστικής δύναμης, της πρόσβασης σε τεράστια σύνολα δεδομένων και της ανάπτυξης νέων αλγορίθμων. Μεταξύ των αξιοσημείωτων επιτευγμάτων που σημειώθηκαν κατά τη διάρκεια αυτής της περιόδου ήταν όταν ο Deep Blue της IBM νίκησε τον παγκόσμιο πρωταθλητή σκακιού Garry Kasparov το 1997 [11]. Στη συνέχεια, η ανάπτυξη της

μηχανικής μάθησης, των νευρωνικών δικτύων και της βαθιάς μάθησης άνοιξε νέα μέσα για τους ερευνητές της AI. Αυτές οι μέθοδοι επέτρεψαν στα συστήματα της AI να μαθαίνουν οποιαδήποτε δεδομένο και να τα χρησιμοποιούν αυτά αποτελεσματικά [12].

Η χρήση της AI στα συστήματα ασφαλείας ξεκίνησε στα τέλη του 20ού αιώνα. Ορισμένες από τις πρώτες εφαρμογές που αναπτύχθηκαν ήταν απλοί αλγόριθμοι αναγνώρισης και συστήματα ανίχνευσης που χρησιμοποιήθηκαν στην ασφάλεια. Για παράδειγμα, τα συστήματα αυτά μπορούσαν να προειδοποιούν εάν υπάρχει ασυνήθιστη δραστηριότητα που θα μπορούσε να υποδηλώνει παραβίαση της ασφάλειας [13]. Αλλά οι δυνατότητες της AI εξακολουθούσαν να καθορίζονται από την υπολογιστική ισχύ και τα δεδομένα που ήταν διαθέσιμα σε αυτόν τον αιώνα.

Η δεκαετία του 2010 είναι η περίοδος κατά την οποία σημειώθηκε σημαντική πρόοδος στην ανάπτυξη της AI και στη χρήση της σε όλους τους κλάδους, αλλά και στα συστήματα ασφαλείας. Η χρήση της βαθιάς μάθησης, δηλαδή ενός τύπου μηχανικής μάθησης που χρησιμοποιεί νευρωνικά δίκτυα με πολλά επίπεδα, είχε τεράστιο αντίκτυπο στην AI. Τα συστήματα AI μπορούσαν να προσλαμβάνουν πλέον τεράστια σύνολα δεδομένων, να εντοπίζουν περίπλοκες συσχετίσεις και να προβλέπουν με μεγάλη ακρίβεια [14].



Εικόνα 1 - Εξέλιξη της Τεχνητής Νοημοσύνης σε Χρόνια

Μία από τις αξιόλογες εφαρμογές της AI στα συστήματα ασφαλείας κατά τη διάρκεια αυτής της περιόδου ήταν η ηλεκτρονική παρακολούθηση. Τα συστήματα CCTV με την AI μπορούσαν να καταγράφουν εικόνες αλλά και να τις αναλύουν επί τόπου. Τα συστήματα αυτά χρησιμοποιούσαν μεθόδους υπολογιστικής όρασης για τον εντοπισμό αποκλίσεων, την αναγνώριση προσώπων και την αναγνώριση

αντικειμένων. Για παράδειγμα, οι αλγόριθμοι βαθιάς μάθησης μπορούσαν να εκπαιδευτούν για να αναγνωρίζουν ανθρώπους από βίντεο, να παρακολουθούν τις κινήσεις τους και ακόμη και να παίρνουν αποτέλεσμα για πιθανούς κινδύνους για την ασφάλεια με βάση τη συμπεριφορά τους [15]. Με τη βοήθεια της τεχνητής νοημοσύνης βελτιώθηκαν διάφορα συστήματα ανίχνευσης και αναγνώρισης. Καθώς τα θεμελιώδη συστήματα συναγερμού χρησιμοποιούν συνήθως απλούς αισθητήρες, ήταν ευάλωτα σε ψευδείς συναγερμούς. Από την άλλη πλευρά, όμως, τα συστήματα που βασίζονται στην AI χρησιμοποιούν έναν συνδυασμό αισθητήρων, καμερών και αλγορίθμων μηχανικής μάθησης για τη διαπίστωση της διαφοροποίησης μεταξύ πραγματικών απειλών και αθώων δραστηριοτήτων. Με αυτόν τον τρόπο, τα συστήματα αυτά είχαν τη δυνατότητα να βελτιώνουν την ακρίβειά τους με την πάροδο του χρόνου λαμβάνοντας γνώση από τα ιστορικά δεδομένα [16].

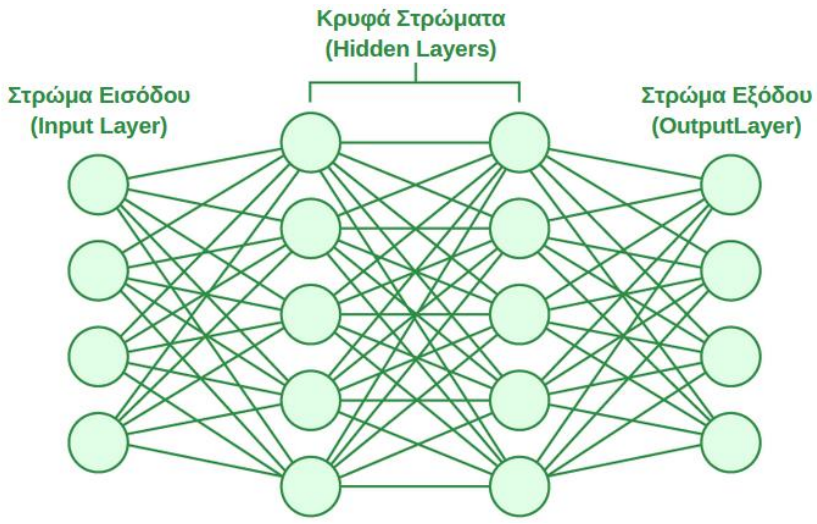
Ο συνδυασμός της AI με τα συστήματα οικιακής ασφάλειας μπορεί να θεωρηθεί σημαντική εξέλιξη της δεκαετίας του 2010 και του 2020. Τα έξυπνα οικιακά συστήματα ασφαλείας με δυνατότητα AI προσφέρουν αυξημένη ασφάλεια και άνεση στους ιδιοκτήτες [17]. Μια από τις πιο χρήσιμες λειτουργίες των συστημάτων οικιακής ασφάλειας στις μέρες μας είναι η σύνδεσή τους με κινητές συσκευές. Η τεχνολογία κινητής τηλεφωνίας επιτρέπει στους χρήστες να παρακολουθούν τα σπίτια τους εξ αποστάσεως μέσω τηλεφώνων και τάμπλετ. Αλλά και οι εφαρμογές για κινητά με τη βοήθεια της AI, προσφέρουν άμεσες ειδοποιήσεις, ζωντανές μεταδόσεις βίντεο και απομακρυσμένη διαχείριση των συσκευών ασφαλείας [18].

Επιπλέον, με την ανάπτυξη της AI, τα συστήματα αναγνώρισης προσώπου προχώρησαν περισσότερο και έγιναν πρότυπα στα οικιακά συστήματα ασφαλείας. Οι εξελιγμένες κάμερες ασφαλείας μπορούν να αναγνωρίζουν φίλους και συγγενείς και ποιος είναι εισβολέας ή ξένος. Τα συστήματα αναγνώρισης προσώπου μπορούν επίσης να ενσωματωθούν με έξυπνες κλειδαριές για πρόσβαση όταν οι κωδικοί της πόρτας δεν είναι απαραίτητοι [19]. Ένας άλλος βοηθός της οικιακής ασφάλειας είναι η ανίχνευση κίνησης με προηγμένο τρόπο. Η τεχνολογία έχει καταστήσει δυνατή την εξέλιξη των CCTV σε τέτοιο βαθμό, ώστε να είναι σε θέση να χρησιμοποιούν AI για να αναλύουν μοτίβα κίνησης και να διακρίνουν μεταξύ ανθρώπων, ζώων και άλλων αντικειμένων σε κίνηση [20].

Εξετάζοντας την εξέλιξή της τα τελευταία χρόνια, η AI θα βρεθεί στο επίκεντρο της επανάστασης στον κλάδο των λύσεων ασφαλείας στα επόμενα χρόνια. Μεταξύ αυτών, θα μπορούσαν να είναι οι ακόλουθες τεχνολογίες: προγνωστική ανάλυση, αυτόνομα μη επανδρωμένα αεροσκάφη, ενισχυμένη βιομετρική ασφάλεια, καθώς και ενσωμάτωση του κυβερνοχώρου και της φυσικής ασφάλειας. Ωστόσο, είναι εξαιρετικά σημαντικό να αντιμετωπιστούν τα ζητήματα ηθικής και προστασίας της ιδιωτικής ζωής σε σχέση με αυτές τις τεχνολογίες, ώστε να διασφαλιστεί ότι εξυπηρετούν τον σκοπό της βοήθειας προς την κοινωνία [21].

2.2.1 Νευρωνικά Δίκτυα στην Τεχνητή Νοημοσύνη

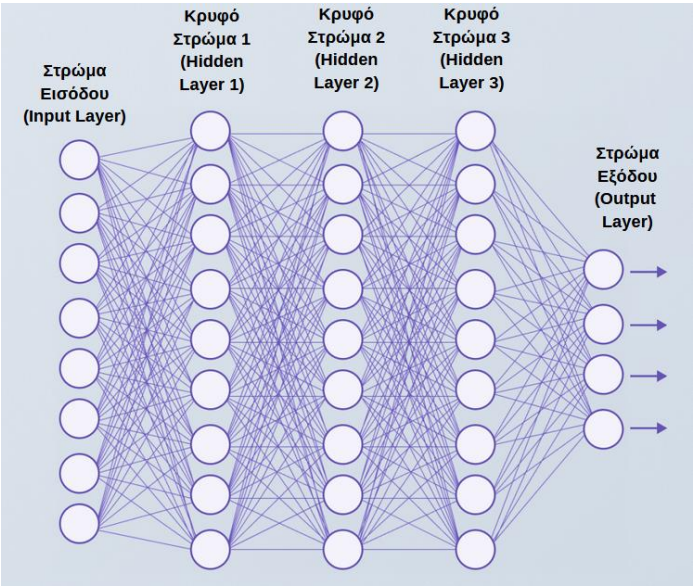
Η τεχνητή νοημοσύνη αποτελείται από νευρωνικά δίκτυα, τα οποία βρίσκονται σε εξέλιξη από τη στιγμή που σχεδιάστηκαν για πρώτη φορά. Το πρώτο μοντέλο αναπτύχθηκε από τους Warren McCulloch και Walter Pitts το 1943 και παρείχε τη βάση για τη λογική λειτουργία των νευρώνων. Το 1958 ο Frank Rosenblatt ανέπτυξε το Perceptron που επέτρεψε την κατασκευή απλών νευρωνικών δικτύων που μπορούν να μαθαίνουν από δεδομένα [22]. Ωστόσο, η πρόοδος επιβραδύνθηκε τη δεκαετία του 1970 λόγω του περιορισμού των υπολογιστικών πόρων και της έλλειψης αποτελεσματικών μεθόδων εκπαίδευσης. Το ενδιαφέρον επανήλθε τη δεκαετία του 1980, ενισχυμένο από την τεχνική backpropagation των Rumelhart, Hinton και Williams και τη διαθεσιμότητα περισσότερης υπολογιστικής δύναμης [23].



Εικόνα 2 - Αρχιτεκτονική Νευρωνικών Δικτύων [24]

Τα νευρωνικά δίκτυα αναφέρονται σε μια διασυνδεδεμένη και ιεραρχική δομή στοιβάδων κόμβων ή νευρώνων που λαμβάνουν και μεταδίδουν πληροφορίες. «Το επίπεδο εισόδου, ένα ή περισσότερα κρυφά επίπεδα και ένα επίπεδο εξόδου αποτελούν μαζί την πρωταρχική αρχιτεκτονική του δικτύου» [25]. Οι νευρώνες δέχονται είσοδο, πολλαπλασιάζονται με το διάνυσμα συντελεστών βάρους, περνούν από τη συνάρτηση ενεργοποίησης και εκδίδουν στην έξοδο κάτι. Ο σύνδεσμος μεταξύ ενός νευρώνα και ενός άλλου νευρώνα είναι επίσης γνωστός ως βάρη (weights), τα βάρη εκπαιδεύονται συνεχώς με τέτοιο τρόπο ώστε η διαφορά μεταξύ του αποτελέσματος και του πραγματικού αποτελέσματος να ελαχιστοποιείται [25].

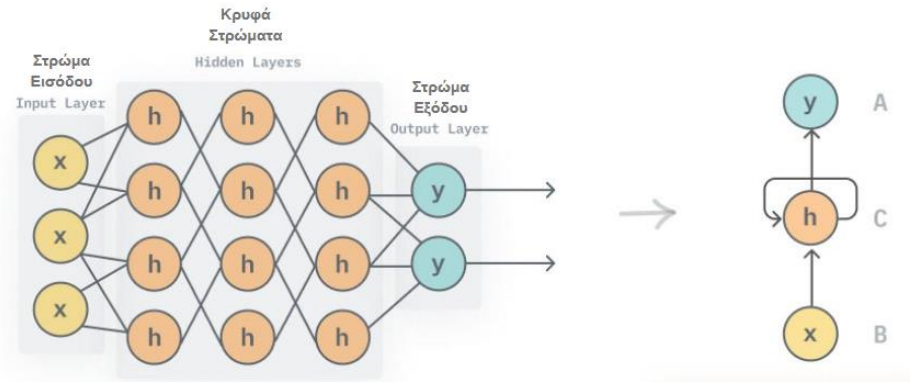
Η εκπαίδευση των νευρωνικών δικτύων γίνεται σε δύο στάδια, το εμπρόσθιο και το οπίσθιο στάδιο. Στην προς τα εμπρός διάδοση (propagation) γίνονται οι πραγματικοί υπολογισμοί στα δεδομένα που εισέρχονται στο δίκτυο για την παραγωγή μιας εξόδου. Αυτό δίνει μια ιδέα για το πόσο ακριβείς είναι οι έξοδοι σε σχέση με τον πραγματικό κόσμο και στη συνέχεια υπολογίζεται η διαφορά μεταξύ των πραγματικών και των προβλεπόμενων εξόδων. Στο αντίστροφο διάδοση, αυτό το σφάλμα περνάει προς τα πίσω μέσω του δικτύου και τα βάρη προσαρμόζονται με τρόπο ανάλογο της καθόδου κλίσης για την ελαχιστοποίηση του σφάλματος. Αυτή η διαδικασία προσαρμογής των τιμών των βαρών μεταξύ των νευρώνων με την προσδοκία καλύτερων αποτελεσμάτων πρόβλεψης ονομάζεται οπισθοδιάδοση (backpropagation) και συνεχίζεται μέχρι το δίκτυο να ικανοποιεί τα προκαθορισμένα επίπεδα απόδοσης [12].



Εικόνα 3 - CNN [26]

Τα νευρωνικά δίκτυα χρησιμοποιούνται για την ανάπτυξη εφαρμογών μέσω της μηχανικής μάθησης μαζί με τη βαθιά μάθηση. Η χρήση της βαθιάς μάθησης, ενός υποσυνόλου της μηχανικής μάθησης, σηματοδοτεί ένα σημαντικό σκαλοπάτι προς τα εμπρός με τη χρήση βαθιών νευρωνικών δικτύων (DNN) με πολλά επίπεδα για τη μοντελοποίηση σύνθετων μοτίβων και αναπαραστάσεων. Τα συνελικτικά νευρωνικά δίκτυα (CNN) και τα επαναλαμβανόμενα νευρωνικά δίκτυα (RNN) είναι εξειδικευμένοι τύποι DNN που χρησιμοποιούνται για την επεξεργασία εικόνων και διαδοχικών δεδομένων, αντίστοιχα [14].

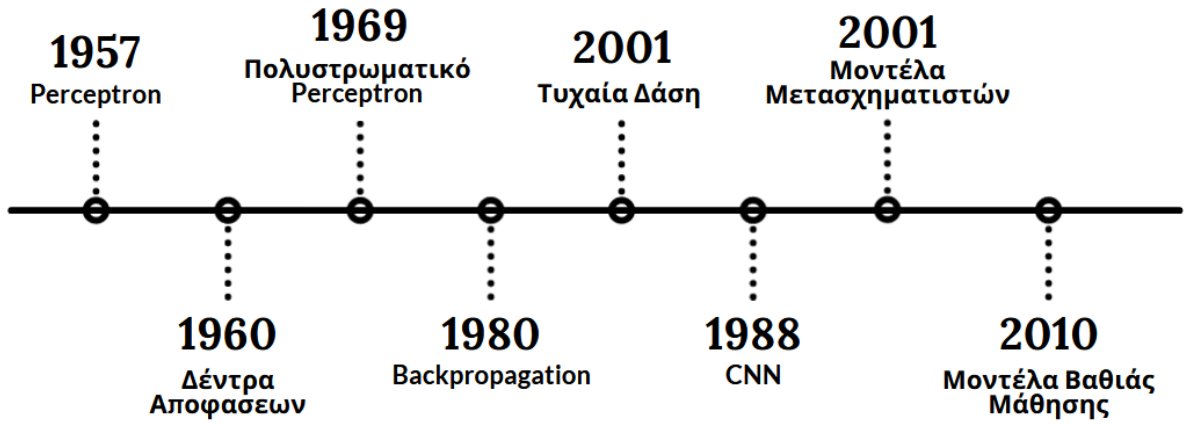
Η ανάπτυξη των νευρωνικών δικτύων βοήθησε πολύ στη βελτιστοποίηση των αποδόσεων των υπολογιστών, των GPU και των μεγάλων συνόλων δεδομένων. Αυτές οι εξελίξεις συνέβαλαν στην ικανότητα εκπαίδευσης μεγάλων δικτύων και εκπαίδευσης μοντέλων, τα οποία είναι ικανά να εκπαιδεύονται σχεδόν όπως ο ανθρώπινος εγκέφαλος [27].



Εικόνα 4 - RNN [28]

2.2.2 Μηχανική Μάθηση: Εξέλιξη και Εφαρμογές

Η μηχανική μάθηση (ML) θεωρείται ένας κλάδος της τεχνητής νοημοσύνης και αποτελεί μια από τις κυρίαρχες τεχνολογίες με τεράστιο και συνεχή ρυθμό ανάπτυξης. Η μηχανική μάθηση μπορεί να οριστεί με τα λόγια ενός από τους ιδρυτές της, του Arthur Samuel - «Η μηχανική μάθηση είναι ένα πεδίο μελέτης που δίνει στους υπολογιστές την ικανότητα να μαθαίνουν χωρίς να προγραμματίζονται» [29]. Η εργασία του στα μέσα της δεκαετίας του 1950 σε αυτό που ήταν ουσιαστικά δύο προγράμματα που έπαιζαν ντάμα βοήθησε να ανοίξει ο δρόμος προς το μέλλον της μηχανικής μάθησης που επιτρέπει στα εν λόγω προγράμματα να γίνονται καλύτερα στο να παίζουν ένα παιχνίδι.



Εικόνα 5 - Σημαντικές Ημερομηνίες στην Ιστορία της ML

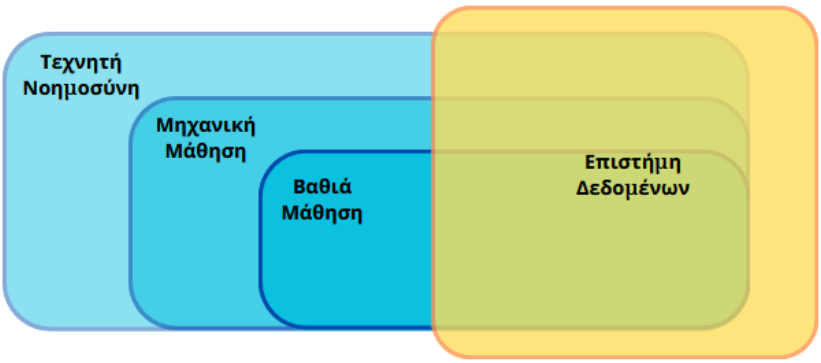
Τα πρώτα χρόνια, τα νευρωνικά δίκτυα ήταν το κύριο επίκεντρο της έρευνας και της ανάπτυξης της ML. Το Perceptron είναι ένα άλλο μοντέλο νευρωνικού δικτύου που επινοήθηκε από τον Frank Rosenblatt το 1958 με στόχο την αναγνώριση και ταξινόμηση πατρόνων [30]. Λόγω ορισμένων μειονεκτημάτων που χαρακτηρίζουν το Perceptron, συμπεριλαμβανομένης της αδυναμίας αντιμετώπισης μη γραμμικών προβλημάτων, το ενδιαφέρον και η χρηματοδότηση που κατευθύνεται προς την περαιτέρω ανάπτυξη των νευρωνικών δικτύων άρχισε να μειώνεται.

Κατά τη διάρκεια της δεκαετίας του 1990, ο τομέας άρχισε να γνωρίζει τεράστια ανάπτυξη λόγω της εμφάνισης προηγμένων αλγορίθμων και του αυξημένου αριθμού εισόδων. Νέες τεχνικές όπως τα δέντρα αποφάσεων, οι μηχανές διανυσμάτων υποστήριξης και οι μέθοδοι συνόλου έδωσαν χαρά στους ερευνητές, οι οποίοι

απέκτησαν ισχυρά εργαλεία για την επίλυση αμέτρητων προβλημάτων σε αυτό το μέτωπο [31]. Επίσης, εμφανίστηκε το θεωρητικό υπόβαθρο που ενίσχυσε την ανάπτυξη των αλγορίθμων ML.

Στη δεκαετία του 2000, τα μεγάλα δεδομένα ήρθαν μαζί με τη πρόσβαση του διαδικτύου σε ολόκληρο τον κόσμο, έτσι ο όγκος των ψηφιακών πληροφοριών αυξήθηκε ραγδαία, με αποτέλεσμα την ανάπτυξη της μηχανικής μάθησης [32]. Ένας από τους σημαντικούς τομείς της μηχανικής μάθησης είναι τα συστήματα οικιακής ασφάλειας. Χρησιμοποιώντας τη μηχανική μάθηση, τα συστήματα ασφάλειας έχουν εξελιχθεί σε έξυπνες και δυναμικές δράσεις. Τα σύγχρονα συστήματα οικιακής ασφάλειας μπορούν να ενσωματώσουν τη χρήση της μηχανικής μάθησης στον εντοπισμό απειλών σε πραγματικό χρόνο και στα αντίμετρα. Η μηχανική μάθηση το τελευταίο διάστημα συνεχίζει επίσης να βελτιώνεται λόγω της προόδου στη φύση της τεχνολογίας καθώς και της διαθεσιμότητας μεγάλου όγκου δεδομένων. Υπάρχουν διάφορες τάσεις και μελλοντικές εξελίξεις, οι οποίες τροφοδοτούν σήμερα την πρόοδο της μηχανικής μάθησης [13].

Μια αξιοσημείωτη τάση είναι η αυξανόμενη ζήτηση για τα οφέλη που μπορούν να προκύψουν από την ανάπτυξη της εξηγήσιμης AI (Explainable AI). Τελευταία, τα μοντέλα μηχανικής μάθησης έχουν γίνει πιο εξελιγμένα, αλλά με αυτή την εξελιγμένη μορφή έρχεται η ανάγκη εξήγησής τους. Η εξηγήσιμη AI είναι ένα υποπεδίο της μηχανικής μάθησης που επικεντρώνεται στην ερμηνεία των μοντέλων και των μονάδων μηχανικής μάθησης, ώστε οι χρήστες να μπορούν να τα κατανοήσουν και να έχουν εμπιστοσύνη στα αποτελέσματά τους [33]. Αυτό είναι ιδιαίτερα σημαντικό σε επαγγέλματα όπως η υγειονομική περίθαλψη και η ασφάλεια, καθώς τα λανθασμένα ή προκατειλημμένα συμπεράσματα μπορεί να είναι καταστροφικά.



Εικόνα 6 - Πεδία της AI, Μηχανική Μάθηση

2.2.3 Όραση Υπολογιστών: Τεχνικές και Εφαρμογές

Η όραση υπολογιστών ως κλάδος της τεχνητής νοημοσύνης είναι η διαδικασία μέσω της οποίας οι μηχανές είναι σε θέση να αναγνωρίζουν βίντεο ή εικόνες από τον πραγματικό κόσμο. Εμφανιζόμενες στη δεκαετία του 1960, οι πρώτες από τις εξελίξεις της μηχανικής όρασης επικεντρώθηκαν σε προκαταρκτικές διαδικασίες χειρισμού εικόνων με εργαλεία όπως η ανίχνευση ακμών και η αναγνώριση προτύπων. Μεγαλύτερη πρόοδος προέκυψε κυρίως με την εμφάνιση της μηχανικής μάθησης και της βαθιάς μάθησης για την ανακάλυψη νέων μοτίβων στην αναγνώριση οπτικών πληροφοριών. Με τις τρέχουσες εξελίξεις, η όραση υπολογιστών έχει καθοριστικό ρόλο σε διάφορες εφαρμογές, όπως η ασφάλεια στο σπίτι, η υγειονομική περίθαλψη και τα αυτόνομα οχήματα [34].

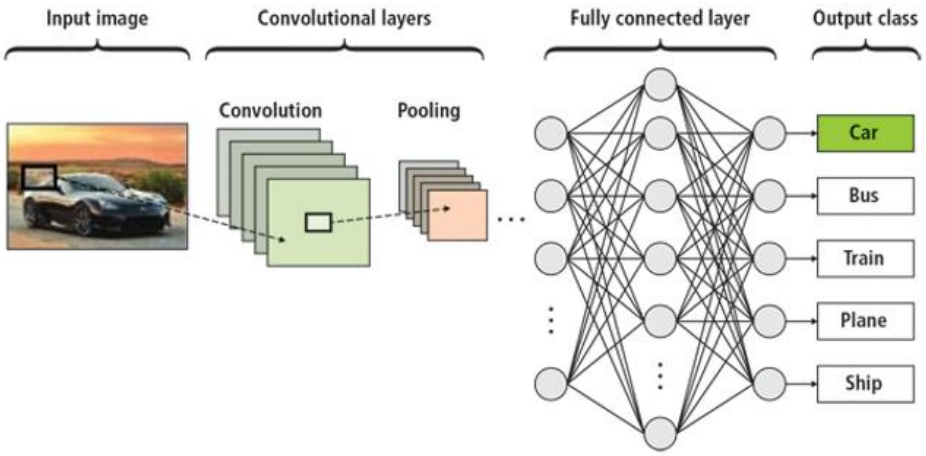
Η υπολογιστική όραση συνήθως ακολουθεί μια δομημένη διαδικασία: ανάγνωση εικόνας, επεξεργασία, εξαγωγή χαρακτηριστικών και ερμηνεία. Η ανάγνωση εικόνας αναφέρεται στη διαδικασία σύλληψης πληροφοριών εικόνας ή βίντεο με χρήση μιας κάμερας ή μιας αισθητήριας για την παροχή εξόδου σήματος εικόνας ή βίντεο. Η επεξεργασία αυτών των εικόνων γίνεται με διάφορους τρόπους όπως η αφαίρεση θορύβου, η ρύθμιση αντίθεσης και η παραμόρφωση εικόνας ως προετοιμασία για την ανάλυση [35]. Η εξαγωγή χαρακτηριστικών περιλαμβάνει τη διαδικασία αναγνώρισης μόνο συγκεκριμένων χαρακτηριστικών της εικόνας ή χαρακτηριστικών όπως ακμές, υφές ή ορισμένα αντικείμενα. Οι μέθοδοι που χρησιμοποιούνται τακτικά περιλαμβάνουν τη χρήση αλγορίθμων όπως ο τελεστής Sobel[1] για την ανίχνευση ακμών καθώς και αλγορίθμων ανίχνευσης γωνιών. Τέλος, η ερμηνεία συνεπάγεται τη χρήση αυτών των χαρακτηριστικών για διαδικασίες λήψης αποφάσεων ή πρόβλεψης με τη χρήση μοντέλων τεχνητής νοημοσύνης, κυρίως των νευρωνικών δικτύων συνελίξεων (CNN). Συγκεκριμένα, τα CNNs είναι πολύ πολύτιμα για οπτικές εργασίες λόγω της αρχιτεκτονικής τους στην οποία τα χαρακτηριστικά μαθαίνονται σε στρώματα από τις ακμές προς τα αντικείμενα κατά τη διάρκεια της οπισθοδιάδοσης [36].

Η όραση υπολογιστών έχει αποκτήσει σημαντικό ρόλο στην αύξηση της ευαισθησίας και του ελέγχου των απειλών στην ασφάλεια του σπιτιού. Τα συστήματα ασφαλείας

[1] Sobel operator: Ανιχνεύει ακμές χρησιμοποιώντας φίλτρα κλίσης με συνελικτική ανάλυση.

στον σύγχρονο κόσμο ενσωματώνουν βιντεοκάμερες με λειτουργίες της όρασης υπολογιστή για την αναγνώριση προσώπων, την παρακολούθηση διαφόρων δραστηριοτήτων και δυνητικά απειλητικών καταστάσεων. Για παράδειγμα, οι αισθητήρες PIR[2] μπορούν να διακρίνουν μεταξύ ανθρώπων, ζωντανών και μη ζωντανών οντοτήτων, μειώνοντας έτσι τους ψευδείς συναγερμούς και ενισχύοντας την πολυπλοκότητα του συστήματος ασφαλείας [37].

Η τεχνολογία της όρασης υπολογιστών δεν βοηθά μόνο στη βελτίωση της οικιακής ασφάλειας, αλλά είναι σημαντική και σε άλλους τομείς. Για παράδειγμα, στον τομέα της υγειονομικής περίθαλψης είναι χρήσιμη για την ανάλυση εικόνων και μπορεί να χρησιμοποιηθεί για τον εντοπισμό διαταραχών που θα μπορούσαν να είναι όγκοι σε μια ακτινογραφία ή σε μια μαγνητική τομογραφία [16]. Επίσης, τα αυτοκινούμενα αυτοκίνητα χρησιμοποιούν μοντέλα πρόβλεψης που βασίζονται σε εισροές από ένα συνδυασμό αισθητήρων για τον εντοπισμό αντικειμένων στο δρόμο και τη δημιουργία αποφάσεων σε πραγματικό χρόνο [38].



Εικόνα 7 - Παράδειγμα Λειτουργίας της Όρασης Υπολογιστών [39]

Σε αυτόν τον τομέα, η τεχνολογία θα στηριχθεί στην όραση των υπολογιστών, αντικατοπτρίζοντας τις αλλαγές που παρατηρούνται στην επαυξημένη πραγματικότητα (AR) και την εικονική πραγματικότητα (VR), οι οποίες χρησιμοποιούν οπτικά δεδομένα για τη δημιουργία εικονικής υλικής πραγματικότητας. Η υπολογιστική

[2] Ο αισθητήρας PIR ανιχνεύει την κίνηση χρησιμοποιώντας ακτινοβολία υπέρυθρων.

όραση έχει δυνατότητες στον υπολογισμό των άκρων, που είναι απαραίτητος για την άμεση επεξεργασία βίντεο στα αυτοκινούμενα αυτοκίνητα και στις έξυπνες κάμερες [40].

Εν κατακλείδι, η όραση υπολογιστών είναι ένα συναρπαστικό μέρος της τεχνητής νοημοσύνης, που εκπαιδεύει μηχανές από δεδομένα εικόνας. Οι χρήσεις της εκτείνονται από την ασφάλεια του σπιτιού έως την υγειονομική περίθαλψη και τα αυτοκινούμενα αυτοκίνητα, υποδηλώνοντας τις τεράστιες δυνατότητές της. Η συνεχιζόμενη έρευνα και οι τεχνολογικές εξελίξεις υποδηλώνουν ακόμη βαθύτερες επιπτώσεις στο μέλλον.

2.3 Τεχνικές της Ανίχνευσης Προσώπου

Η ανίχνευση προσώπου είναι μια από τις μεθόδους αναγνώρισης προτύπων και όρασης υπολογιστών η οποία τα τελευταία 50 χρόνια εξελίσσεται συνέχεια. Στις αρχές του 1970, η ανίχνευση προσώπου ήταν ένα πρόβλημα αναγνώρισης μοτίβων 2D. Για την ανίχνευση των προσώπων υπολογιζόταν η απόσταση μεταξύ των ματιών ή άλλων σημαντικών σημείων ως βάση [41].

2.3.1 Eigenfaces

Το 1991, ο Matthew Turk και ο Alex Pentland έφεραν επανάσταση στον τομέα της μηχανικής μάθησης με την πρωτοποριακή εργασία τους για την επίτευξη της πρώτης επιτυχημένης ανίχνευσης προσώπου με τη χρήση Eigenfaces [42]. Αυτό το σημείο αναφοράς σηματοδότησε ένα σημαντικό άλμα προς τα εμπρός στην όραση υπολογιστών, ανοίγοντας τις πόρτες σε ένα ευρύ φάσμα εφαρμογών που βασίζονται στην αυτοματοποιημένη αναγνώριση προσώπου.

Εικόνα 8 - Γραμμικός Συνδυασμός των Eigenfaces [43]

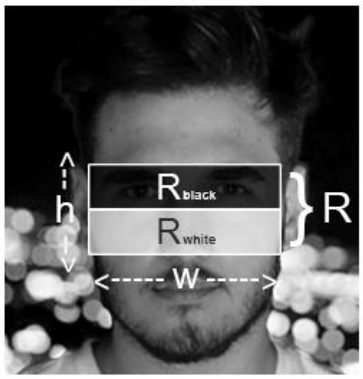
Η προσέγγισή τους επικεντρώθηκε γύρω από την έννοια των Eigenfaces, ένας όρος που προέρχεται από τη μαθηματική έννοια των ιδιοδιανυσμάτων. Υπολογίζοντας τα ιδιοδιανύσματα ενός πίνακα συνδιακύμανσης που προέρχεται από ένα σύνολο εικόνων προσώπου, οι Turk και Pentland αποκάλυψαν τα υποκείμενα μοτίβα και τις

δομές που ενυπάρχουν στα ανθρώπινα πρόσωπα [42]. Αυτά τα ιδιοδιανύσματα, ή ιδιοπρόσωπα, αντιπροσώπευαν τις κύριες συνιστώσες της παραλλαγής του προσώπου εντός του συνόλου δεδομένων.

2.3.2 Αλγόριθμος Viola-Jones

Ο Paul Viola και ο Michael Jones έκαναν μια σημαντική ανακάλυψη στο πρόσωπο με την ανάπτυξη του αλγορίθμου Viola-Jones το 2001, μια δεκαετία μετά το Eigenfaces των Turk και Pentland. Αυτός ο αλγόριθμος, γνωστός για την αποτελεσματικότητα και την αποδοτικότητά του, λειτουργεί μέσω δύο διακριτά στάδια: *εκπαίδευση* και *αναγνώριση* [44].

Κατά τη διάρκεια της φάσης εκπαίδευσης, ο αλγόριθμος μαθαίνει να εντοπίζει συγκεκριμένα χαρακτηριστικά σε εικόνες που είναι ενδεικτικά της παρουσίας ενός προσώπου. Αυτά τα χαρακτηριστικά, που συχνά αναφέρονται ως χαρακτηριστικά Haar-like, περιλαμβάνουν μοτίβα όπως ακμές, γωνίες και υφές που εμφανίζονται συνήθως σε περιοχές του προσώπου [45]. Μέσω επαναληπτικής εκπαίδευσης σε ένα ποικίλο σύνολο δεδομένων, ο αλγόριθμος προσαρμόζει τις παραμέτρους του ώστε να αναγνωρίζει με ακρίβεια αυτά τα χαρακτηριστικά του προσώπου.



$$F_{\text{haar}} = \frac{E(R_{\text{black}}) - E(R_{\text{white}})}{w \cdot h \cdot \sqrt{|E(R_\mu)^2 - E(R_\mu)^2|}}$$

Εικόνα 9 - Υπολογισμός Haar-like Χαρακτηριστικών

Αφού εκπαιδευτεί, ο αλγόριθμος Viola-Jones προχωρά στο στάδιο της ανίχνευσης προσώπου, όπου εφαρμόζει τους μαθημένους ανιχνευτές χαρακτηριστικών για την ανάλυση των εισερχόμενων εικόνων σε πραγματικό χρόνο [19]. Ο αλγόριθμος σαρώνει την εικόνα με υποπαράθυρα διαφόρων μεγεθών παραθύρων, οποία συνήθως είναι 24x24 pixels, και εξάγει τα δεδομένα αυτά για να υποβάλλονται σε επεξεργασία και έτσι εκτιμάται αν υπάρχει πρόσωπο στο συγκεκριμένο καρέ ή όχι. Οι εκτιμήσεις των χαρακτηριστικών που εξάγονται είναι πάνω από 160.000 [46].

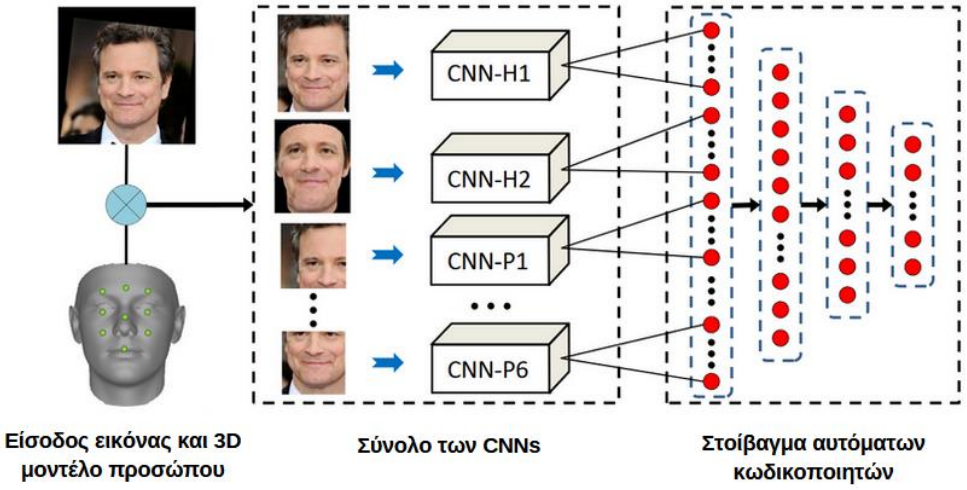
Αξιολογώντας την παρουσία και τη διάταξη αυτών των χαρακτηριστικών εντός της εικόνας, ο αλγόριθμος καθορίζει αν υπάρχει πρόσωπο και, αν ναι, τη θέση και τον προσανατολισμό του. Μια βασική καινοτομία του αλγορίθμου Viola-Jones είναι η ικανότητά του να θέτει ένα ελάχιστο κατώφλι για την ανίχνευση χαρακτηριστικών, ενισχύοντας έτσι την ανθεκτικότητά του στις μεταβολές του φωτισμού, της στάσης και της έκφρασης του προσώπου [47]. Αυτός ο προσαρμοστικός μηχανισμός καθορισμού κατωφλίου επιτρέπει στον αλγόριθμο να επιτυγχάνει υψηλή ακρίβεια στην ανίχνευση προσώπου σε διαφορετικές συνθήκες.

Παρά τις αξιοσημείωτες επιδόσεις του, ο αλγόριθμος Viola-Jones δεν είναι χωρίς περιορισμούς. Μια αξιοσημείωτη πρόκληση είναι η ευαισθησία του σε ψευδώς θετικά αποτελέσματα, όπου μη-πρόσωπα αντικείμενα ή μοτίβα μπορεί λανθασμένα να ενεργοποιήσουν τον μηχανισμό ανίχνευσης προσώπου. Για να μετριάσουν αυτόν τον κίνδυνο, οι Viola και Jones εκπαίδευσαν σχολαστικά τον αλγόριθμό τους σε ένα τεράστιο σύνολο δεδομένων που περιλαμβάνει εικόνες χωρίς πρόσωπο [48]. Εκθέτοντας τον αλγόριθμο σε ένα ευρύ φάσμα μη-προσωπικών χαρακτηριστικών, επιδίωξαν να ενισχύσουν την ικανότητά του να διακρίνει μεταξύ γνήσιων προσώπων και ψευδών ανιχνεύσεων.

Εν ολίγοις, ο αλγόριθμος Viola-Jones αποτελεί σημαντικό κομμάτι της όρασης υπολογιστών, αποδεικνύοντας τη δύναμη της μηχανικής μάθησης και της αναγνώρισης προτύπων στο πεδίο της ανίχνευσης προσώπων. Η ικανότητά του να λειτουργεί σε πραγματικό χρόνο και η στιβαρή απόδοσή του υπό δύσκολες συνθήκες έχουν εδραιώσει τη θέση του ως τεχνολογία ακρογωνιαίου λίθου σε εφαρμογές που καλύπτουν την ασφάλεια, την επιτήρηση και την αλληλεπίδραση ανθρώπου-υπολογιστή.

2.4 Τεχνικές της Αναγνώρισης Προσώπου

Η αναγνώριση προσώπου είναι ένα σημαντικό υποπεδίο της όρασης υπολογιστών ή και της τεχνητής νοημοσύνης, καθώς ο κύριος στόχος της μεθόδου είναι η αναγνώριση προσώπων από εικόνες ή βίντεο. Επιπλέον και με τη χρήση της τεχνολογίας LIDAR, είναι δυνατή η λήψη ακριβών τρισδιάστατων πληροφοριών χώρου, συμπληρώνοντας αυτά τα συστήματα με την ενίσχυση της αντίληψης βάθους και των δυνατοτήτων ανίχνευσης των στόχων. Πρόκειται για μια τεχνολογία που κατέχει βαθιά σημασία σε πολυάριθμους τομείς, όπως στους τομείς της ασφάλειας, της ιατρικής και των μοναδικών υπηρεσιών. Επομένως, παρά τις ομοιότητες με την ανίχνευση προσώπου που αναγνωρίζει ότι ένα πρόσωπο υπάρχει σε μια δεδομένη εικόνα, η έννοια της αναγνώρισης προσώπου υπονοεί την αναγνώριση ή την επαλήθευση του προσώπου στην εικόνα. Η διαδικασία περιλαμβάνει την εξαγωγή χαρακτηριστικών και την αναγνώριση προσώπου με χρήση μοντέλων μηχανικής μάθησης και βαθιάς μάθησης για τη σύγκριση σχημάτων προσώπου σε μια βάση δεδομένων [49].



Εικόνα 10 - Διάγραμμα Ροής του Πλαισίου της Προτεινόμενης Πολυτροπικής Βαθιάς Αναπαράστασης Προσώπου (MM-DFR) με τη Χρήση Ενός Συνόλου CNNs [50]

Η αναγνώριση προσώπου περιλαμβάνει συνήθως διάφορα βασικά βήματα: ταυτοποίηση προσώπου, τοπικός περιορισμός νευρωνικού πεδίου, εξαγωγή χαρακτηριστικών και ομοιότητα συνημίτονου. Η πρώτη λειτουργία είναι επομένως η αναγνώριση προσώπου σε μια εικόνα ή ένα βίντεο [4]. Αυτό το βήμα είναι σημαντικό

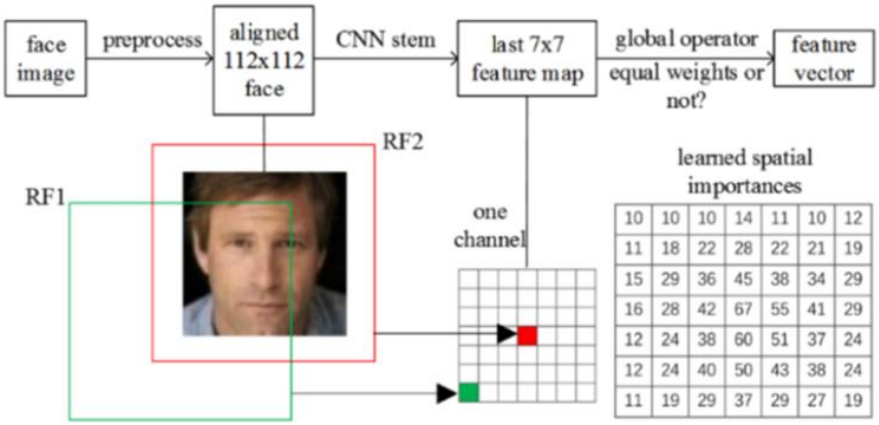
επειδή παρέχει σαφή διαχωρισμό της περιοχής του προσώπου από το φόντο. Για το σκοπό αυτό μπορούν να χρησιμοποιηθούν εφαρμογές όπως ο αλγόριθμος Viola-Jones, όπως αναφέρθηκε στο προηγούμενο κεφάλαιο.

Μετά την αναγνώριση προσώπου, το επόμενο βήμα είναι η ευθυγράμμιση του προσώπου, ώστε όλα τα χαρακτηριστικά του να τοποθετηθούν στη σωστή θέση. Αυτό περιλαμβάνει την εφαρμογή προσαρμογών όπως η αλλαγή μεγέθους και η περιστροφή του προσώπου σε κανονική θέση. Αυτή η στοίχιση οδηγεί σε μείωση της απόκλισης που προκαλείται από αυτή τη στάση και βοηθά στην επίτευξη καλύτερης ακρίβειας αναγνώρισης στην επόμενη φάση [44]. Η εξαγωγή χαρακτηριστικών γίνεται για τον εντοπισμό χαρακτηριστικών που μπορούν να χρησιμοποιηθούν για τον διαχωρισμό ενός προσώπου από ένα άλλο. Ορισμένες πτυχές μπορεί να είναι το πλάτος μεταξύ των ματιών, το διάφραγμα και η δομή της μύτης, η καμπυλότητα και ο όγκος των χειλιών και η τραχύτητα ή η απαλότητα του δέρματος του προσώπου [49]. Τα συγκεκριμένα χαρακτηριστικά που εξάγονται για την αναγνώριση προσώπου έχουν εξελιχθεί αρκετά με τα μοντέλα βαθιάς μάθησης, όπου έχουν βελτιώσει αυτή τη διαδικασία μαθαίνοντας μόνα τους τα καλύτερα χαρακτηριστικά. Ορισμένα από τα σημαντικότερα μοντέλα περιλαμβάνουν τα VGG-Face, FaceNet, DeepFace [51].

Η τελευταία διαδικασία είναι η αντιστοίχιση αυτών των χαρακτηριστικών με τη βάση δεδομένων προσώπων που έχει ανακτηθεί προηγουμένως. Αυτό γίνεται συχνά με τη χρήση μιας τεχνολογίας που ονομάζεται μέτρο ομοιότητας, όπως για παράδειγμα η ευκλείδεια απόσταση ή η ομοιότητα συνημίτονου. Γίνεται ανάλυση ευαισθησίας του αποτελέσματος ομοιότητας και αν το αποτέλεσμα ξεπεράσει ένα ορισμένο όριο, δηλώνεται ταύτιση [12].

Τα συστήματα αναγνώρισης προσώπου θεωρούνται σημαντικά για την ανάπτυξη και την επέκτασή τους στο πλαίσιο της βαθιάς μάθησης και της μηχανικής μάθησης. Οι αλγόριθμοι βιομετρικής σάρωσης και ειδικότερα οι αλγόριθμοι αναγνώρισης προσώπου αναπτύσσονται με βάση μεγάλα σύνολα δεδομένων εικόνων που έχουν ήδη επισημανθεί ή χαρακτηριστεί έτσι ώστε οι μηχανές να μαθαίνουν το ένα πρόσωπο σε σύγκριση με το άλλο. Αυτά τα συγκεκριμένα μοντέλα αποτελούνται από πολυάριθμα στρώματα νευρώνων και καθώς προχωρά το ένα στρώμα στο επόμενο, αποκτά ακόμα πιο εξελιγμένα χαρακτηριστικά [12]. Η μάθηση με επίβλεψη είναι η πιο χρησιμοποιούμενη προσέγγιση στην εκπαίδευση μοντέλων αναγνώρισης

προσώπων, επειδή το σύνολο δεδομένων έχει εικόνες και την ταυτότητα των ατόμων. Αυτό επιτρέπει στο μοντέλο να συσχετίζει σωστά τα πρόσωπα με συγκεκριμένα διαφορετικά άτομα όταν είναι στο μοντέλο [14].



Εικόνα 11 - Αλγόριθμος Αναγνώρισης Προσώπου [52]

Η τεχνολογία αναγνώρισης προσώπου μπορεί να ενσωματωθεί χωρίς προβλήματα στα οικιακά συστήματα ασφαλείας για να ενισχύσει την ασφάλεια και την ευκολία. Η αναγνώριση προσώπου μπορεί να χρησιμοποιηθεί για τον έλεγχο πρόσβασης σε έξυπνα σπίτια. Συνδέοντας το διαδικτυακό σύστημα με κάμερες κουδουνιού και έξυπνες κλειδαριές, το σύστημα είναι σε θέση να αναγνωρίζει και να επιτρέπει την είσοδο στα επιτρεπόμενα άτομα χωρίς τη χρήση κλειδιών ή κωδικών πρόσβασης [53]. Τα συστήματα ασφαλείας αναγνώρισης προσώπου στο σπίτι βοηθούν επίσης στο να διασφαλιστεί ότι δεν επιτρέπεται η είσοδος σε άγνωστα άτομα στους χώρους, καθώς μπορούν να παρακολουθούνται από τα συστήματα ασφαλείας που είναι εγκατεστημένα στο σπίτι συνεχώς. Σε περίπτωση ανίχνευσης ενός άγνωστου προσώπου, το σύστημα μπορεί να εκδώσει ειδοποιήσεις στους ιδιοκτήτες του σπιτιού ή σε άλλο προσωπικό [54].

Παρόλο που οι ερευνητές και οι προγραμματιστές έχουν δημιουργήσει αποτελεσματικά συστήματα αναγνώρισης προσώπου, τα ακόλουθα τεχνικά ζητήματα επηρεάζουν την αποτελεσματικότητα του συστήματος. Η ανίχνευση με υψηλή ακρίβεια υπό διαφορετικές συνθήκες φωτισμού και μη δύσκαμπτων κινήσεων ή εκφράσεων του κεφαλιού εξακολουθεί να αποτελεί πρόβλημα. Ορισμένες από αυτές τις μεταβολές περιλαμβάνουν, παρά το γεγονός αυτό συνεχίζονται ακόμη οι εργασίες για τη

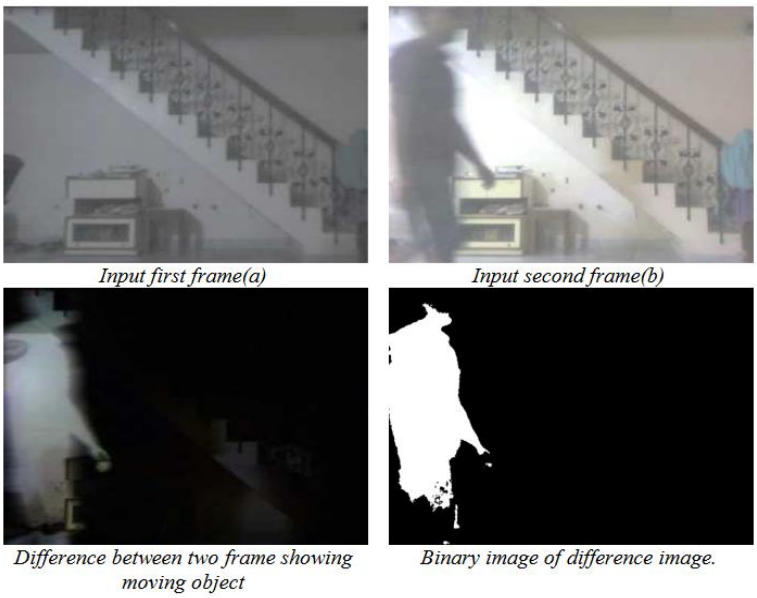
δημιουργία ισχυρότερων αλγορίθμων που μπορούν να προσαρμοστούν σε αυτές τις μεταβολές. Αυτές οι μεταβολές περιλαμβάνουν αρκετές έρευνες που εξακολουθούν να διεξάγονται με στόχο τη δημιουργία καλύτερων αλγορίθμων που μπορούν να αντιμετωπίσουν τις παραπάνω μεταβολές [55]. Στην παρούσα φάση η χρήση της αναγνώρισης προσώπου είναι υψηλή και αυτό κάνει πολλούς ανθρώπους να φοβούνται για την ιδιωτική τους ζωή. Υπάρχει μια αυξανόμενη έκκληση για καλύτερη ρύθμιση της τεχνολογίας και για την τήρηση κατάλληλου κώδικα δεοντολογίας από όσους χρησιμοποιούν την τεχνολογία, ώστε να μην παραβιάζεται η ιδιωτική ζωή των ανθρώπων [56]. Στην τρέχουσα κατάστασή τους, τα συστήματα αναγνώρισης προσώπου είναι γνωστό ότι παρουσιάζουν σφάλματα με βάση τη φυλή, το φύλο και την ηλικία [45]. Έχουν αναληφθεί πρωτοβουλίες για την αύξηση της διαφοροποίησης των δεδομένων, καθώς και για τον σχεδιασμό αλγορίθμων μηχανικής μάθησης με ελάχιστη δυνατή επιφύλαξη. Μια από τις αυστηρές ανάγκες σε εφαρμογές όπως η επιτήρηση και η ασφάλεια στο σπίτι είναι η επεξεργασία σε πραγματικό χρόνο. Αυτή η πρόκληση αντιμετωπίζεται μέσω της νέας ανάπτυξης στον υπολογισμό ακμών και των βελτιστοποιημένων αρχιτεκτονικών νευρωνικών δικτύων [57].

Συμπερασματικά, η αναγνώριση προσώπου είναι μια ισχυρή και σύνθετη τεχνολογία, η οποία διαπερνά τον τομέα της ασφάλειας, της υγειονομικής περίθαλψης, του λιανικού εμπορίου και άλλους. Λόγω της αποτελεσματικότητάς της στην εκμάθηση χαρακτηριστικών από εικόνες, η βαθιά μάθηση καθιστά το σύστημα αναγνώρισης προσώπου ικανό να προσφέρει αξιόπιστη και ακριβή ταυτοποίηση. Γι' αυτό και ο ρόλος της τεχνολογίας πρόκειται να γίνει όλο και πιο σημαντικός στη ζωή των ανθρώπων, βελτιώνοντας την ασφάλεια των ατόμων και παρέχοντας στους ανθρώπους εξατομικευμένες υπηρεσίες καθ' όλη τη διάρκεια της διαδικασίας υπέρβασης των τεχνικών και ηθικών ζητημάτων που προκύπτουν [58].

2.5 Προηγμένες Τεχνικές στην Τεχνολογία Ανίχνευσης Κίνησης

Η ανίχνευση κίνησης είναι μια βασική τεχνολογία που χρησιμοποιείται σε διάφορα συστήματα ασφαλείας, συμπεριλαμβανομένης της οικιακής ασφάλειας, της επιτήρησης και του αυτοματισμού. Περιλαμβάνει τη χρήση αισθητήρων και αλγορίθμων για την ανίχνευση κίνησης σε μια καθορισμένη περιοχή, με αποτέλεσμα την ενεργοποίηση συναγερμών, την καταγραφή συμβάντων και την αποστολή ειδοποίησης στους χρήστες σε πιο νέες τεχνολογίες. Ενώ η ανίχνευση κίνησης μπορεί να επιτευχθεί με διάφορες μεθόδους, όπως αισθητήρες υπέρυθρων και ραντάρ, υπάρχουν επίσης συστήματα που ανιχνεύουν την κίνηση από εικόνες χρησιμοποιώντας βιντεοκάμερες και προηγμένες τεχνικές επεξεργασίας εικόνας.

Υπάρχουν αρκετοί τρόποι ανίχνευσης της κίνησης και ο πιο συνηθισμένος είναι η χρήση βιντεοκάμερας. Το κεντρικό σημείο εντοπίζεται στη σύγκριση κάθε καρέ βίντεο με το προηγούμενο με σκοπό τον εντοπισμό εμφανών αλλαγών ή κίνησης. Η υλοποίησή του περιλαμβάνει τη χρήση των αλγορίθμων αφαίρεσης υποβάθρου, οπτικής ροής και διαφοράς καρέ για την ελαχιστοποίηση των ψευδών συναγερμών και τη μεγιστοποίηση της πιθανότητας ανίχνευσης.



Εικόνα 12 - Ανίχνευση Κίνησης με Βάση τη Μέθοδο Διαφοράς Καρέ [78]

Η οπτική ροή αναλυτικότερα, υπολογίζει τη ροή από το ένα καρέ στο επόμενο ακολουθώντας την κίνηση των διαφορών των κάθε εικονοστοιχείων. Η μέθοδος έχει υψηλή πυκνότητα πληροφορίας κίνησης, οποία συνοδεύεται από υπολογιστικό κόστος που δημιουργεί καθυστέρηση. Για αυτόν τον λόγο, για να είναι ακριβής, παρέχει λιγότερο ακριβή αποτελέσματα με κάποιο περιθώριο, για να είναι ταχύτερη [59]. Αν και εξακολουθεί να αποδεικνύεται αποτελεσματική από άποψη χρόνου, δεν είναι τόσο

αποτελεσματική στην αντιμετώπιση της πολυπλοκότητας και του θορύβου στα δεδομένα. Ομοίως, τροποποιήσεις όπως οι μορφολογικές πράξεις μπορούν να χρησιμοποιηθούν για την αντιμετώπιση των ζητημάτων θορύβου [20]. Όταν η διαφοροποίηση καρέ ενσωματώνεται σε άλλους αλγορίθμους, όπως η αφαίρεση του φόντου, τότε είναι πιο ισχυρή.

Η αφαίρεση φόντου είναι μια μέθοδος κατά την οποία το σύστημα διατηρεί συνεχώς μοντέλα για το στατικό φόντο, χωρίς αντικείμενα σε κίνηση. Στη συνέχεια, τα ζωντανά καρέ βίντεο αφαιρούνται από αυτό το μοντέλο φόντου για τον εντοπισμό κινούμενων αντικειμένων στο τρέχον καρέ. Η μέθοδος αυτή περιλαμβάνει την ενσωμάτωση μιας μονάδας αφαίρεσης υποβάθρου που πρέπει να ενημερώνεται τακτικά ανάλογα με τις αλλαγές στις συνθήκες φωτισμού ή στο φυσικό περιβάλλον. Για να επιτευχθεί αυτό, χρησιμοποιείται το Gaussian Mixture Model, καθώς μοντελοποιεί το φόντο με πιθανότητα και μπορεί να προσαρμόσει το μοντέλο φόντου ανάλογα με τις σταδιακές αλλαγές στο φωτισμό και την επαναλαμβανόμενη κίνηση [60]. Αυτό καθιστά την αφαίρεση φόντου εξαρτώμενη από την ικανότητα ακριβούς μοντελοποίησης του φόντου και την ανάγκη με την οποία πρέπει να γίνει η μοντελοποίηση.

Τα μοντέρνα συστήματα έχουν ενσωματώσει τη χρήση μηχανικής μάθησης, και πιο συγκεκριμένα νευρωνικά δίκτυα συνελίξεων (CNN), για να βελτιώσουν την ακρίβεια. Καθώς τα CNN είναι σε θέση να μαθαίνουν χαρακτηριστικά κίνησης διαφορετικής πολυπλοκότητας από δεδομένα εκπαίδευσης χωρίς άμεση οδηγία, μπορεί να ταξινομεί τις κινήσεις, περιλαμβάνοντας συνήθως την προεπεξεργασία ενός καρέ και την εξαγωγή των χαρακτηριστικών [61]. Οι εξελίξεις στα σχέδια ανίχνευσης κίνησης εξακολουθούν να υφίστανται μέσω της χρήσης του νευρωνικού δικτύου.

Μέσω της ενσωμάτωσης αισθητήρων υψηλής τεχνολογίας, μαθηματικών εξισώσεων και AI, τα σημερινά συστήματα ανίχνευσης κίνησης είναι σε θέση να προσφέρουν πολύ υψηλότερες ποιότητες παρακολούθησης. Η πρόοδος και η εξέλιξη της τεχνολογίας μπορούν σαφώς να εκφράσουν ότι στην κατάλληλη πορεία μπορεί να υπάρξουν περαιτέρω εξελίξεις που μπορούν να βελτιώσουν τη συνολική αποδοτικότητα αυτού του τύπου συστήματος ανίχνευσης κίνησης.

3. Μεθοδολογία

Σε αυτό το κεφάλαιο αναλύονται οι λεπτομέρειες της προτεινόμενης μεθόδου και η εφαρμογή των διάφορων βημάτων. Αρχικά, η ιδέα της ανάπτυξης ενός ψηφιακού συστήματος συναγερμού ασφαλείας προήλθε από τις ανησυχίες των φοιτητών που κατοικούν σε φοιτητικές εστίες με επικίνδυνες καταστάσεις. Ταυτόχρονα, στοχεύει στην κάλυψη των αναγκών ασφαλείας όλων των ατόμων που ενδιαφέρονται να προστατεύσουν τον ιδιωτικό τους χώρο, προσπαθώντας παράλληλα να τα δημιουργήσουν όλα αυτά με μια οικονομική λύση. Προκειμένου να σχεδιαστεί η εφαρμογή για το ψηφιακό σύστημα συναγερμού ασφαλείας, εξετάστηκε μια τεχνολογική ανάλυση των δυνατοτήτων δημιουργίας μιας εφαρμογής βασισμένης στην τεχνητή νοημοσύνη, σε συνδυασμό με την όραση υπολογιστών και τη μηχανική μάθηση. Συνεχίζοντας, εκτελέστηκε βιβλιογραφική ανασκόπηση σχετικά με το τεχνικό κομμάτι για την χρήση κατάλληλου εξοπλισμού συσκευών.

Αυτή η μεθοδολογία αντιμετωπίζει την πτυχή της ασφάλειας των τελικών χρηστών καθ' όλη τη διάρκεια της φάσης έρευνας και ανάπτυξης, ώστε να ληφθούν υπόψη τα μέτρα ασφαλείας στο οικιακό χώρο. Ωστόσο, έπειτα από την έρευνα του εξοπλισμού συσκευών, οι Android συσκευές επιλέχθηκαν κατάλληλες για την υλοποίηση. Πραγματοποιήθηκαν συνεντεύξεις με ενδιαφερόμενους χρήστες για συλλογή πληροφοριών σχετικά με τους κινδύνους και προκλήσεις για τους ιδιωτικού τους χώρο. Οι συνεντεύξεις αυτές βοήθησαν επίσης στην εξεύρεση των χαρακτηριστικών και των απαιτούμενων λειτουργιών που πρέπει να συμπεριληφθούν στην εφαρμογή του ψηφιακού συστήματος συναγερμού ασφαλείας.

Ύστερα από τον καθορισμό των απαιτήσεων, πραγματοποιήθηκε ανάλυση της αγοράς για παρόμοιες εφαρμογές με τον στόχο που είχε τεθεί. Αυτή η έρευνα παρέχει πληροφορίες για την βελτίωση αλλά και για πιθανά προβλήματα που πρέπει να αποφευχθούν κατά τη διαδικασία σχεδιασμού και ανάπτυξης. Για την ευρύτερη δυνατή χρήση της εφαρμογής, αλλά και για την αξιοπιστία των συσκευών Android, η εφαρμογή θα σχεδιαστεί έτσι ώστε να εκτελεί όλες τις λειτουργίες μέσω της κάμεράς της. Έπειτα, έγινε η ανάλυση των απαιτήσεων, ο σχεδιασμός και η ανάπτυξη της εφαρμογής. Το στάδιο αυτό περιλαμβάνει τον καθορισμό της δομής, την οργάνωση των βασικών αλγορίθμων τεχνητής νοημοσύνης, προκειμένου να δημιουργηθεί ένα

απλό σύστημα στην πλοήγηση, στη χρήση, αλλά και καθώς η ανάπτυξη αφορά την ασφάλεια του οικιακού χώρου, την ασφάλεια των δεδομένων του χρήστη.

Επιπλέον, επειδή η εφαρμογή του ψηφιακού συστήματος συναγερμού ασφαλείας πρέπει να λειτουργεί συνεχώς σε συσκευές Android, η διαχείριση της χρήσης της μνήμης και η αποτελεσματική επεξεργασία των εικόνων είναι εξαιρετικά σημαντική.

Τέλος, πραγματοποιήθηκαν δοκιμές χρήσης με τους χρήστες για την αξιολόγηση των σχεδιαστικών αποφάσεων και την αντιμετώπιση τυχόν προβλημάτων χρήσης, διασφαλίζοντας ότι η εφαρμογή ανταποκρίνεται στις ανάγκες των χρηστών.

3.1 Ερευνητικά Στάδια

Στα πρώτα ερευνητικά στάδια της ανάπτυξης του ψηφιακού συστήματος συναγερμού ασφαλείας, πραγματοποιήθηκε μια ολοκληρωμένη έρευνα για την κατανόηση των τεχνολογικών και πρακτικών απαιτήσεων που απαιτούνται για την επιτυχή εφαρμογή του συστήματος. Το στάδιο αυτό περιλαμβάνει επίσης μια εκτεταμένη βιβλιογραφική ανασκόπηση με έμφαση στις τεχνικές πτυχές της δημιουργίας μιας εφαρμογής που χρησιμοποιεί τεχνητή νοημοσύνη, όραση υπολογιστών και μηχανική μάθηση. Στόχος ήταν να εντοπιστούν οι καταλληλότερες τεχνολογικές προσεγγίσεις και συσκευές που θα εξασφάλιζαν την αποτελεσματικότητα, την αξιοπιστία και τη φιλικότητα του συστήματος προς τον χρήστη.

3.1.1 Επιλογή εξοπλισμού συσκευών

Η επιλογή του κατάλληλου εξοπλισμού της συσκευής ήταν ένα κρίσιμο βήμα στα αρχικά στάδια της εργασίας. Συγκρίθηκαν διάφορες τεχνολογίες, συμπεριλαμβανομένων των συσκευών Arduino, Raspberry Pi και Android, προκειμένου να καθοριστεί η καταλληλότερη πλατφόρμα για το ψηφιακό σύστημα συναγερμού ασφαλείας. Κάθε μία από αυτές τις πλατφόρμες προσφέρει ξεχωριστά πλεονεκτήματα και δυνατότητες, οι οποίες αξιολογήθηκαν προσεκτικά.

Το Arduino είναι μια δημοφιλής ηλεκτρονική πλατφόρμα ανοικτού κώδικα που βασίζεται σε εύχρηστο hardware και λογισμικό. Χρησιμοποιείται ευρέως για την κατασκευή ψηφιακών συσκευών και διαδραστικών αντικειμένων που μπορούν να ανιχνεύσουν και να ελέγξουν τον φυσικό κόσμο. Οι πλακέτες Arduino μπορούν να ενσωματωθούν με διάφορους αισθητήρες, συμπεριλαμβανομένων των αισθητήρων PIR, οι οποίοι χρησιμοποιούνται συνήθως για την ανίχνευση κίνησης. Τα κύρια πλεονεκτήματα της χρήσης του Arduino περιλαμβάνουν το χαμηλό κόστος, την εκτεταμένη υποστήριξη της κοινότητας και την ευελιξία όσον αφορά την προσαρμογή και την ενσωμάτωση με διαφορετικούς τύπους αισθητήρων [62]. Ωστόσο, το Arduino έχει περιορισμούς στην επεξεργαστική ισχύ και τη μνήμη, οι οποίοι θα μπορούσαν να αποτελέσουν περιορισμό κατά την εφαρμογή σύνθετων αλγορίθμων AI για την επεξεργασία εικόνας και την αναγνώριση προσώπου σε πραγματικό χρόνο.

Το Raspberry Pi είναι μια άλλη ευέλικτη πλατφόρμα που προσφέρει μεγαλύτερη επεξεργαστική ισχύ σε σύγκριση με το Arduino. Είναι ένας μικρός, προσιτός υπολογιστής που μπορεί να χρησιμοποιηθεί για ένα ευρύ φάσμα εφαρμογών, συμπεριλαμβανομένων εκείνων που απαιτούν περισσότερες υπολογιστικές δυνατότητες. Το Raspberry Pi μπορεί επίσης να ενσωματωθεί με διάφορους αισθητήρες και περιφερειακά, καθιστώντας το κατάλληλο για την κατασκευή εξελιγμένων συστημάτων ασφαλείας. Υποστηρίζει κάμερες υψηλής ανάλυσης και μπορεί να τρέξει ολοκληρωμένα λειτουργικά συστήματα, επιτρέποντας πιο σύνθετες υλοποιήσεις λογισμικού [63]. Τα βασικά πλεονεκτήματα της χρήσης του Raspberry Pi περιλαμβάνουν την επεξεργαστική του ισχύ, την ευελιξία και την υποστήριξη γλωσσών προγραμματισμού υψηλού επιπέδου και λειτουργικών συστημάτων. Ωστόσο, το κόστος του είναι υψηλότερο από το Arduino και απαιτεί περισσότερη τεχνική εμπειρία για τη δημιουργία και τη συντήρησή του.

Λαμβάνοντας υπόψη την ανάγκη για λιγότερο κόστος, πρόσβαση και φιλική προς τον χρήστη, επιλέχθηκαν οι Android συσκευές για την υλοποίηση του ψηφιακού συστήματος συναγερμού ασφαλείας. Οι συσκευές Android διαθέτουν προηγμένο υλικό, όπως κάμερες υψηλής ποιότητας, ισχυρούς επεξεργαστές και διάφορες επιλογές συνδεσιμότητας. Αυτά τα χαρακτηριστικά καθιστούν τις συσκευές Android ιδανική πλατφόρμα για την ανάπτυξη μιας εφαρμογής ασφαλείας που μπορεί να είναι εύκολα προσβάσιμη και να χρησιμοποιείται από μια ευρεία βάση χρηστών. Το

λειτουργικό σύστημα Android παρέχει εκτεταμένη υποστήριξη για προγραμματιστές, ένα ευρύ φάσμα API και ισχυρά χαρακτηριστικά ασφαλείας, τα οποία είναι απαραίτητα για τη δημιουργία αξιόπιστων εφαρμογών ασφαλείας. Επιπλέον, η χρήση συσκευών Android καταργεί την ανάγκη για πρόσθετους αισθητήρες ή μεθόδους ελέγχου αυθεντικότητας, καθώς η εφαρμογή μπορεί να αξιοποιήσει την ενσωματωμένη κάμερα για παρακολούθηση σε πραγματικό χρόνο και αναγνώριση προσώπου. Η προσέγγιση αυτή εξασφαλίζει ευρύτερη προσβασιμότητα και ευκολία χρήσης για τους τελικούς χρήστες.

Σε αντίθεση με τις εξειδικευμένες πλατφόρμες Arduino και Raspberry Pi, οι συσκευές Android είναι ήδη προσβάσιμες από πολλούς χρήστες. Αυτό καθιστά δυνατή την ανάπτυξη της εφαρμογής ασφαλείας χωρίς να απαιτείται από τους χρήστες να επενδύσουν σε πρόσθετο υλικό. Επιπλέον, το εκτεταμένο οικοσύστημα εφαρμογών και υπηρεσιών του Android παρέχει ένα οικείο και φιλικό UI, μειώνοντας την εκμάθηση για τους νέους χρήστες.

3.1.2 Απαιτήσεις χρηστών

Για την ανάπτυξη ενός αποτελεσματικού ψηφιακού συστήματος συναγερμού ασφαλείας, η κατανόηση των αναγκών και των προσδοκιών των τελικών χρηστών είναι σημαντική. Η διαδικασία αυτή περιλαμβάνει τη διενέργεια ερευνών και την παρατήρηση των χρηστών για τη συλλογή λεπτομερών πληροφοριών σχετικά με τις προτιμήσεις και τις απαιτήσεις τους κατά τη χρήση μιας εφαρμογής ασφαλείας. Επιπλέον, πραγματοποιήθηκαν συνεντεύξεις για να αποκτηθούν βαθύτερες γνώσεις σχετικά με τους στόχους και τις απαιτήσεις. Τα ευρήματα από αυτές τις μεθόδους συνέβαλαν στη διαμόρφωση των βασικών χαρακτηριστικών και λειτουργιών που έπρεπε να συμπεριληφθούν στην εφαρμογή.

Οι χρήστες, σε γενικές γραμμές, θα είναι οι ιδιοκτήτες σπιτιών, οι ενοικιαστές και οι ιδιώτες που επιθυμούν να ενισχύσουν την ασφάλεια των χώρων κατοικίας τους. Οι χρήστες αυτοί πρέπει κυρίως θα ήθελα να ασφαλίσουν τα σπίτια τους, να έχουν ζωντανή πρόσβαση στα σπίτια τους μέσω της εφαρμογής και να είναι σε θέση να ανταποκρίνονται άμεσα σε τυχόν εντοπισμένες απειλές. Έχουν εκφράσει την ανάγκη

ώστε το σύστημα να έχει τη δυνατότητα να παίζει μια σειρήνα σε περίπτωση παραβίασης ιδιωτικού τους χώρο, ειδοποιώντας τους ενοίκους και ενδεχομένως αποτρέποντας τους εισβολείς. Οι χρήστες σημείωσαν επίσης τη πιθανή χρησιμότητα της παρακολούθησης των δραστηριοτήτων του συστήματος, όπως την καταγραφή ημερομηνίας και ώρας για ανίχνευση κινήσεων, ενεργοποίησης συναγερμού και άλλων δραστηριοτήτων. Το κόστος και η προσβασιμότητα επίσης αποτελούν σημαντικούς περιορισμούς, επομένως, οι χρήστες προτιμούν μια προσιτή λύση που δεν απαιτεί ακριβό ή δυσεύρετο εξοπλισμό και είναι εύκολη στην εγκατάσταση και τη χρήση χωρίς να απαιτούνται εκτεταμένες τεχνικές γνώσεις. Προτιμούν ένα σύστημα που επιτρέπει την εύκολη απενεργοποίηση του συστήματος μέσω μιας ασφαλούς μεθόδου ελέγχου ταυτότητας και να ενσωματώνεται απρόσκοπτα με τις καθημερινές τους συσκευές, όπως τα κινητά τηλέφωνα, εξασφαλίζοντας την άνετη παρακολούθηση του σπιτιού τους.

3.1.3 Παρόμοιες εφαρμογές

Μετά τον καθορισμό της πλατφόρμας υλοποίησης και των απαιτήσεων του χρήστη, πραγματοποιήθηκε ανάλυση της αγοράς για την εξέταση παρόμοιων εφαρμογών και τον εντοπισμό βέλτιστων πρακτικών, επιτυχημένων χαρακτηριστικών και πιθανών προβλημάτων που έπρεπε να αποφευχθούν κατά τη διαδικασία σχεδιασμού και ανάπτυξης. Η έρευνα αυτή παρείχε πολύτιμες πληροφορίες σχετικά με τα χαρακτηριστικά και τις λειτουργίες που θα ήταν πιο ωφέλιμες για τους στοχευόμενους χρήστες.

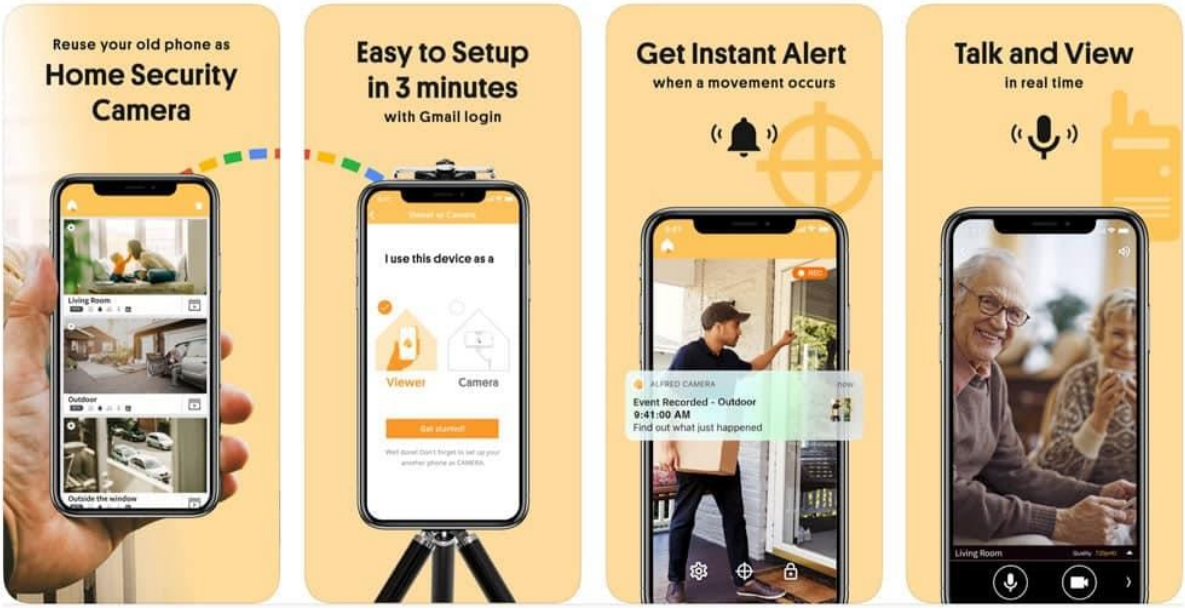
3.1.3.1 Alfred Camera

Η Alfred Camera είναι μια εφαρμογή οικιακής ασφάλειας που μετατρέπει παλιά κινητά τηλέφωνα, ταμπλέτες ή υπολογιστές σε λειτουργικές κάμερες ασφαλείας. Αυτή η εφαρμογή παρέχει μια οικονομικά αποδοτική και φιλικό UI για την ασφάλεια στο σπίτι, καθιστώντας την προσβάσιμη για άτομα που μπορεί να μην θέλουν να επενδύσουν σε ακριβά συστήματα παρακολούθησης. Η διαδικασία εγκατάστασης είναι εύκολη, οι χρήστες κατεβάζουν την εφαρμογή Alfred Camera στις παλιές και τις νέες συσκευές

τους, συνδέονται με τον ίδιο λογαριασμό και στις δύο και ορίζουν τη μία συσκευή ως κάμερα και την άλλη ως συσκευή προβολής . Η εφαρμογή προσφέρει ροή βίντεο σε πραγματικό χρόνο, η οποία επιτρέπει στους χρήστες να παρακολουθούν τα σπίτια τους εξ αποστάσεως από οπουδήποτε [64].

Κάποιες δυνατότητες που προσφέρει η εφαρμογή:

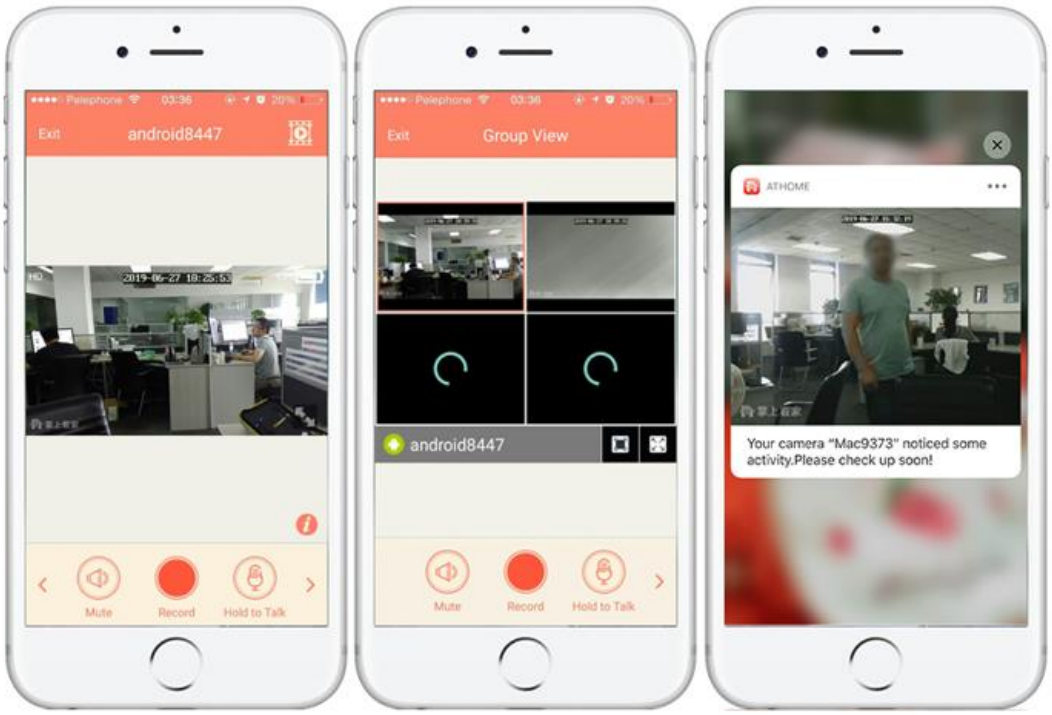
- *Εύκολη εγκατάσταση:* Η εφαρμογή είναι απλή στη ρύθμιση. Οι χρήστες μπορούν να κατεβάσουν την Alfred Camera στις παλιές και τις νέες συσκευές τους, να συνδεθούν με τον ίδιο λογαριασμό και στη συνέχεια να ορίσουν τη μία συσκευή ως κάμερα και την άλλη ως συσκευή προβολής.
- *Ζωντανή μετάδοση:* Η Alfred Camera παρέχει ζωντανή ροή βίντεο, επιτρέποντας στους χρήστες να παρακολουθούν τα σπίτια τους σε πραγματικό χρόνο από οπουδήποτε χρησιμοποιώντας τις κινητές συσκευές τους.
- *Ανίχνευση κίνησης:* Η εφαρμογή περιλαμβάνει μια λειτουργία ανίχνευσης κίνησης που στέλνει ειδοποιήσεις στο χρήστη όταν ανιχνεύεται κίνηση.
- *Νυχτερινή όραση:* Η εφαρμογή περιλαμβάνει δυνατότητες νυχτερινής όρασης, για να καταγράφει καθαρό βίντεο ακόμη και σε συνθήκες χαμηλού φωτισμού.
- *Ρύθμιση πολλαπλών καμερών:* Οι χρήστες μπορούν να ρυθμίσουν πολλαπλές συσκευές καμερών κάτω από τον ίδιο λογαριασμό για μια ολοκληρωμένη κάλυψη διαφορετικών περιοχών μέσα στα σπίτια τους.



Εικόνα 13 - Alfred Camera [65]

3.1.3.2 AtHome Camera

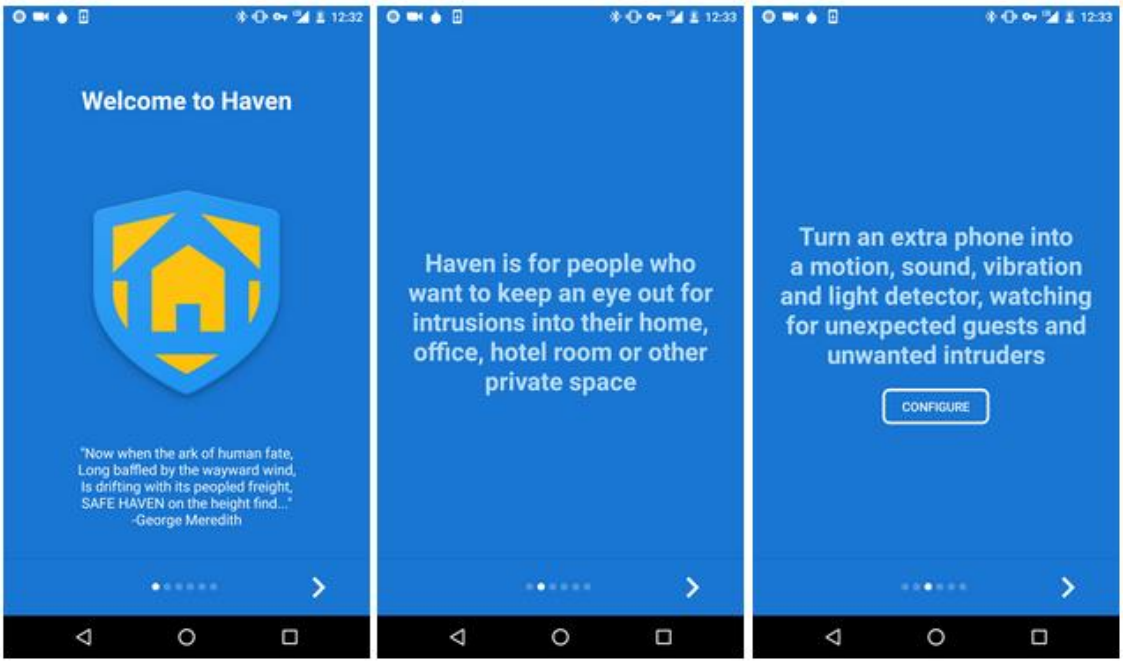
Η AtHome Camera είναι μια άλλη εφαρμογή οικιακής ασφάλειας και προστασίας που επιτρέπει στους χρήστες να μετατρέψουν το κινητό τους τηλέφωνο ή άλλες συσκευές σε κάμερα. Αυτή η εφαρμογή όπως και την Alfred Camera, μπορεί να είναι χρήσιμη επειδή βοηθά τους χρήστες να μετατρέψουν αποτελεσματικά τις συσκευές τους σε αρκετά αποδοτικά μέσα παρακολούθησης. Η εφαρμογή επιτρέπει στους χρήστες να εγκαταστήσουν ένα δίκτυο καμερών και να έχουν πρόσβαση σε όλες ταυτόχρονα, γεγονός που είναι χρήσιμο για την παρακολούθηση του χώρου κατοικίας τους. Επίσης, η εφαρμογή έρχεται με τη λειτουργία αμφίδρομου ήχου και έτσι οι χρήστες είναι σε θέση να μιλήσουν με τα άτομα που βρίσκονται κοντά στην κάμερα. Προς το παρόν, η εφαρμογή AtHome Camera διαθέτει τόσο μια δωρεάν όσο και μια premium έκδοση, με την premium είναι σε θέση να παρέχει στον χρήστη τη δυνατότητα αποθήκευσης στο cloud για τα καταγεγραμμένα βίντεο, καθώς και πιο ακριβείς ρυθμίσεις όσον αφορά την ανίχνευση κίνησης [66]. Στην ουσία, η AtHome Camera είναι μια εύχρηστη και πρακτική προσέγγιση για την προστασία του σπιτιού, καθώς επιτρέπει στα άτομα να επιβλέπουν το σπίτι τους ανεξάρτητα από την τοποθεσία στην οποία βρίσκονται, δεδομένου ότι διαθέτουν σύνδεση στο διαδίκτυο.



Εικόνα 14 - AtHome Camera [66]

3.1.3.3 Haven: Keep Watch

Η Haven είναι μια εφαρμογή που εστιάζει στην προστασία της ιδιωτικής ζωής. Χρησιμοποιεί τους κύριους αισθητήρες μιας κινητής συσκευής για την παρακολούθηση των φυσικών χώρων των χρηστών. Ξεχωρίζει για τον χαρακτήρα του ανοιχτού κώδικα, επιτρέποντας την προσαρμογή και τη βελτίωση από προγραμματιστές Android. Ο πηγαίος κώδικάς του είναι ελεύθερα προσβάσιμος και δίνει τη δυνατότητα στους χρήστες και τους προγραμματιστές να συνεργάζονται για τη συνεχή βελτίωση των χαρακτηριστικών ασφαλείας. Η εφαρμογή προσφέρει δυνατότητες ειδοποίησης στους χρήστες για τυχόν συμβάντα ανίχνευσης ή ασφάλειας μέσω SMS ή Signal[3]. Αυτές οι ειδοποιήσεις περιλαμβάνουν λεπτομέρειες του συμβάντος και χρονοδιαγράμματα, επιτρέποντας την άμεση ανάληψη δράσης σε πιθανές απειλές. Η διαισθητική διεπαφή της Haven επιτρέπει στους χρήστες να ρυθμίζουν τους αισθητήρες και να παρακολουθούν εύκολα το περιβάλλον τους. Οι χρήστες μπορούν να ρυθμίσουν τα επίπεδα ευαισθησίας και να ορίσουν έναν κωδικό ασφαλείας για να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση, εξασφαλίζοντας την ασφάλεια των ρυθμίσεων επιτήρησης [67].



Εικόνα 15 - Haven: Keep Watch [67]

[3] Η Signal είναι μια εφαρμογή για ιδιωτικές συνομιλίες όπου κάθε μήνυμα είναι κρυπτογραφημένο.

3.1.4 Περιβάλλον Υλοποίησης

Για την υλοποίηση της εφαρμογής ψηφιακού συναγερμού ασφαλείας χρησιμοποιήθηκε το εργαλείο Android Studio, το οποίο είναι ένα ολοκληρωμένο περιβάλλον ανάπτυξης (IDE) που δημιουργήθηκε από την Google και προσφέρει εξαιρετικές δυνατότητες και εργαλεία για την ανάπτυξη εφαρμογών για περιβάλλοντα Android. Δεδομένου ότι υποστηρίζει τη γλώσσα σήμανσης γνωστή ως XML, κατέστη εύκολη η ανάπτυξη ενός καθαρού και ευέλικτου περιβάλλοντος εργασίας της εφαρμογής. Επίσης, είναι χρήσιμη η αναφορά ότι τα εργαλεία αυτά ήταν χρήσιμα για να γίνει μια αποδοτική διαδικασία ανάπτυξης.

Το Android Studio διαθέτει ένα αποτελεσματικό περιβάλλον κωδικοποίησης και έναν σχεδιαστή για την σχεδίαση του UI. Ορισμένα από αυτά τα χαρακτηριστικά του περιβάλλον περιλαμβάνουν έλεγχο των σφαλμάτων σε πραγματικό χρόνο, βοηθήματα στον κώδικα με την βοήθεια της AI, και πρακτικά εφαρμοζόμενα χαρακτηριστικά όπως η αναδιαμόρφωση. Επίσης, μία από τις πιο πολύτιμες επιλογές που παρέχει το Android Studio είναι η στενή ενσωμάτωση με το Android Software Development Kit (SDK), το οποίο επιτρέπει στους προγραμματιστές να χρησιμοποιούν νέα API, καθώς και άλλα εργαλεία, τα οποία είναι απαραίτητα για τη δημιουργία των σημερινών εφαρμογών Android [68]. Ο ενσωματωμένος εξομοιωτής είναι ιδιαίτερα χρήσιμος, καθώς μπορεί να προσομοιώσει εφαρμογές σε διάφορες συσκευές και συνθήκες χωρίς να χρειάζεται να κατέχουν φυσικές συσκευές. Επιβεβαιώνει την ανταπόκριση της εφαρμογής σε διαφορετικές οθόνες, αναλύσεις και εκδόσεις του Android, καθιστώντας τη λήψη ενός ευρέος τεστ που βοηθά στον εντοπισμό σφαλμάτων ειδικά στα αρχικά στάδια του κύκλου ανάπτυξης.

Εικόνα 16 - Λογότυπο του Android Studio [69]

3.1.4.1 Γλώσσα προγραμματισμού της υλοποίησης

Κατά τη διάρκεια της επιλογής της γλώσσας προγραμματισμού για την υλοποίηση της εφαρμογής ψηφιακού συναγερμού ασφαλείας, εξετάστηκαν τόσο η Java όσο και η Kotlin. Η Java, με τη μακρόχρονη παρουσία της στο οικοσύστημα ανάπτυξης Android, προσφέρει σταθερότητα, ωριμότητα και εκτεταμένη υποστήριξη βιβλιοθηκών. Ωστόσο, και η Kotlin παρουσιάζει αρκετά πλεονεκτήματα έναντι της Java, όπως την πιο συνοπτική και εκφραστική σύνταξη, και ενσωματωμένη ασφάλεια για null τιμές. Επιπλέον, η Kotlin είναι πλήρως συμβατή με τη Java, επιτρέποντας την ομαλή ενσωμάτωση των υφιστάμενων βιβλιοθηκών και πλαισίων της Java [70].

Όσον αφορά την υλοποίηση της εφαρμογής ψηφιακού συναγερμού ασφαλείας, η Kotlin επιλέχθηκε κυρίως λόγω των σύγχρονων χαρακτηριστικών και των αναβαθμίσεών της από τη γλώσσα Java. Η γλώσσα βελτιώνει την παραγωγικότητα του κώδικα, απλοποιώντας την πολυπλοκότητα και την αναγνωσιμότητα του κώδικα. Ένα άλλο πλεονέκτημα της Kotlin όπως επισημάνθηκε, είναι η ασφάλεια για τις null τιμές, οποία μειώνει την πιθανότητα να προκύψουν σφάλματα κατά την εκτέλεση με βάση τις null αναφορές καθιστώντας έτσι τις εφαρμογές πιο ασφαλείς. Συμπερασματικά, τα καλύτερα χαρακτηριστικά που προσφέρει η Kotlin με την ικανότητά της να συνεργάζεται συνεκτικά με τη Java, χρησιμοποιήθηκε ως κατάλληλη γλώσσα για την ανάπτυξη της εφαρμογής ψηφιακού συναγερμού ασφαλείας.

4. Λογική Αρχιτεκτονική & Ανάπτυξη Εφαρμογής

Η λογική αρχιτεκτονική και η ανάπτυξη της εφαρμογής του ψηφιακού συστήματος συναγερμού ασφαλείας περιλαμβάνει τη σχεδίαση, τη δόμηση και την ενσωμάτωση διαφόρων τεχνολογιών και βιβλιοθηκών για τη δημιουργία μιας συνεκτικής και λειτουργικής εφαρμογής. Η φάση αυτή επικεντρώνεται στον τρόπο με τον οποίο τα διάφορα συστήματα αλληλεπιδρούν εντός του συστήματος για την επίτευξη των επιθυμητών λειτουργιών, όπως η παρακολούθηση σε πραγματικό χρόνο, η επαλήθευση του χρήστη μέσω προσώπου, οι ειδοποιήσεις συναγερμού, και η ενημέρωση του χρήστη. Η διαδικασία ανάπτυξης περιλαμβάνει την επιλογή και την εφαρμογή των κατάλληλων τεχνολογιών για να διασφαλιστεί ότι η εφαρμογή είναι αποτελεσματική, αξιόπιστη και φιλική προς τον χρήστη. Έμφαση δίνεται στη χρήση σύγχρονων βιβλιοθηκών και πλαισίων που διευκολύνουν τη δημιουργία μιας ισχυρής λύσης ασφάλειας ικανής να τρέξει σε συσκευές Android.

4.1 Σχεδιαστική Ιδέα και Οπτική Αναπαράσταση της Εφαρμογής

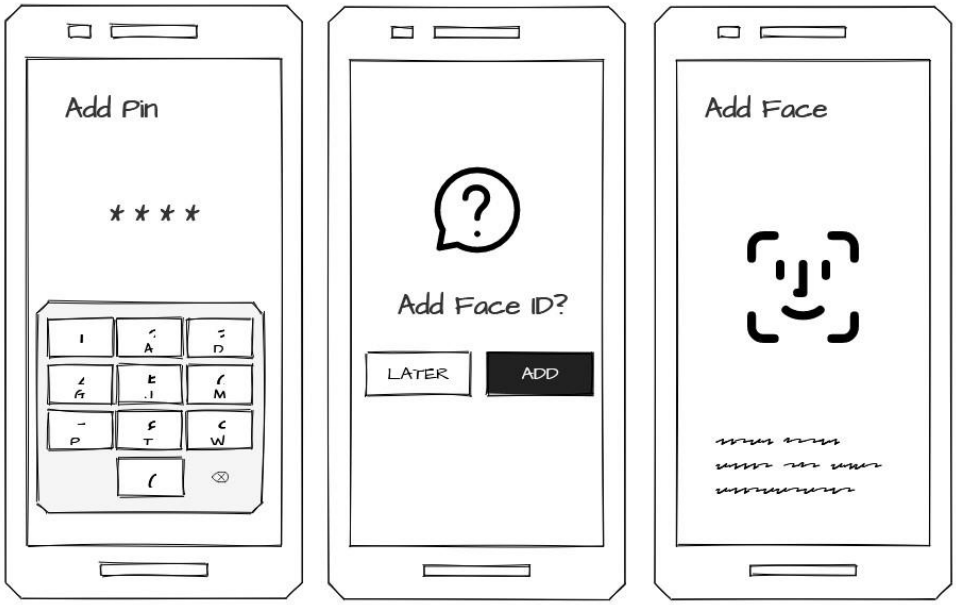
Σε αυτό το υποκεφάλαιο, περιγράφεται η σχεδιαστική ιδέα για την κινητή εφαρμογή του ψηφιακού συναγερμού ασφαλείας, η οποία θα ονομάζεται *Flame Guard*, και παρέχονται οπτικές αναπαραστάσεις μέσω πρόχειρων σχεδίων και του λογότυπου της εφαρμογής. Η σχεδιαστική ιδέα εστιάζει στην ενίσχυση της εμπειρίας του χρήστη, στην εξασφάλιση διαισθητικής πλοήγησης και στη διατήρηση μιας συνεκτικής οπτικής αναγνώρισης σε όλη την εφαρμογή.

Τα πρόχειρα σχέδια, επίσης γνωστά ως wireframes ή mockups, είναι απλοποιημένες οπτικές αναπαραστάσεις ενός UI ή ενός σχεδιασμού προϊόντος. Δημιουργούνται συνήθως κατά τα αρχικά στάδια της διαδικασίας σχεδιασμού, πριν από την έναρξη της λεπτομερούς υλοποίησης. Τα πρόχειρα σχέδια επικεντρώνονται στη μεταφορά της βασικής διάταξης, δομής και λειτουργικότητας μιας εφαρμογής χωρίς να αποτυπωθούν λεπτομέρειες όπως τα χρώματα, οι γραμματοσειρές ή τα περίπλοκα στοιχεία σχεδιασμού [71].

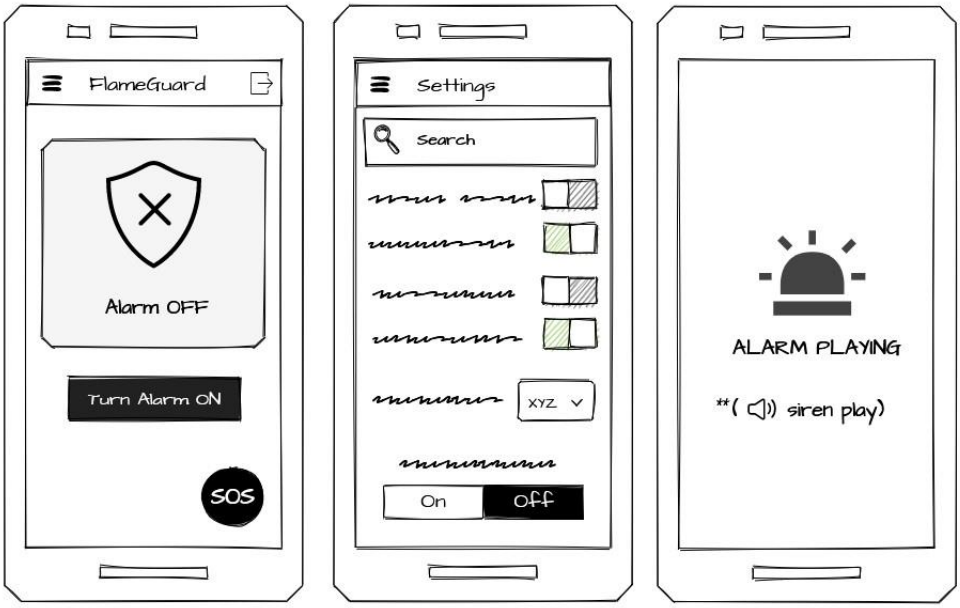
Παρακάτω παρουσιάζονται κάποια πρόχειρα σχέδια που απεικονίζουν το προτεινόμενο UI για την εφαρμογή Flame Guard. Τα σχέδια αυτά χρησιμεύουν ως προκαταρκτική απεικόνιση των βασικών οθονών και χαρακτηριστικών της εφαρμογής. Οι ολοκληρωμένες εκδόσεις αυτών των σχεδίων θα παρασχεθούν αναλυτικά στα επόμενα κεφάλαια, προσφέροντας μια ολοκληρωμένη επισκόπηση του UI της εφαρμογής.

Πρόχειρα Σχέδια

Εικόνα 17 - Πρόχειρα Σχέδια για Σύνδεση/Εγγραφή/Καλωσόρισμα



Εικόνα 18 - Πρόχειρα Σχέδια για Διάφορες Προτεινόμενες Οθόνες



Εικόνα 19 - Πρόχειρα Σχέδια για Αρχική/Ρυθμίσεις/Συναγερμός

Λογότυπο της εφαρμογής (Flame Guard)

Εικόνα 20 - Λογότυπο της Εφαρμογής (Flame Guard)

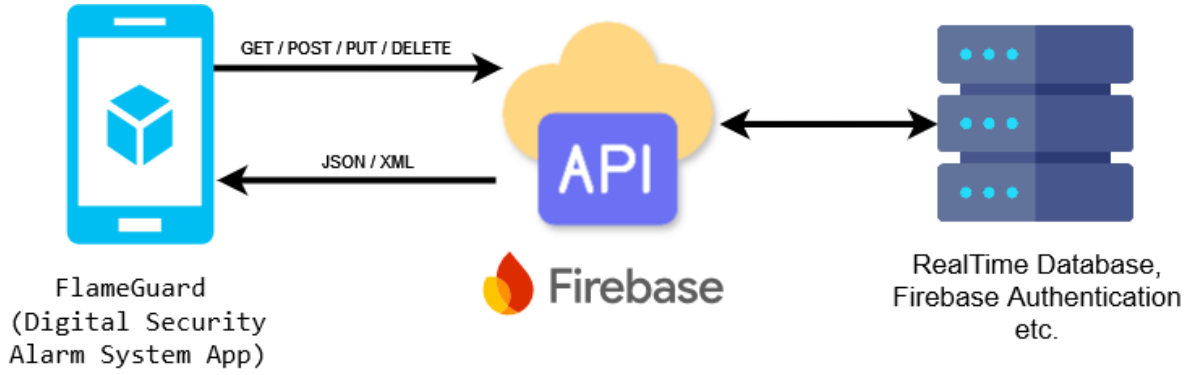
Το λογότυπο της εφαρμογής Flame Guard αποτελεί την ουσία της *ασφάλειας*, της *προστασίας* και της *αξιοπιστίας*. Διαθέτει ένα διακριτικό σύμβολο που μεταφέρει την προσωπικότητα της εφαρμογής μαζί με το όνομα της.

4.2 Τεχνολογίες & Βιβλιοθήκες

Σε αυτό το υποκεφάλαιο περιγράφονται οι βασικές τεχνολογίες και βιβλιοθήκες που χρησιμοποιήθηκαν για την ανάπτυξη του ψηφιακού συστήματος συναγερμού ασφαλείας. Κάθε τεχνολογία επιτελεί κρίσιμο ρόλο στη διασφάλιση ότι το σύστημα πληροί τις απαιτήσεις απόδοσης, ασφάλειας και χρησιμότητας.

4.2.1 Google Firebase

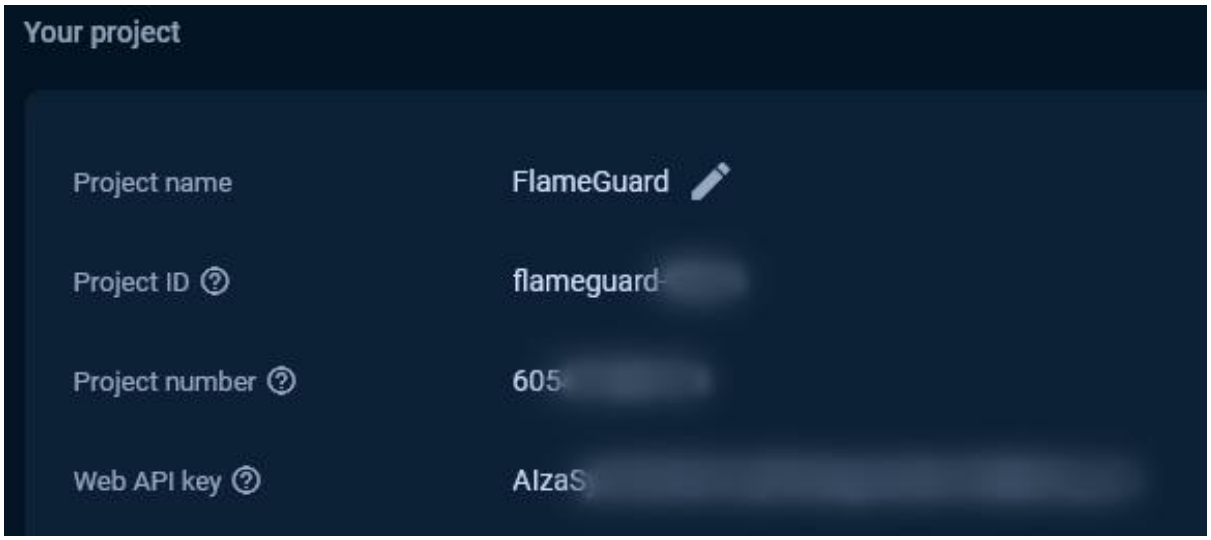
Η Firebase είναι μια ολοκληρωμένη συλλογή εργαλείων, βασισμένα στο νέφος που παρέχει η Google. Υποστηρίζει την ανάπτυξη και την εγκατάσταση διάφορων εφαρμογών για κινητές και διαδικτυακές εφαρμογές. Το ψηφιακό σύστημα συναγερμού ασφαλείας αξιοποιεί διάφορα στοιχεία της Firebase, καθένα από τα οποία παρέχει μοναδικά χαρακτηριστικά που βοηθούν στη συνολική λειτουργικότητα [72].



Εικόνα 21 - Διάγραμμα Δικτύου Μεταξύ Εφαρμογής και Firebase

Η επικοινωνία με την Firebase πραγματοποιείται μέσω ενός API, το οποίο απαιτεί έναν λογαριασμό στην πλατφόρμα Firebase. Μετά τη δημιουργία ενός λογαριασμού και τη διαμόρφωση των ρυθμίσεων της εργασίας στο Firebase, η εφαρμογή Flame Guard συνδέεται με το Firebase μέσω της χρήσης των SDK της Firebase. Αυτά τα SDKs παρέχουν διάφορες λειτουργίες, όπως πιστοποίηση ταυτότητας χρήστη, πρόσβαση

σε βάσεις δεδομένων (DBs) σε πραγματικό χρόνο, μηνύματα στο νέφος και υπηρεσίες αποθήκευσης.



Εικόνα 22 - Στοιχεία της Εφαρμογής Flame Guard για το Firebase API

Για την ενσωμάτωση των SDKs της Firebase στην υλοποίηση της εφαρμογής Flame Guard, είναι απαραίτητο να διαμορφωθεί η εργασία με τα κατάλληλα κλειδιά Web API και τη διεύθυνση του server της εργασίας. Αυτή η ρύθμιση δημιουργεί την αρχική επικοινωνία μεταξύ της εφαρμογής και των υπηρεσιών Firebase. Η διαμόρφωση γίνεται συνήθως με την προσθήκη των στοιχείων από το αρχείο *google-services.json* στην υλοποίηση, τα οποία στοιχεία δημιουργούνται από την Firebase.

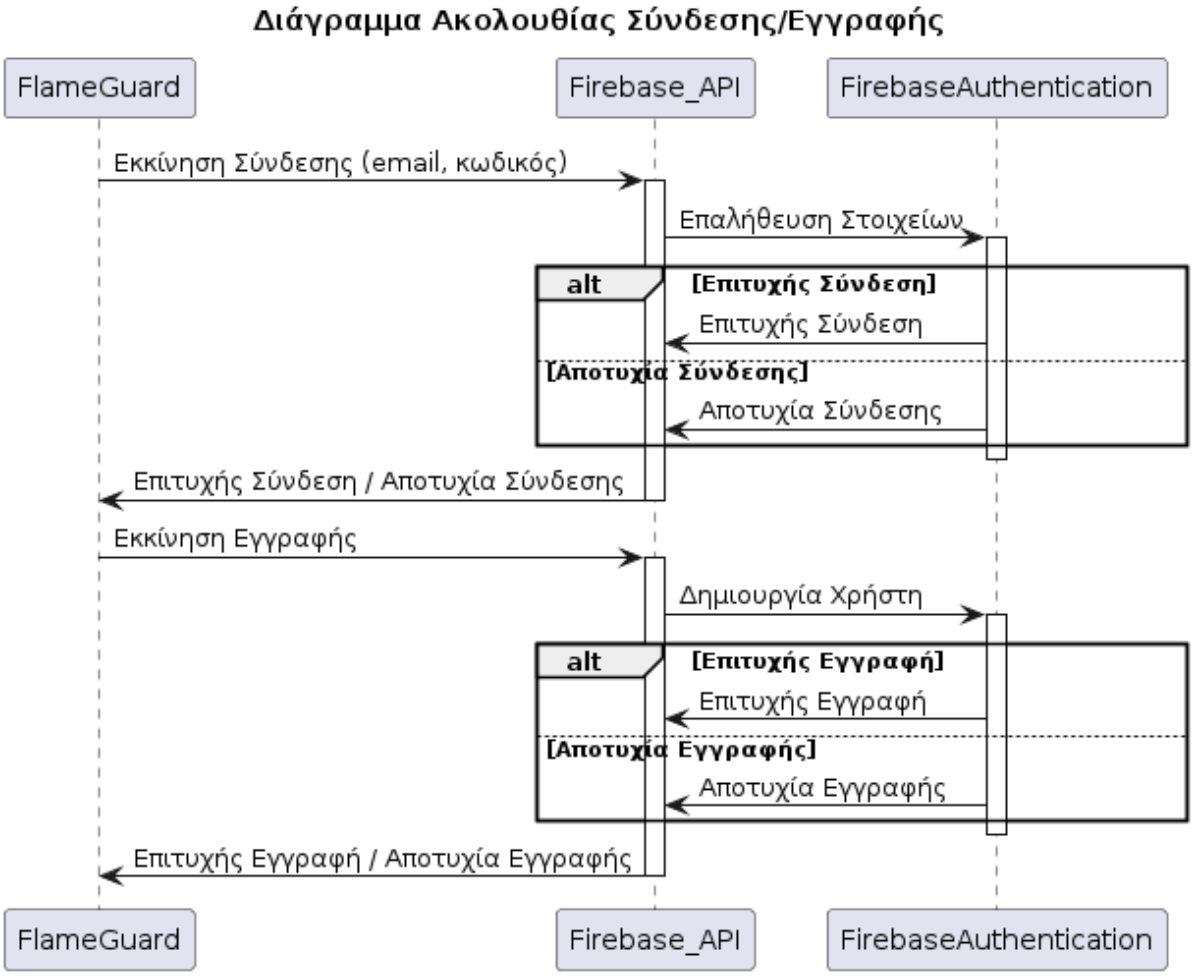
```
if (FirebaseApp.getApps( context: this).isEmpty()) {
    val options = FirebaseOptions.Builder()
        .setApplicationId("1:60**************************************")
        .setApiKey("AIza**************************************")
        .setDatabaseUrl("https://flameguard-*********************************************")
        .build()

    FirebaseApp.initializeApp( context: this, options)
}
```

Εικόνα 23 - Απόκομμα Κώδικα για την Διασύνδεση της Εφαρμογής Flame Guard με τις Υπηρεσίες Firebase

Με τη σωστή ρύθμιση των στοιχείων, η εφαρμογή Flame Guard διασφαλίζει την απρόσκοπτη ενσωμάτωση με τη Firebase, επιτρέποντάς της να χρησιμοποιεί αποτελεσματικά τις υπηρεσίες Firebase.

Firebase Αυθεντικοποίηση (Firebase Authentication)

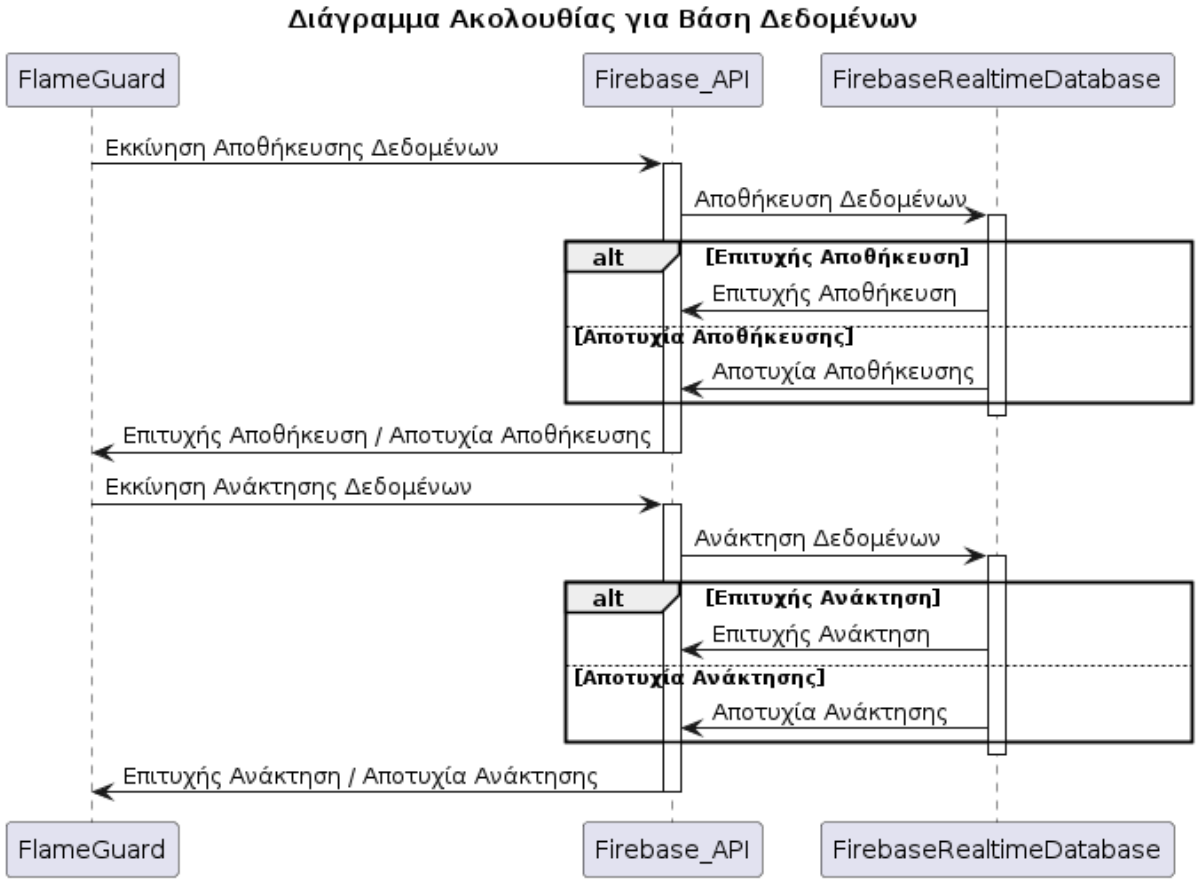
Μέσω APIs διαχειρίζεται με ασφάλεια οι διαδικασίες ελέγχου σύνδεσης των χρηστών, υποστηρίζοντας διάφορες μεθόδους, όπως email με έναν κωδικό πρόσβασης ή έναν λογαριασμό Google ή και Facebook. Αυτή η δυνατότητα απλοποιεί την υλοποίηση ασφαλούς ελέγχου ταυτότητας χρηστών παρέχοντας ένα εύχρηστο SDK που χειρίζεται εργασίες όπως η σύνδεση και εγγραφή χρήστη. Εξασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση και να ελέγχουν το σύστημα ψηφιακού συναγερμού ασφαλείας. Στην εργασία υλοποιήθηκε μόνο η δυνατότητα της σύνδεσης και εγγραφής με χρήση έναν email και έναν κωδικό πρόσβασης.



Εικόνα 24 - Διάγραμμα Ακολουθίας Σύνδεσης/Εγγραφής

Βάση Δεδομένων της Firebase (Firebase Database)

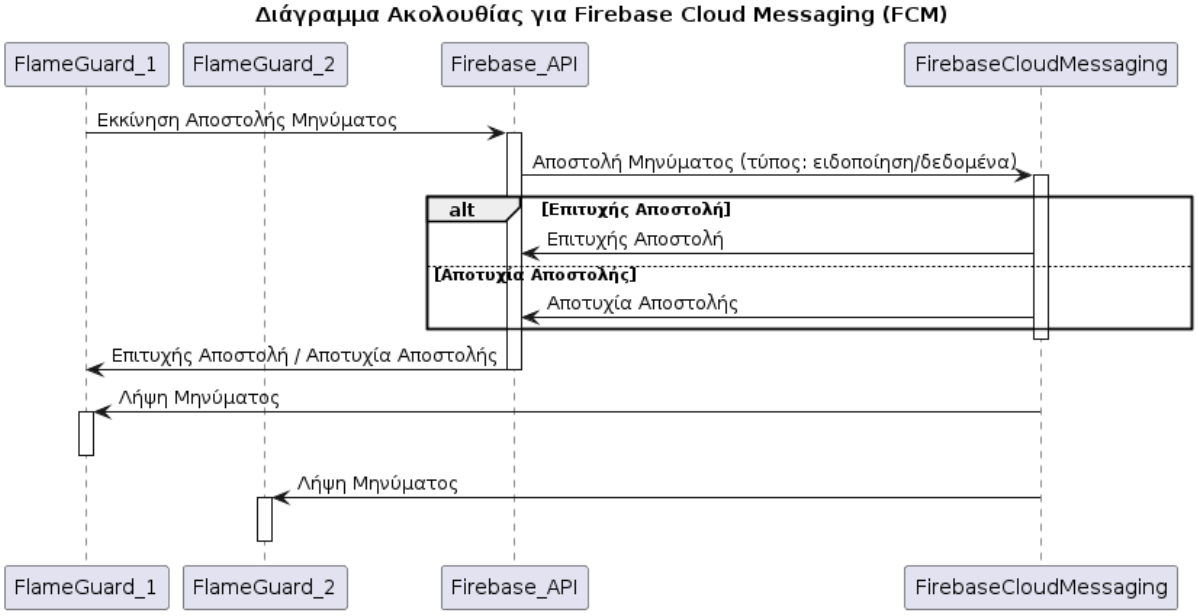
Η Firebase Database είναι μια βάση δεδομένων που φιλοξενείται στο νέφος και επιτρέπει το συγχρονισμό δεδομένων σε πραγματικό χρόνο σε όλους τους συνδεδεμένους πελάτες. Αυτό είναι σημαντικό για το ψηφιακό σύστημα συναγερμού ασφαλείας, το οποίο απαιτεί άμεσες ενημερώσεις για τον εντοπισμό και την αντιμετώπιση περιστατικών ασφαλείας. Η βάση δεδομένων επιτρέπει την αποθήκευση δομημένων δεδομένων σε μορφή JSON, επιτρέποντας την αποτελεσματική ανάκτηση και συγχρονισμό δεδομένων. Οι βασικές περιπτώσεις χρήσης περιλαμβάνουν την αποθήκευση ρυθμίσεων χρηστών, αρχείων καταγραφής συστήματος και ενημερώσεων κατάστασης, διασφαλίζοντας ότι όλοι οι χρήστες και οι συσκευές έχουν τις πιο ενημερωμένες διαθέσιμες πληροφορίες.



Εικόνα 25 - Διάγραμμα Ακολουθίας Αποθήκευσης/Ανάκτησης Δεδομένων

Μηνύματα Μέσω Firebase (Firebase Cloud Messaging - FCM)

Το Firebase Cloud Messaging χρησιμοποιείται για την αποστολή ειδοποιήσεων στους χρήστες μέσω της εφαρμογής Flame Guard σε άλλη κινητή συσκευή, διασφαλίζοντας ότι ειδοποιούνται άμεσα για συμβάντα ασφαλείας, όπως μη εξουσιοδοτημένη πρόσβαση στο περιβάλλον τους. Αυτό το στοιχείο εξασφαλίζει την αξιόπιστη και έγκαιρη παράδοση κρίσιμων ειδοποιήσεων, επιτρέποντας στους χρήστες να αναλάβουν άμεση δράση για την ασφάλεια των χώρων τους.



Εικόνα 26 - Διάγραμμα Ακολουθίας για Firebase Cloud Messaging (FCM)

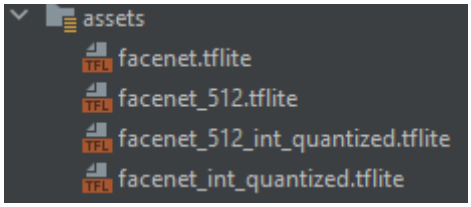
Αυτές οι υπηρεσίες της Firebase επιτρέπουν συνολικά την ισχυρή πιστοποίηση των χρηστών, τις ενημερώσεις δεδομένων σε πραγματικό χρόνο, την αποτελεσματική παράδοση μηνυμάτων και την ασφαλή αποθήκευση πολυμέσων, οι οποίες είναι σημαντικές για την αποτελεσματικότητα και την αξιοπιστία του ψηφιακού συστήματος συναγερμού ασφαλείας.

4.2.2 Αναγνώριση Προσώπου με TensorFlow Lite

Η TensorFlow Lite είναι ένα ευέλικτο, διαπλατφορμικό (cross-platform) πλαίσιο για την ανάπτυξη μοντέλων μηχανικής μάθησης σε φορητές και ενσωματωμένες συσκευές. Είναι σχεδιασμένο για να είναι αποδοτικό, με ελάχιστη καθυστέρηση και χαμηλή κατανάλωση ενέργειας, καθιστώντας το ιδανικό για κινητές εφαρμογές. Η TensorFlow Lite υποστηρίζει μια σειρά από μοντέλα μηχανικής μάθησης, όπως ταξινόμηση εικόνων, ανίχνευση αντικειμένων και αναγνώριση προσώπων [73].

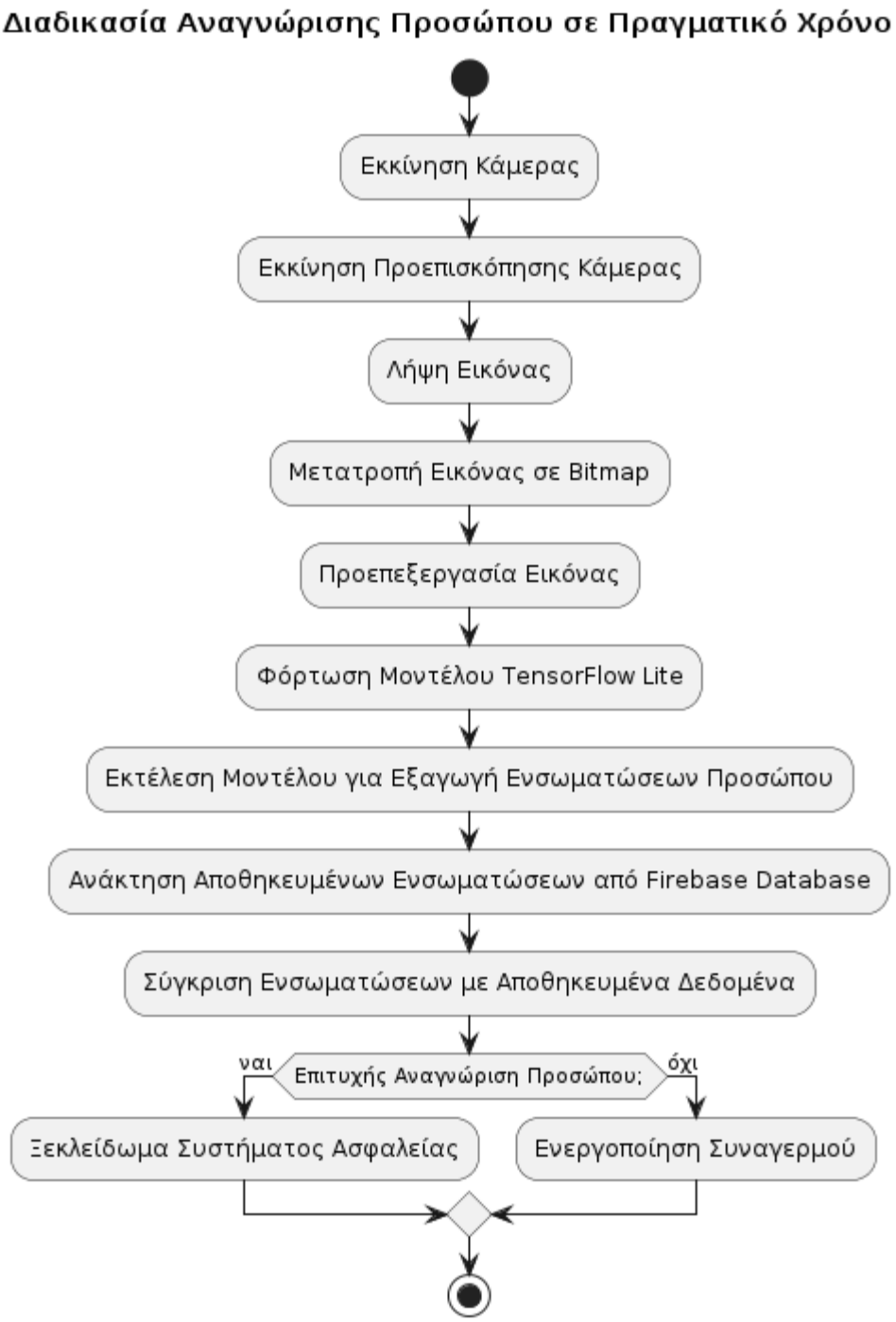
4.2.2.1 TensorFlow Lite στην Αναγνώριση Προσώπου

Τα μοντέλα της TensorFlow Lite μετατρέπονται πρώτα σε μια ευέλικτη μορφή *(.tflite)* κατάλληλη για κινητές και ενσωματωμένες συσκευές. Αυτά τα μοντέλα εκτελούνται στη συνέχεια σε κινητές συσκευές χρησιμοποιώντας τον μεταγλωττιστή της TensorFlow Lite, ο οποίος βελτιστοποιεί τη διαδικασία εξαγωγής συμπερασμάτων για να εξασφαλίσει αποδοτικές επιδόσεις. Επιπλέον, η TensorFlow Lite υποστηρίζει επιτάχυνση GPU, η οποία βελτιώνει περαιτέρω την απόδοση της εξαγωγής συμπερασμάτων των μοντέλων αξιοποιώντας την GPU της συσκευής.



Εικόνα 27 - Μοντέλα TensorFlow Lite στην Υλοποίηση

Στη Flame Guard, η TensorFlow Lite χρησιμοποιείται για την αναγνώριση προσώπου σε πραγματικό χρόνο μέσω ενός προεκπαιδευμένου μοντέλου FaceNet. Το μοντέλο φορτώνεται χρησιμοποιώντας τον διερμηνέα της TensorFlow Lite και οι εικόνες εισόδου υποβάλλονται σε προεπεξεργασία ώστε να πληρούν τις απαιτήσεις του μοντέλου. Στη συνέχεια, το μοντέλο εκτελεί συμπερασμό σε αυτές τις επεξεργασμένες εικόνες για να εξάγει ενσωματώσεις προσώπου. Τέλος, αυτές οι ενσωματώσεις συγκρίνονται με αποθηκευμένες ενσωματώσεις για την επαλήθευση ή την αναγνώριση προσώπων. Αυτή η ακολουθία εξασφαλίζει αποτελεσματική και ακριβή αναγνώριση προσώπων στο πλαίσιο της εφαρμογής Flame Guard.



Εικόνα 28 - Διάγραμμα Ροής για την Διαδικασία Αναγνώρισης Προσώπου σε Πραγματικό Χρόνο με TF Lite

4.2.3 Ανίχνευση Προσώπου με ML Kit

Το ML Kit Face Detection, ένα από τα στοιχεία της πλατφόρμας Firebase της Google, είναι ένα ευέλικτο και ισχυρό εργαλείο που έχει σχεδιαστεί για τον εντοπισμό και την ανάλυση ανθρώπινων προσώπων τόσο σε εικόνες όσο και σε βίντεο. Αξιοποιεί προηγμένα μοντέλα μηχανικής μάθησης για τον εντοπισμό και την παροχή λεπτομερών πληροφοριών σχετικά με τα πρόσωπα που υπάρχουν σε οπτικά δεδομένα [74]. Αυτή η λειτουργικότητα είναι κρίσιμη για εφαρμογές που κυμαίνονται από συστήματα ασφαλείας έως φίλτρα κοινωνικών μέσων.

4.2.3.1 Βασικά χαρακτηριστικά της ML Kit

Ανίχνευση προσώπου: Η κύρια λειτουργία είναι η ανίχνευση προσώπου σε ένα καρέ εικόνας, προσδιορίζοντας τη θέση, το μέγεθος και τον προσανατολισμό τους. Αυτή η ανίχνευση είναι εξαιρετικά ακριβής, ακόμη και σε διάφορες συνθήκες φωτισμού και πολύπλοκα φόντα.

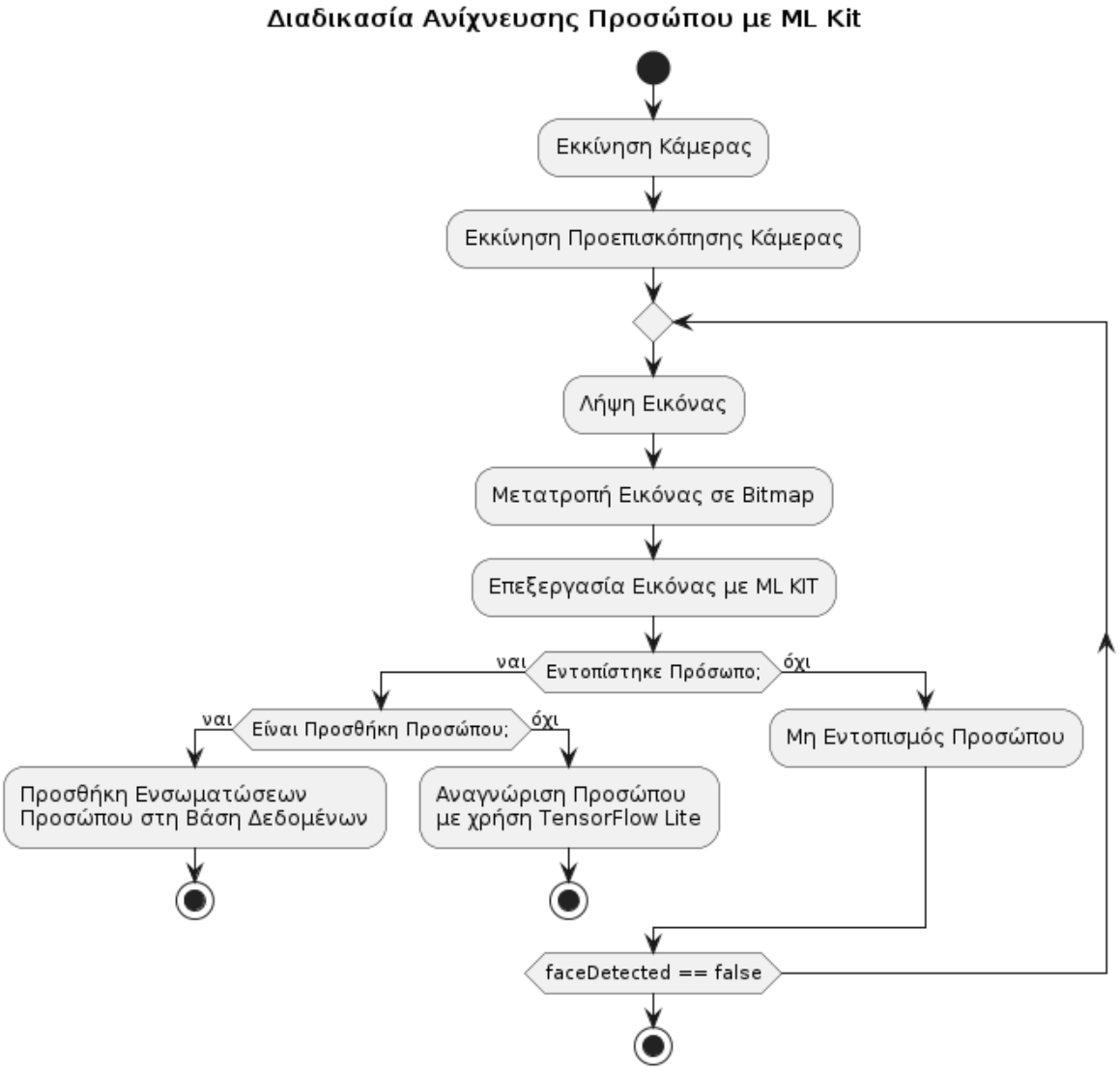
Εξαγωγή χαρακτηριστικών: Πέρα από την απλή ανίχνευση, το ML Kit μπορεί να εξάγει λεπτομερή χαρακτηριστικά του προσώπου, όπως τα μάτια, η μύτη, το στόμα και το συνολικό σχήμα του προσώπου. Μπορεί επίσης να εντοπίσει σημεία αναφοράς του προσώπου, παρέχοντας ακριβείς συντεταγμένες για αυτά τα χαρακτηριστικά.

Επεξεργασία σε πραγματικό χρόνο: Το ML Kit υποστηρίζει ανίχνευση προσώπου σε πραγματικό χρόνο, καθιστώντας το κατάλληλο για εφαρμογές που απαιτούν άμεση ανατροφοδότηση, όπως την Flame Guard.

Επεκτασιμότητα: Σχεδιασμένο για να λειτουργεί αποτελεσματικά σε κινητές συσκευές, το ML Kit διασφαλίζει ότι οι διαδικασίες ανίχνευσης προσώπου βελτιστοποιούνται για απόδοση, χρησιμοποιώντας ελάχιστους υπολογιστικούς πόρους, διατηρώντας παράλληλα υψηλή ακρίβεια.

Στην υλοποίηση της εφαρμογής Flame Guard, το ML Kit Face Detection χρησιμοποιείται για την καταγραφή των προσώπων κατά τη διαδικασία ελέγχου αυθεντικότητας ή κατά την αποθήκευση ενός προσώπου, καθιστώντας περιττή τη χειροκίνητη εισαγωγή δεδομένων από τον χρήστη. Ο ανιχνευτής προσώπου

διαμορφώνεται με συγκεκριμένες επιλογές προσαρμοσμένες στις απαιτήσεις της εφαρμογής, όπως η λειτουργία απόδοσης και οι ρυθμίσεις ανίχνευσης χαρακτηριστικών σημείων. Οι εικόνες που λαμβάνονται από την κάμερα αναλύονται από τον ανιχνευτή προσώπου για τον εντοπισμό και την αναγνώριση προσώπων σε κάθε καρέ. Τα πρόσωπα που ανιχνεύονται υποβάλλονται σε επεξεργασία για την εξαγωγή ορόσημων και χαρακτηριστικών του προσώπου, παρέχοντας λεπτομερείς πληροφορίες για κάθε πρόσωπο. Τα αποτελέσματα από τη διαδικασία ανίχνευσης προσώπου χρησιμοποιούνται για την ενημέρωση της διεπαφής χρήστη και την ενεργοποίηση επακόλουθων ενεργειών, όπως η επαλήθευση της ταυτότητας του χρήστη ή η ενεργοποίηση ειδοποιήσεων ασφαλείας.



Εικόνα 29 – Διάγραμμα Ροής για την Διαδικασία Ανίχνευσης Προσώπου με ML Kit

4.2.4 Επισκόπηση της CameraX

Η CameraX είναι μια βιβλιοθήκη που υποστηρίζεται από την Jetpack με βασικό στόχο να καταστήσει δυνατή για τους προγραμματιστές την ενσωμάτωση υπηρεσιών κάμερας στις εφαρμογές Android. Διαθέτει δημοσιευμένο ένα σταθερό API το οποίο είναι καλά βελτιωμένο ώστε να λειτουργεί σε πολλές συσκευές Android, γεγονός που διευκολύνει την ενσωμάτωση των χαρακτηριστικών της κάμερας σε διάφορες εφαρμογές [75]. Η CameraX έχει αναπτυχθεί με συνείδηση των διαφορετικών λύσεων του υποσυστήματος υλικού σε διάφορες συσκευές και ως εκ τούτου παρέχει στους προγραμματιστές ένα απλοποιημένο μέσο χειρισμού της κάμερας σε συσκευές Android.

4.2.4.1 Βασικά χαρακτηριστικά

Ευκολία χρήσης: Διαθέτει ένα API που προσφέρει τον ευκολότερο τρόπο ενσωμάτωσης λειτουργιών γύρω από την κάμερα σε εφαρμογές Android. Προσφέρει επίσης τη δυνατότητα στους προγραμματιστές να προσθέτουν λειτουργίες της κάμερας χωρίς να χρειάζεται να ασχοληθούν με τις ιδιαιτερότητες της κάμερας της συσκευής.

Συνειδητοποίηση του κύκλου ζωής: Η CameraX γνωρίζει τον κύκλο ζωής, παρέχει χαρακτηριστικά για την υποστήριξη του ανοίγματος και του κλεισίματος της κάμερας με βάση τον κύκλο ζωής της συγκεκριμένης εφαρμογής, με αποτέλεσμα να καταργείται η ανάγκη δημιουργίας εκτενέστερων ρουτινών.

Επιδόσεις: Η βιβλιοθήκη είναι η πιο αποδοτική και ελαφριά που είναι φιλική με την ικανότητα επεξεργασίας της συσκευής και την κίνηση όπως η κάμερα.

Στην εφαρμογή Flame Guard, οι λειτουργίες της CameraX είναι να καταγράφει εικόνες ώστε να μπορεί να επεξεργαστεί προκειμένου να ανιχνευθεί ή να αναγνωριστεί το πρόσωπο. Αυτό έχει το πλεονέκτημα ότι η λειτουργία της κάμερας αυτή η τελευταία είναι αξιόπιστη, αποτελεσματική και ομοιογενής σε όλες τις συσκευές Android.

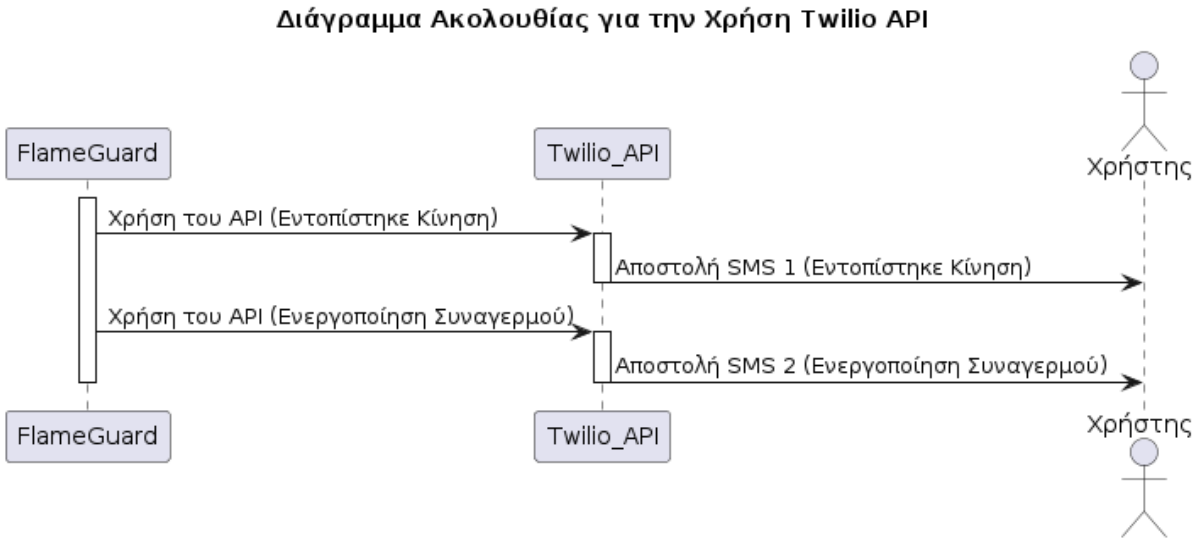
4.2.5 Χρήση του Twilio API

Το Twilio API είναι μια πλατφόρμα επικοινωνιών νέφους που παρέχει ένα ευέλικτο σύνολο εργαλείων για την αποστολή και τη λήψη μηνυμάτων ως SMS ή e-mail, καθώς και για την πραγματοποίηση ή τη λήψη τηλεφωνικών κλήσεων και παρόμοιων λειτουργιών με τη χρήση του API [76]. Ενώ το Firebase Cloud Messaging (FCM) εξαρτάται συχνά από τη σύνδεση του χρήστη στο διαδίκτυο για την αποστολή της ειδοποίησης, το Twilio API επιτρέπει στην εφαρμογή να στέλνει SMS, κάτι που είναι ιδιαίτερα σημαντικό για την ενημέρωση του χρήστη σχετικά με τα γεγονότα που αφορούν το περιβάλλον του.

4.2.5.1 Βασικά χαρακτηριστικά

Μηνύματα SMS: Το Twilio API επιτρέπει στις εφαρμογές να στέλνουν μηνύματα SMS σε χρήστες σε παγκόσμιο επίπεδο, εξασφαλίζοντας ότι λαμβάνουν σημαντικές ειδοποιήσεις και ειδοποιήσεις ανεξάρτητα από τη διαθεσιμότητα του διαδικτύου.

Επεκτασιμότητα: Το Twilio έχει σχεδιαστεί για να διαχειρίζεται μεγάλο όγκο μηνυμάτων και κλήσεων, καθιστώντας το κατάλληλο για εφαρμογές που απαιτούν αξιόπιστες και κλιμακούμενες λύσεις επικοινωνίας.



Εικόνα 30 - Διάγραμμα Ακολουθίας για την Χρήση Twilio API

4.3 Σχεδιασμός της Βάσης Δεδομένων

Η βάση δεδομένων της εφαρμογής Flame Guard είναι δομημένη για την αποτελεσματική διαχείριση των πληροφοριών χρήστη, των στοιχείων πρόσβασης, των ρυθμίσεων και των αρχείων καταγραφής. Αποτελείται από 5 κύριους πίνακες, *UserAuthentication*, *Users*, *Credentials*, *Settings* και *Logs*. Αυτοί οι πίνακες συνδέονται μεταξύ τους μέσω του χαρακτηριστικού *userID*, το οποίο χρησιμεύει ως ψευδοπρωτεύον κλειδί για τη διατήρηση των σχέσεων μεταξύ των πινάκων, παρόλο που η Firebase δεν υποστηρίζει άμεσα περιορισμούς πρωτεύοντος και ξένου κλειδιού.

Πίνακας UserAuthentication

Ο πίνακας *UserAuthentication* δημιουργείται και διαχειρίζεται αυτόματα από το Firebase Authentication. Αυτός ο πίνακας αποθηκεύει τα βασικά στοιχεία ελέγχου ταυτότητας των χρηστών.

- *userID:* Ένα μοναδικό αναγνωριστικό που αποδίδεται από την Firebase για κάθε χρήστη.
- *email:* Το email του χρήστη.
- *password:* Ο κωδικός πρόσβασης του χρήστη, που αποθηκεύεται με ασφάλεια από την Firebase.

Πίνακας Users

Ο πίνακας *Users* περιέχει πρόσθετες πληροφορίες χρηστών που δεν διαχειρίζεται το σύστημα Firebase Authentication. Ο πίνακας αυτός έχει σχεδιαστεί χειροκίνητα για να κρατάει συγκεκριμένες λεπτομέρειες σχετικά με τους χρήστες.

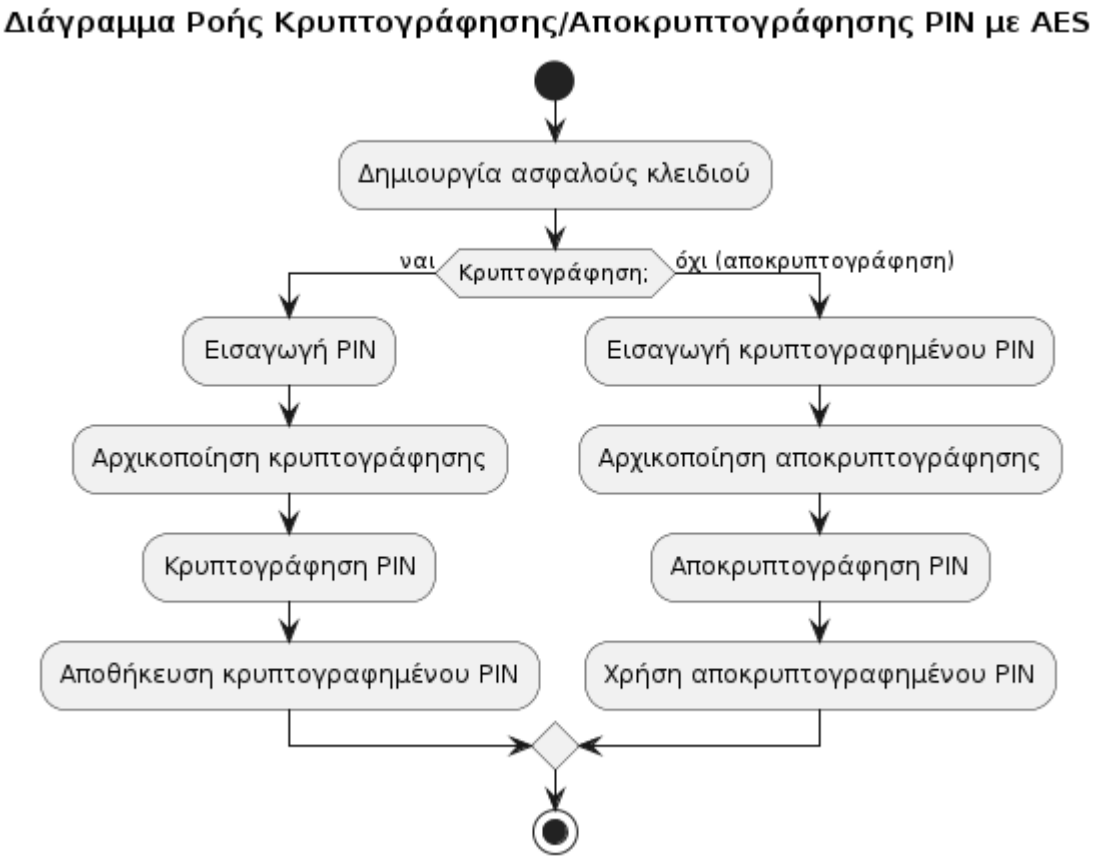
- *userID*
- *email*
- *newUser:* Μια boolean μεταβλητή που δείχνει αν ο χρήστης είναι νέος (true) ή υπάρχον (false).

Πίνακας Credentials

Ο πίνακας Credentials αποθηκεύει ευαίσθητες πληροφορίες που σχετίζονται με την ασφάλεια του χρήστη, όπως το PIN απενεργοποίησης συναγερμού και τα στοιχεία αναγνώρισης προσώπου. Τα δεδομένα αυτά αποθηκεύονται σε κρυπτογραφημένη μορφή για να διασφαλιστεί η ασφάλεια.

- *userID*
- *userFace:* Κρυπτογραφημένα δεδομένα αναγνώρισης προσώπου.
- *userPin:* Κρυπτογραφημένο PIN απενεργοποίησης συναγερμού.

Για την αποκρυπτογράφηση χρησιμοποιείται το Advanced Encryption Standard (AES), το οποίο παρέχει μια ισχυρή μέθοδο για την ασφάλεια ευαίσθητων δεδομένων. Η διαδικασία αποκρυπτογράφησης περιλαμβάνει τη χρήση ενός ασφαλούς κλειδιού για τη μετατροπή των κρυπτογραφημένων δεδομένων πίσω στην αρχική τους μορφή, διασφαλίζοντας ότι μόνο εξουσιοδοτημένες εφαρμογές μπορούν να έχουν πρόσβαση σε αυτές τις πληροφορίες.



Εικόνα 31 - Διάγραμμα Δραστηριοτήτων Κρυπτογράφησης/Αποκρυπτογράφησης PIN με AES

Πίνακας Settings

Ο πίνακας *Settings* αποθηκεύει διάφορες ρυθμίσεις για κάθε χρήστη, οι οποίες διαμορφώνουν τον τρόπο συμπεριφοράς της εφαρμογής Flame Guard για κάθε χρήστη.

- *userID*
- *alarmTriggerStartSec:* Ο χρόνος σε δευτερόλεπτα πριν από την ενεργοποίηση του συναγερμού.
- *cameraFace:* Καθορίζει εάν χρησιμοποιείται η μπροστινή ή η πίσω κάμερα.
- *guardStartTimeSec:* Ο χρόνος σε δευτερόλεπτα κατά τον οποίο ξεκινά η λειτουργία φύλαξης.
- *motionSensitivity:* Επίπεδο ευαισθησίας για την ανίχνευση κίνησης.

Πίνακας Logs

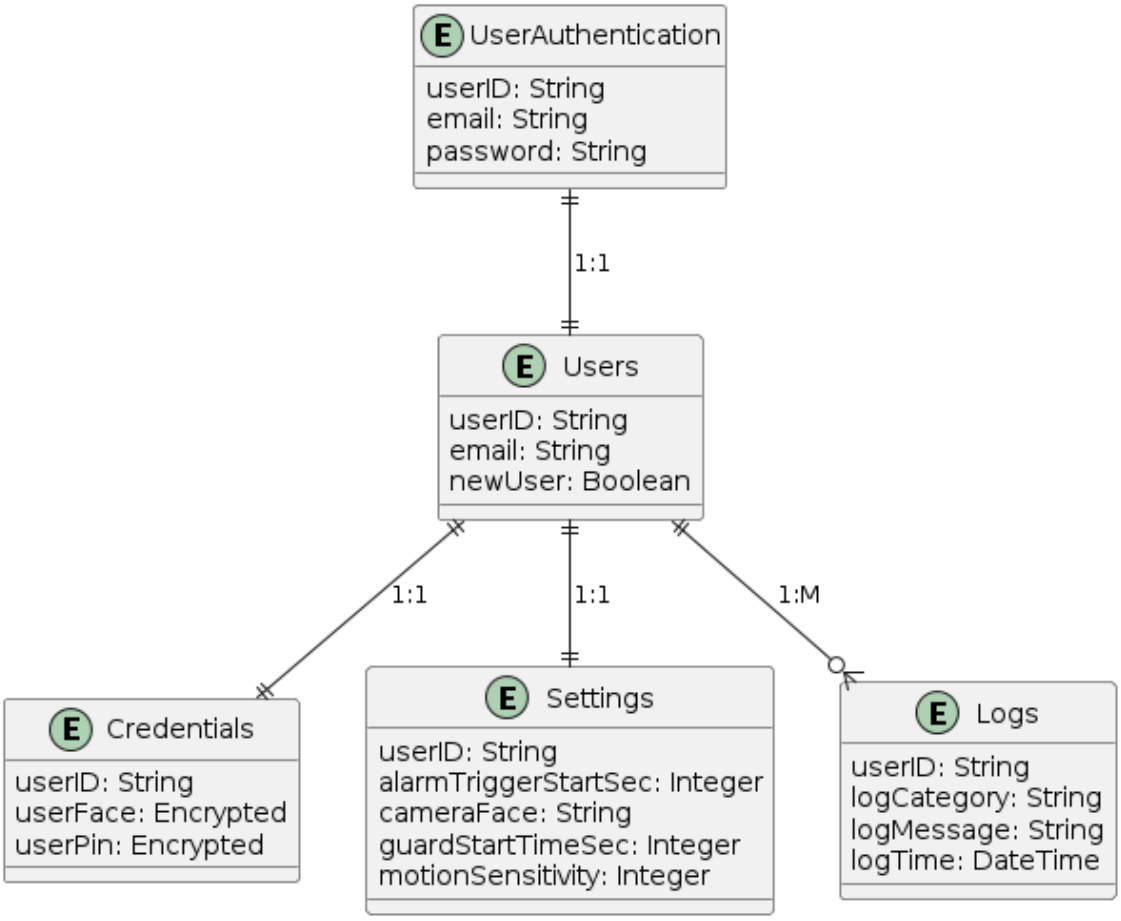
Ο πίνακας *Logs* καταγράφει όλες τις δραστηριότητες του χρήστη εντός της εφαρμογής Flame Guard, παρέχοντας μια λεπτομερή διαδρομή ελέγχου. Αυτός ο πίνακας έχει σχεδιαστεί για να βοηθήσει τους χρήστες και τους διαχειριστές να παρακολουθούν τα συμβάντα ασφαλείας και τη χρήση της εφαρμογής.

- *userID*
- *logCategory:* Κατηγορία της καταγραφής (π.χ. συναγερμός, ανίχνευση κίνησης).
- *logMessage:* Αναλυτικό μήνυμα που περιγράφει το συμβάν καταγραφής.
- *logTime:* Χρονοσήμανση της ημερομηνίας της καταγραφής.

Στην τρέχουσα υλοποίηση, οι χρήστες έχουν πρόσβαση μόνο σε αρχεία καταγραφής που σχετίζονται με συναγερμούς, όπως όταν ενεργοποιείται ο συναγερμός, όταν ανιχνεύεται κίνηση, όταν εισάγεται ο κωδικός PIN, οι προσπάθειες επαλήθευσης προσώπου και άλλα σχετικά στοιχεία.

Κατά την υλοποίηση της Flame Guard, δημιουργήθηκε μια κλάση FirebaseDatabaseHelper για τον αποτελεσματικό χειρισμό διαφόρων λειτουργιών της βάσης δεδομένων. Αυτή η κλάση παρέχει καθολικές λειτουργίες για λειτουργίες όπως η προσθήκη αρχείων καταγραφής, η ανάκτηση διαπιστευτηρίων χρήστη, η ενημέρωση των ρυθμίσεων χρήστη και η ανάκτηση αρχείων καταγραφής χρήστη. Κάθε λειτουργία χρησιμοποιεί ένα databaseReference για να αλληλεπιδράσει με τη βάση δεδομένων πραγματικού χρόνου Firebase, εξασφαλίζοντας ασύγχρονο και αποτελεσματικό χειρισμό δεδομένων, παρέχοντας έτσι μια ομαλή εμπειρία χρήσης.

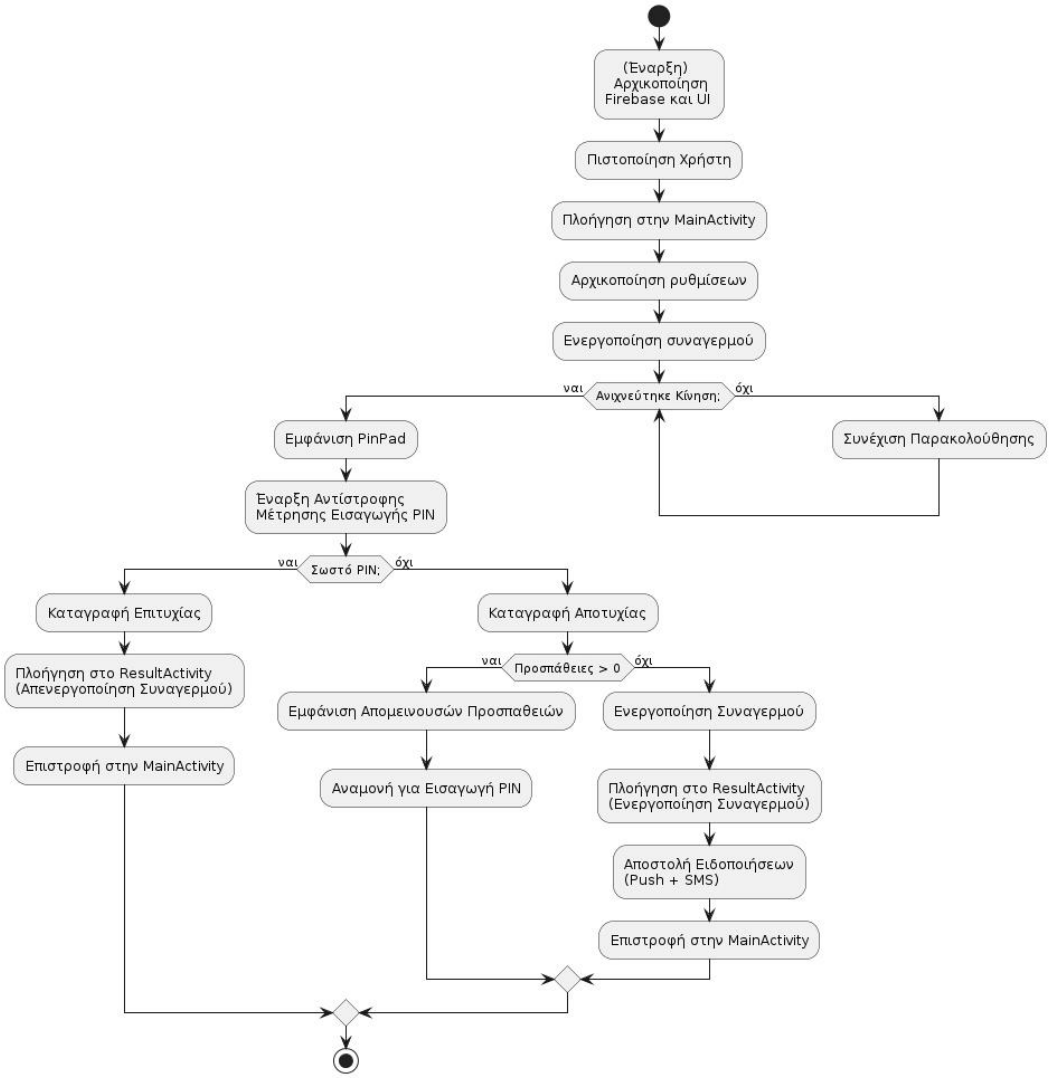
Με τη συγκέντρωση των λειτουργιών της βάσης δεδομένων στην κλάση FirebaseDatabaseHelper, η εφαρμογή διατηρεί καθαρό, συντηρήσιμο και διαχειρίσιμο κώδικα. Αυτή η δομή διευκολύνει τις εύκολες ενημερώσεις και τροποποιήσεις της λογικής αλληλεπίδρασης με τη βάση δεδομένων χωρίς να επηρεάζονται άλλα τμήματα της εφαρμογής.



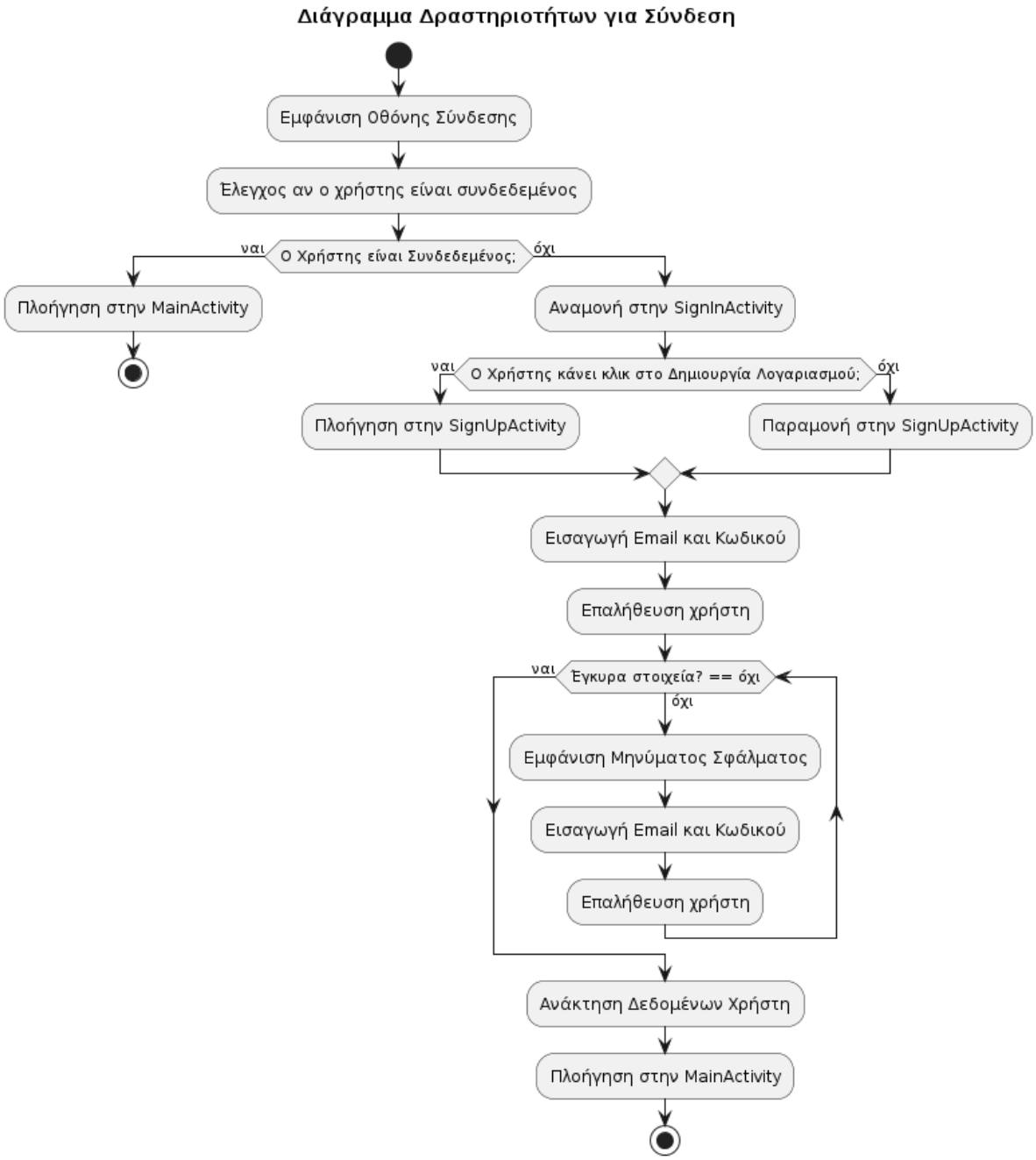
Εικόνα 32 - Ανάλυση και Σχεδίαση Βάση Δεδομένων με UML

4.4 Αρχιτεκτονική και Σχεδιασμός

Ο σχεδιασμός του διαγράμματος ροής της εφαρμογής Flame Guard περιλαμβάνει τη δομή της πλοήγησης και των αλληλεπιδράσεων του χρήστη εντός της εφαρμογής. Το διάγραμμα ροής ξεκινάει με την κύρια οθόνη ως σημείο εισόδου στην εφαρμογή. Από εκεί, οι χρήστες παρουσιάζονται με διάφορες λειτουργίες οργανωμένες σε διακριτές ενότητες. Κάθε λειτουργία αντιπροσωπεύει μια συγκεκριμένη λειτουργικότητα ή πληροφορία με την οποία οι χρήστες μπορούν να αλληλεπιδράσουν. Αυτή η οργανωμένη προσέγγιση εξασφαλίζει μια απρόσκοπτη και διαισθητική εμπειρία χρήστη, επιτρέποντας στους χρήστες να περιηγηθούν αποτελεσματικά στις λειτουργίες της εφαρμογής.



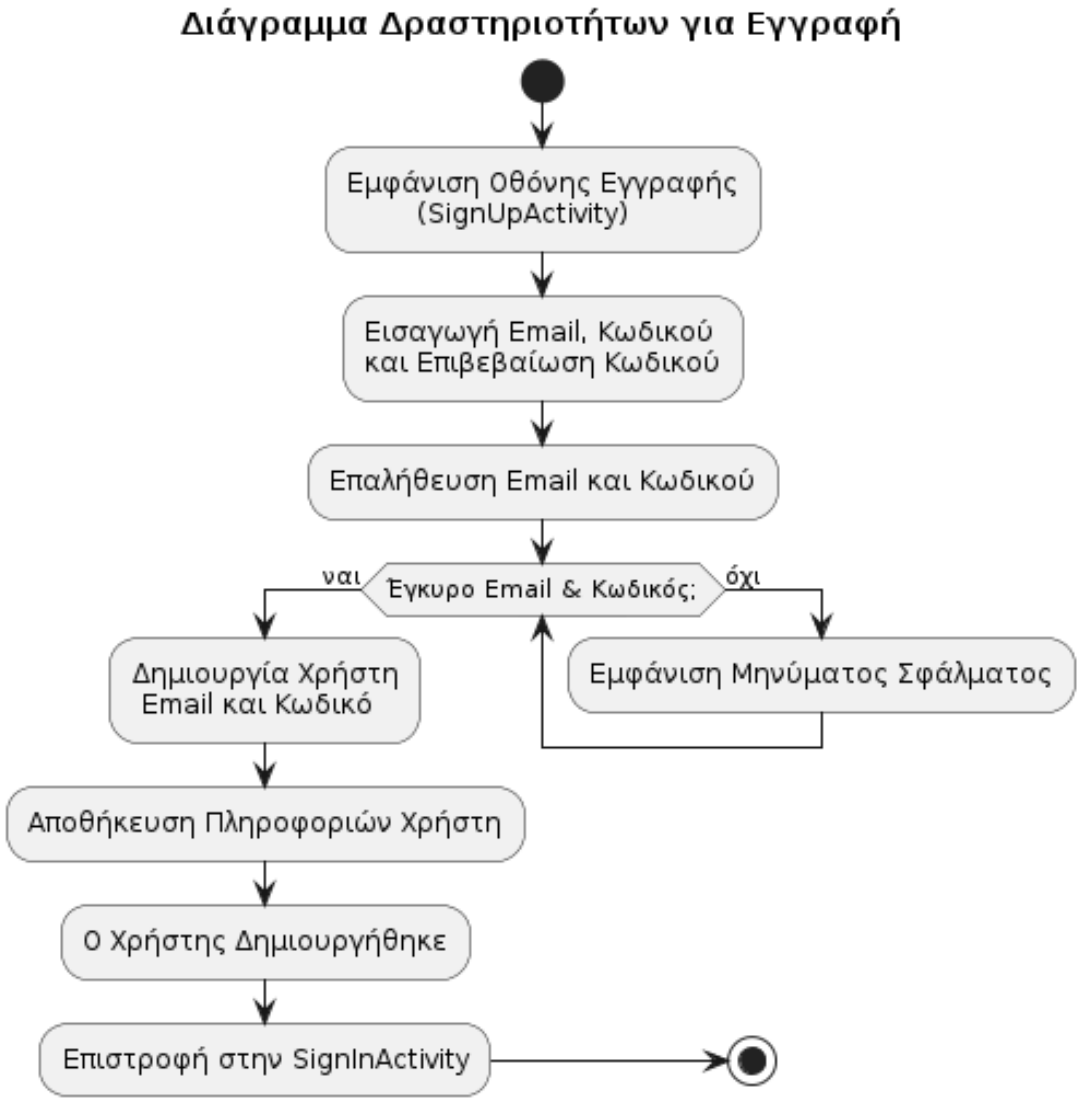
Εικόνα 33 - Διάγραμμα Δραστηριοτήτων Γενικής Αρχιτεκτονικής της Εφαρμογής



Εικόνα 34 - Διάγραμμα Δραστηριοτήτων για Σύνδεση

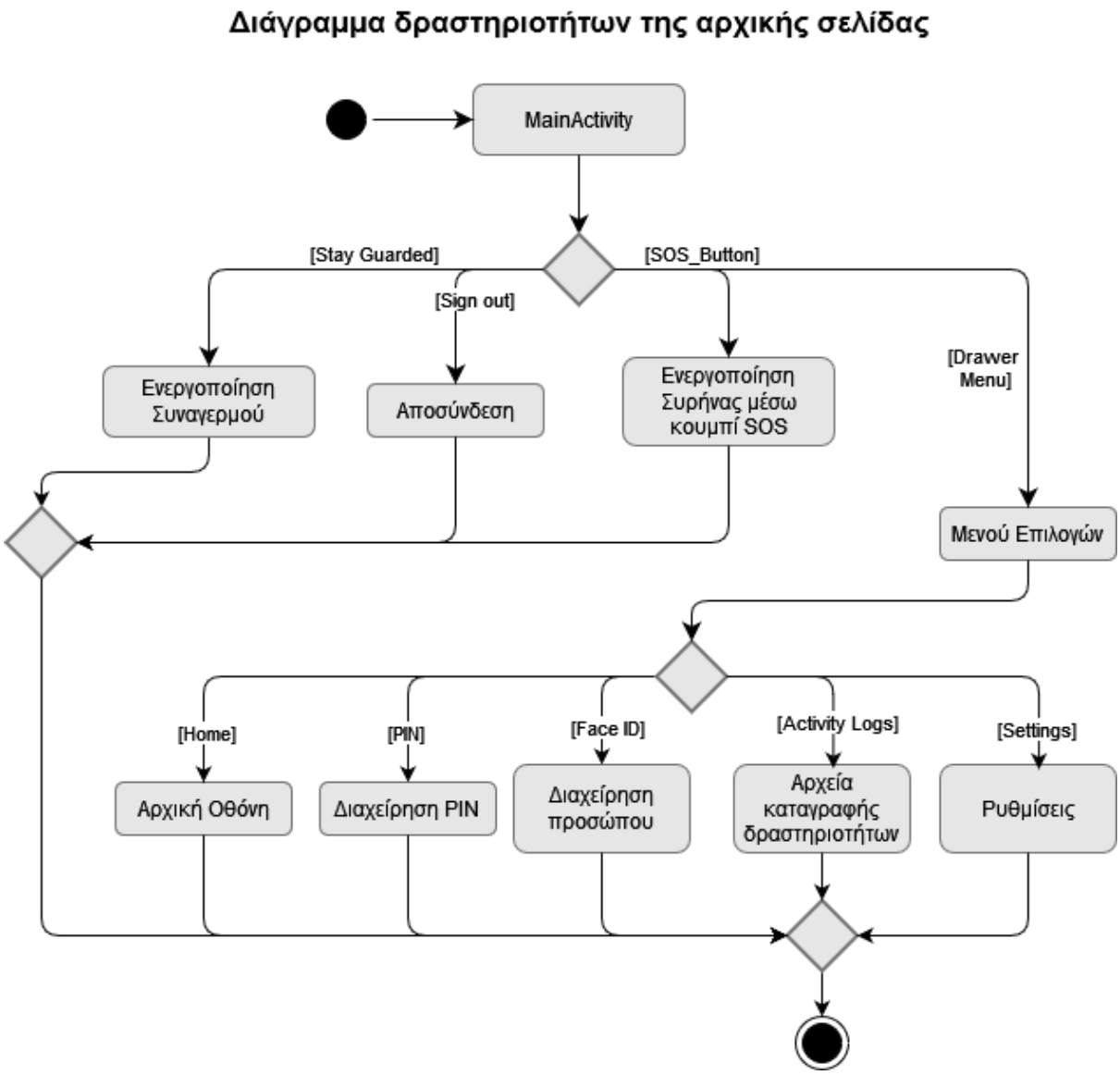
Η οθόνη σύνδεσης (SignInActivity) χρησιμεύει ως πύλη για την πρόσβαση των χρηστών στην εφαρμογή FlameGuard. Σε αυτή την οθόνη, οι χρήστες καλούνται να εισάγουν το email και τον κωδικό πρόσβασής τους για να συνδεθούν στην εφαρμογή. Η οθόνη περιλαμβάνει έναν σύνδεσμο για τους χρήστες που πρέπει να δημιουργήσουν νέο λογαριασμό, ο οποίος τους οδηγεί στη σελίδα εγγραφής (SignUpActivity). Μετά την επιτυχή πιστοποίηση του χρήστη, ο χρήστης πλοηγείται στη σελίδα MainActivity. Εάν τα στοιχεία πιστοποίησης είναι άκυρα, εμφανίζεται ένα

μήνυμα σφάλματος, το οποίο προτρέπει τον χρήστη να εισάγει εκ νέου τις πληροφορίες του.



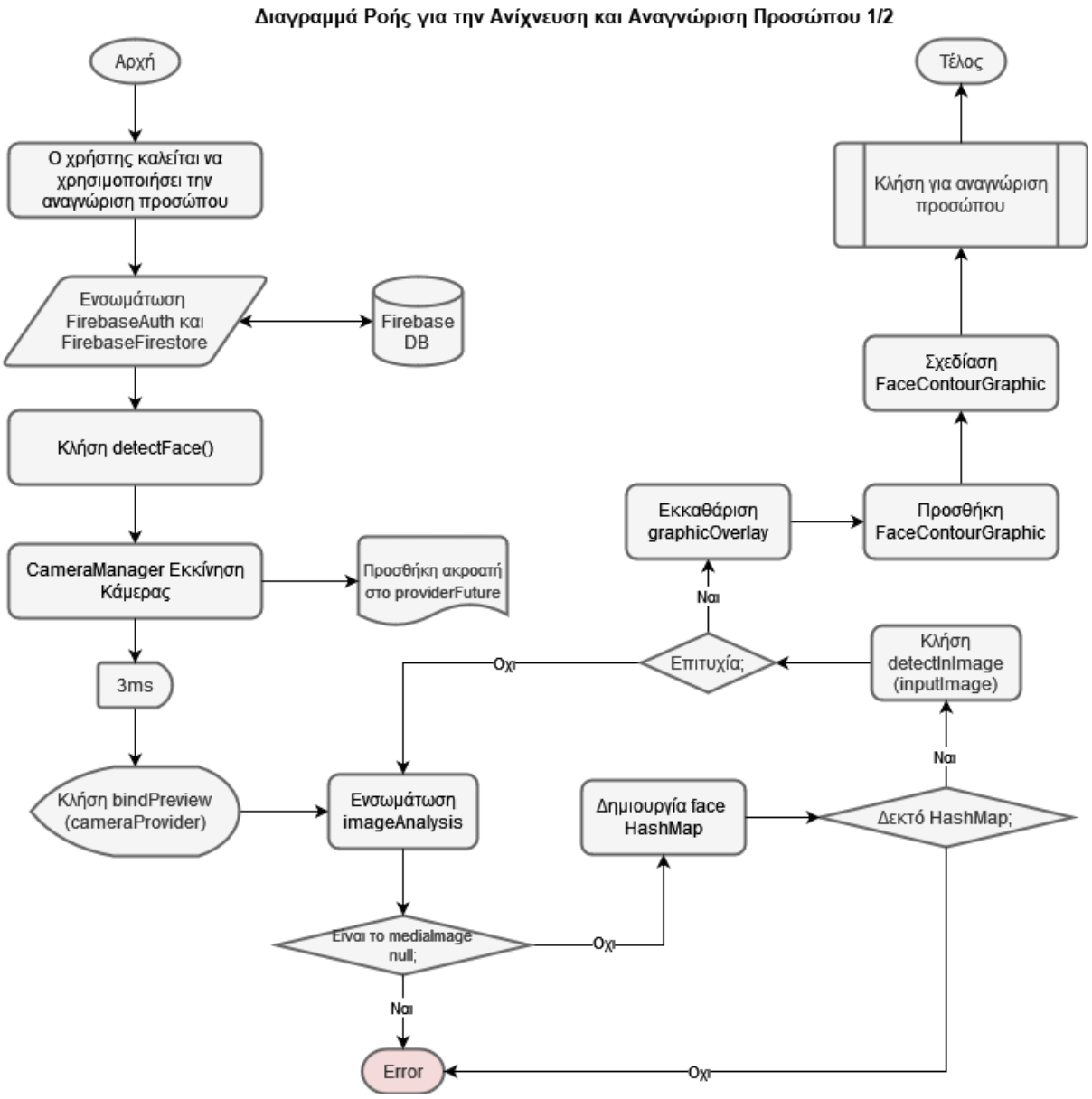
Εικόνα 35 - Διάγραμμα Δραστηριοτήτων για Εγγραφή

Η οθόνη εγγραφής (SignUpActivity) επιτρέπει στους νέους χρήστες να δημιουργήσουν έναν λογαριασμό στην εφαρμογή FlameGuard. Οι χρήστες πρέπει να εισάγουν ένα έγκυρο email, έναν κωδικό πρόσβασης και να επιβεβαιώσουν τον κωδικό πρόσβασης. Αν διασφαλιστεί ότι η μορφή του email είναι σωστή και ότι ο κωδικός πρόσβασης πληροί τις απαιτήσεις ασφαλείας, οι πληροφορίες του χρήστη αποθηκεύονται στη βάση δεδομένων και ο χρήστης ανακατευθύνεται πίσω στη σελίδα σύνδεσης για να συνδεθεί με τα νέα του στοιχεία πρόσβασης.



Εικόνα 36 - Διάγραμμα Δραστηριοτήτων της Αρχικής Σελίδας

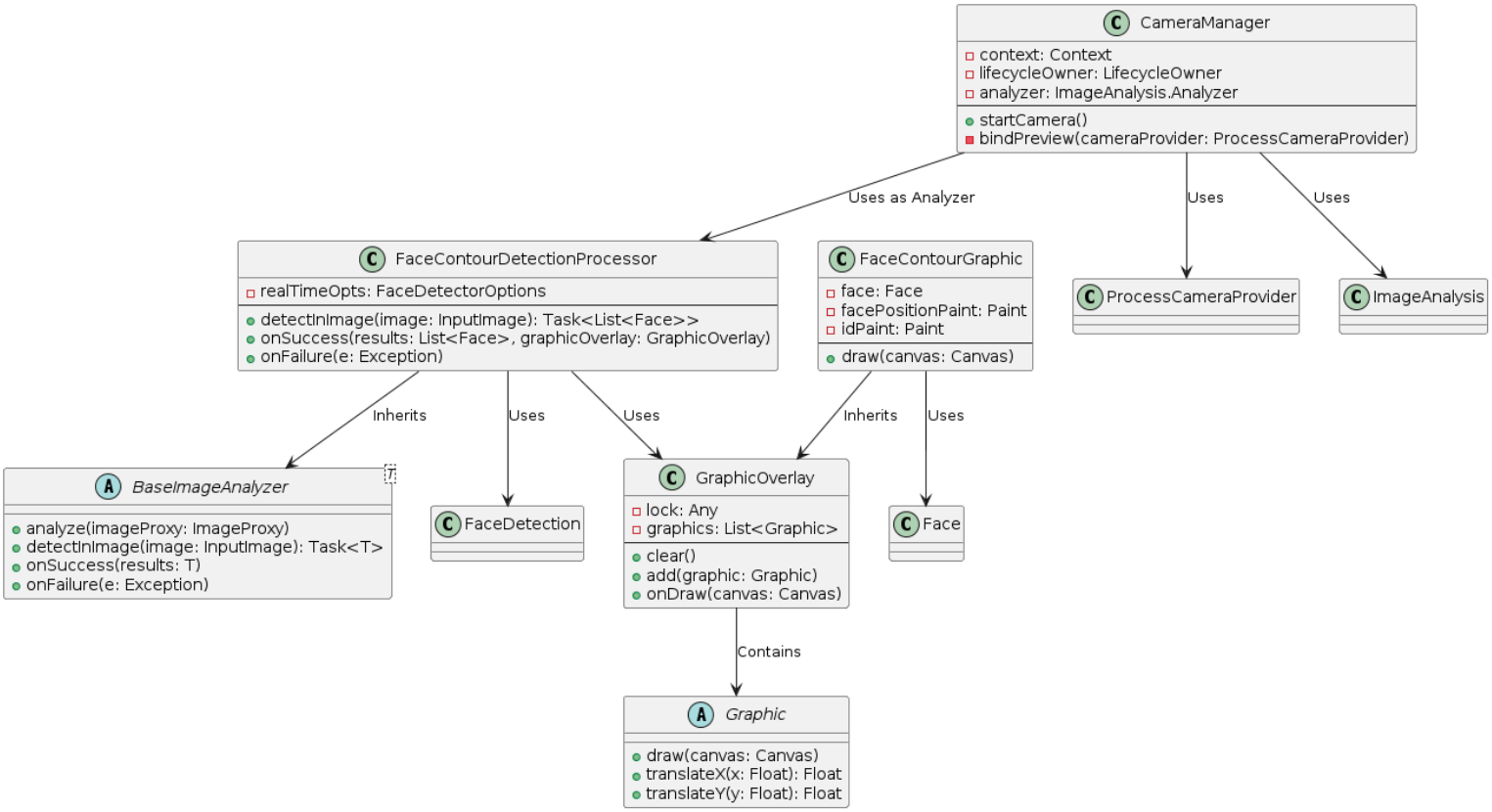
Η δραστηριότητα MainActivity στην εφαρμογή Flame Guard χρησιμεύει ως κεντρικός κόμβος, παρέχοντας στους χρήστες πρόσβαση στις κύριες λειτουργίες της εφαρμογής. Από αυτή τη δραστηριότητα, οι χρήστες μπορούν να ενεργοποιήσουν το σύστημα συναγερμού για να παραμείνει σε φύλαξη, να ενεργοποιήσουν μια συναγερμό SOS ή να περιηγηθούν στην εφαρμογή χρησιμοποιώντας το DrawerMenu. Το DrawerMenu προσφέρει γρήγορη πρόσβαση σε βασικές λειτουργίες, όπως το Home, το Pin Menu, το Face ID Menu, τα Activity Logs και τις Settings. Επιπλέον, οι χρήστες έχουν τη δυνατότητα να αποσυνδεθούν από την εφαρμογή απευθείας από το MainActivity.



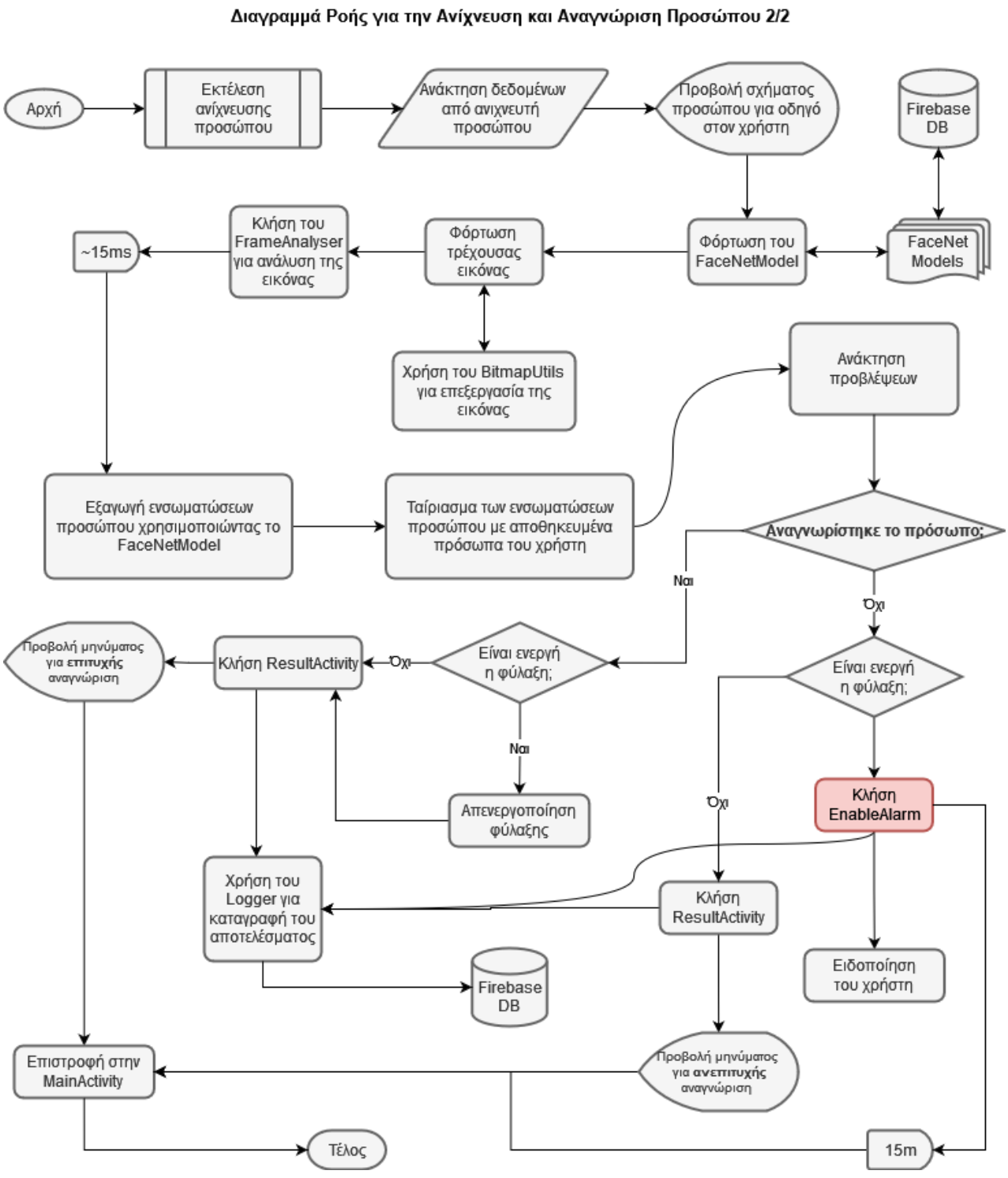
Εικόνα 37 - Διάγραμμα Ροής για την Ανίχνευση και Αναγνώριση Προσώπου 1/2

Η αρχιτεκτονική της ανίχνευσης προσώπου της εφαρμογής ξεκινά με το να καλείται ο χρήστης να χρησιμοποιήσει την αναγνώριση προσώπου. Αρχικά, η εφαρμογή ενσωματώνει το FirebaseAuth για τον έλεγχο ταυτότητας και το Firebase DB για την αποθήκευση δεδομένων. Η διαδικασία συνεχίζεται με την κλήση της detectFace(), ενώ η CameraManager εκκινεί την κάμερα και προσθέτει έναν ακροατή στο providerFuture για τη διαχείριση των δεδομένων της κάμερας. Στη συνέχεια, καλείται η κλήση bindPreview(cameraProvider) για τη δέσμευση της προεπισκόπησης της κάμερας στο σύστημα και ενσωματώνεται η imageAnalysis για την ανάλυση των δεδομένων από

την κάμερα. Εάν το mediaImage δεν είναι null, δημιουργείται ένα inputImage και καλείται η συνάρτηση detectInImage(inputImage). Εάν είναι επιτυχής, το graphicOverlay καθαρίζεται και προστίθεται το FaceContourGraphic. Η διαδικασία συνεχίζεται με την ανίχνευση προσώπου χρησιμοποιώντας έναν προκαθορισμένο αλγόριθμο και ολοκληρώνεται με το τέλος της ανίχνευσης προσώπου.

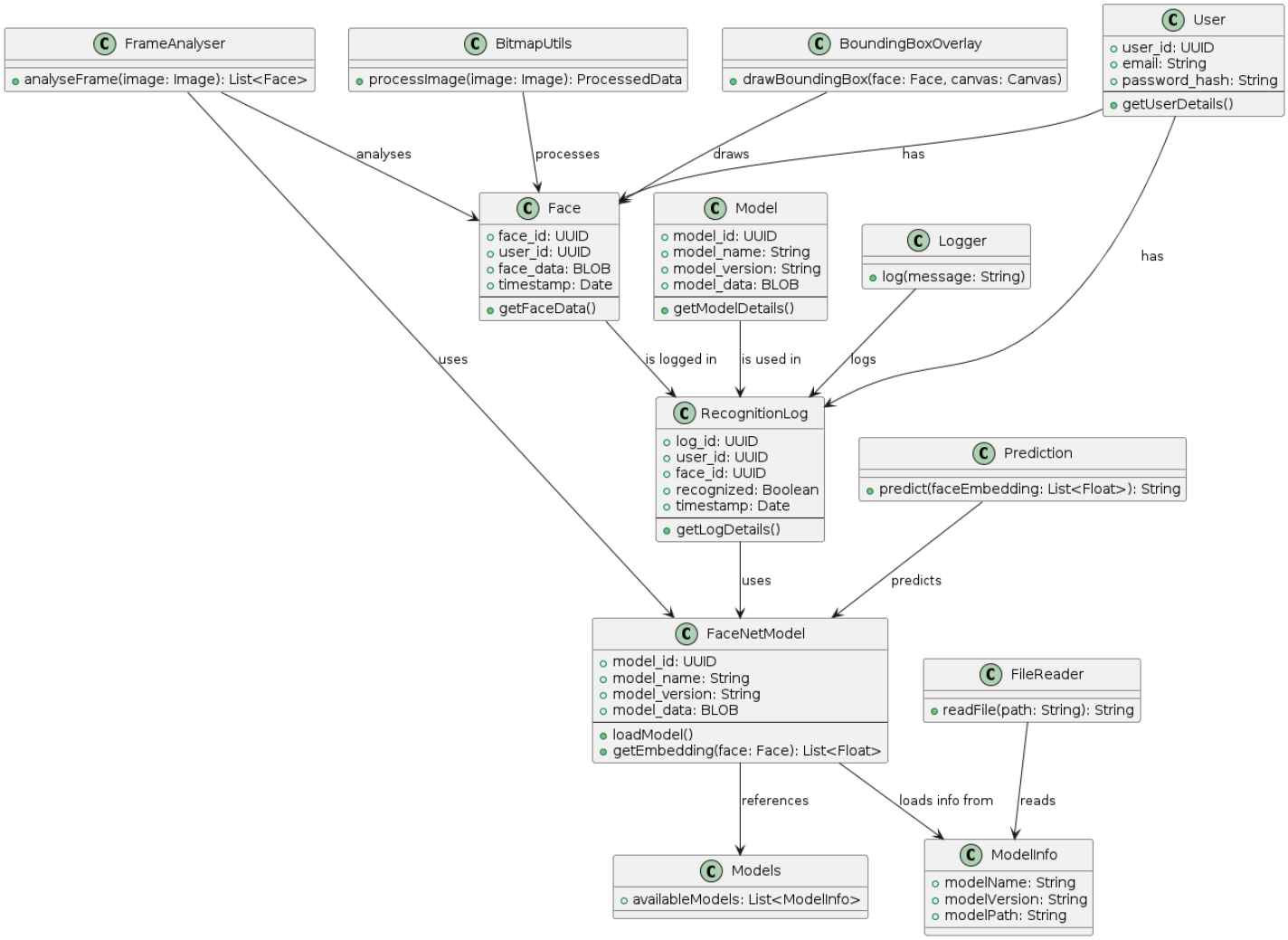


Εικόνα 38 - Διάγραμμα Κλάσης της Ανίχνευσης Προσώπου

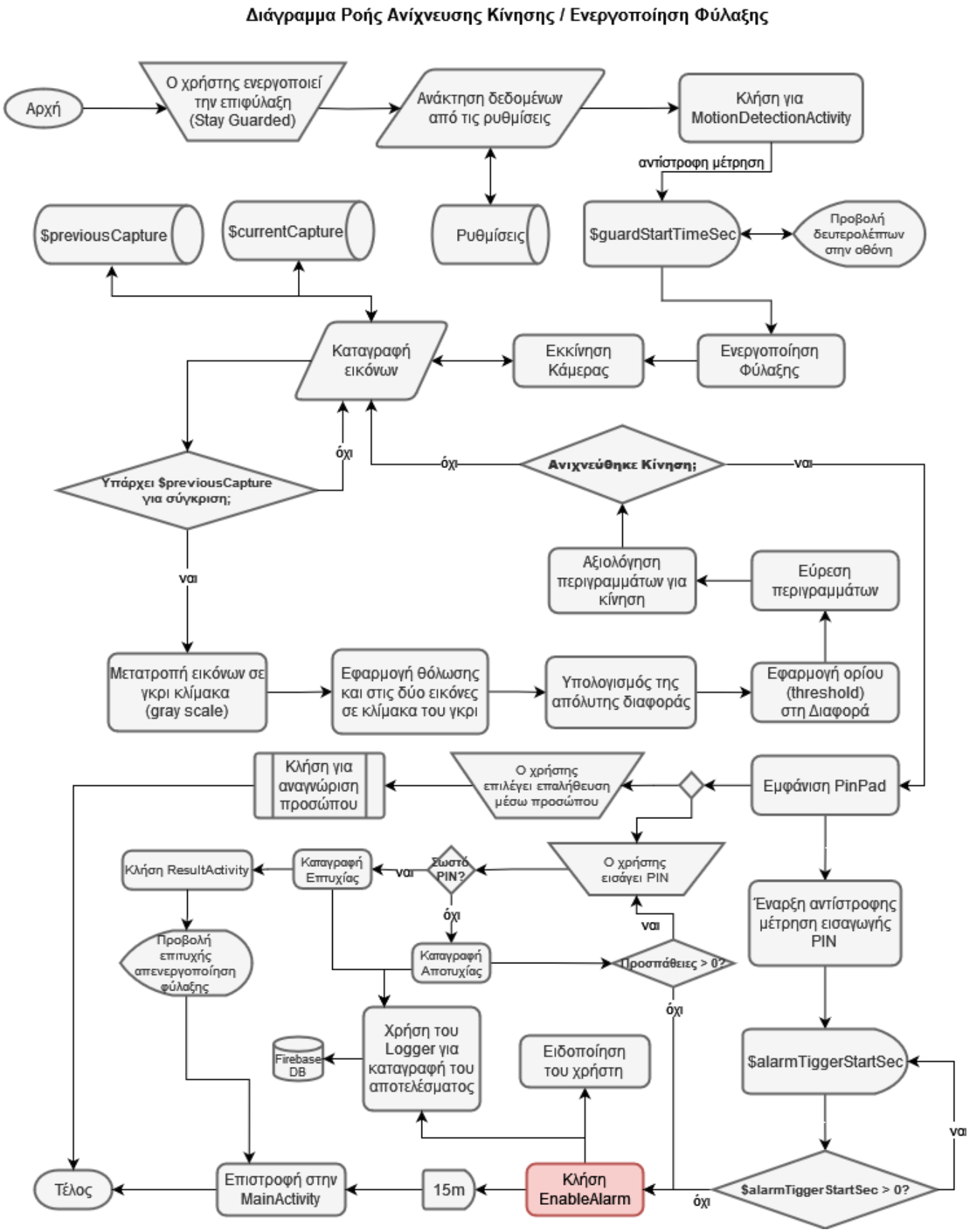


Εικόνα 39 - Διάγραμμα Ροής για την Ανίχνευση και Αναγνώριση Προσώπου 2/2

Η διαδικασία αναγνώρισης προσώπου ξεκινά με την ανίχνευση προσώπου. Μόλις αποκτήσει μια εικόνα από τον ανιχνευτή προσώπου, καλείται η FrameAnalyser για να αναλύσει την εικόνα, ανακτώντας πρόσθετα δεδομένα από τον ανιχνευτή προσώπου και φορτώνοντας το FaceNetModel. Στη συνέχεια, η τρέχουσα εικόνα επεξεργάζεται με τη χρήση του BitmapUtils. Μέσα σε περίπου 15ms, εξάγονται ενσωματώσεις προσώπου χρησιμοποιώντας το FaceNetModel και αντιστοιχίζονται με τα αποθηκευμένα πρόσωπα του χρήστη. Εάν η αναγνώριση είναι επιτυχής, εμφανίζεται ένα μήνυμα στον χρήστη και το αποτέλεσμα καταγράφεται με τη χρήση του Logger. Εάν η φύλαξη είναι ενεργή και το πρόσωπο δεν αναγνωρίζεται, ενεργοποιείται η σειρήνα και ο χρήστης ειδοποιείται μέσω Firebase Cloud Messaging ή SMS με χρήση του Twilio API. Ο συναγερμός σταματά μετά από 15 λεπτά, επιστρέφοντας στη MainActivity. Σε αντίθετη περίπτωση, εμφανίζεται μήνυμα για την επιτυχή αναγνώριση και η φύλαξη απενεργοποιείται.



Εικόνα 40 - Διάγραμμα Κλάσης της Αναγνώρισης Προσώπου



Εικόνα 41 - Διάγραμμα Ροής Ανίχνευσης Κίνησης / Ενεργοποίηση Φύλαξης

Η διαδικασία ανίχνευσης κίνησης στην εφαρμογή ξεκινάει όταν ο χρήστης ενεργοποιεί τη λειτουργία φύλαξης. Το σύστημα λαμβάνει τις ρυθμίσεις διαμόρφωσης, και καταγράφει την ώρα έναρξης της φύλαξης. Ξεκινά η δραστηριότητα ανίχνευσης κίνησης μετά από την προκαθορισμένο χρόνο που αποκτήθηκε από τις ρυθμόσεις. Η κάμερα αρχίζει να καταγράφει εικόνες, αποθηκεύοντας την τρέχουσα εικόνα ως currentCapture, και μεταφέρει το currentCapture στην μεταβλητή previousCapture. Αν η λήψη γίνεται για πρώτη φορά, η εφαρμογή συνεχίζει με την καταγραφεί της επόμενης εικόνας. Οι εικόνες μετατρέπονται σε κλίμακα του γκρι και εφαρμόζεται η θόλωση, για τη μείωση του θορύβου και των μικρών διακυμάνσεων, γεγονός που βοηθά στην ανίχνευση σημαντικών αλλαγών στην κίνηση. Το σύστημα υπολογίζει την απόλυτη διαφορά μεταξύ των εικόνων και εφαρμόζει ένα όριο (threshold) για την ανίχνευση της κίνησης. Εάν ανιχνευθεί κίνηση, αξιολογούνται τα περιγράμματα. Εάν εντοπιστεί σημαντική κίνηση, ο χρήστης ειδοποιείται μέσω ειδοποίησης ή SMS. Ο χρήστης μπορεί είτε να επιβεβαιώσει την ταυτότητα μέσω της αναγνώρισης προσώπου είτε να εισάγει ένα PIN. Εάν η εισαγωγή του PIN αποτύχει, ενεργοποιείται συναγερμός και ο χρήστης ειδοποιείται. Μετά από 15 λεπτά, ο συναγερμός σταματάει και το σύστημα επιστρέφει στη MainActivity, καταγράφοντας όλα τα συμβάντα χρησιμοποιώντας το Logger. Σε περίπτωση που ο χρήστης επιλέγει επαλήθευση μέσω αναγνώρισης προσώπου, μεταφέρεται στην αντίστοιχη διαδικασία.

4.5 Υλοποίηση και Ανάπτυξη της Εφαρμογής

Η εφαρμογή Flame Guard αναπτύχθηκε για να παρέχει μια προηγμένη λύση ασφαλείας που ενσωματώνει χαρακτηριστικά ανίχνευσης και αναγνώρισης προσώπου, ανίχνευσης κίνησης και απόκρισης έκτακτης ανάγκης. Αυτή η ενότητα περιγράφει λεπτομερώς τη διαδικασία υλοποίησης και ανάπτυξης της εφαρμογής FlameGuard, εστιάζοντας στο σχεδιασμό της.

4.5.1 Βασικά χαρακτηριστικά της εφαρμογής

Η εφαρμογή προσφέρει ένα ολοκληρωμένο σύνολο χαρακτηριστικών που έχουν σχεδιαστεί για να ενισχύουν την ασφάλεια και να παρέχουν στους χρήστες ένα αξιόπιστο και αποτελεσματικό μέσο παρακολούθησης και αντιμετώπισης πιθανών απειλών.

Ακολουθούν τα βασικά χαρακτηριστικά της εφαρμογής:

Αναγνώριση προσώπου

- *Ανίχνευση σε πραγματικό χρόνο:* Η εφαρμογή χρησιμοποιεί προηγμένα μοντέλα μηχανικής μάθησης για τον εντοπισμό και την αναγνώριση προσώπων σε πραγματικό χρόνο.
- *Βάση δεδομένων γνωστών προσώπων:* Οι χρήστες μπορούν να αποθηκεύουν πολλά πρόσωπα σε μια ασφαλή βάση δεδομένων, επιτρέποντας την εφαρμογή να αναγνωρίζει γρήγορα τα εγκεκριμένα άτομα.
- *Ακρίβεια και απόδοση:* Αξιοποιώντας το FaceNetModel, η εφαρμογή διασφαλίζει υψηλή ακρίβεια στην εξαγωγή και τη σύγκριση της ενσωμάτωσης προσώπων, καθιστώντας τη διαδικασία αναγνώρισης τόσο γρήγορη όσο και αξιόπιστη.

Ανίχνευση κίνησης

- *Παρακολούθηση σε πραγματικό χρόνο:* Συνεχής παρακολούθηση για κίνηση εντός του πεδίου όρασης της κάμερας.
- *Ρύθμιση ευαισθησίας:* Οι χρήστες μπορούν να ρυθμίσουν το όριο ευαισθησίας κίνησης για να μειώσουν τους ψευδείς συναγερμούς και να προσαρμόσουν την ανίχνευση στις συγκεκριμένες ανάγκες τους.
- *Καταγραφή συμβάντων:* Κάθε συμβάν ανίχνευσης κίνησης καταγράφεται με λεπτομερείς πληροφορίες, συμπεριλαμβανομένης της ώρας και της ημερομηνίας ανίχνευσης, εξασφαλίζοντας μια πλήρη καταγραφή των δραστηριοτήτων.

Ειδοποιήσεις χρηστών

- *Ειδοποιήσεις εφαρμογών:* Ειδοποιήσεις σε πραγματικό χρόνο για συμβάντα ανίχνευσης κίνησης αποστέλλονται σε μια άλλη συσκευή του χρήστη μέσω Firebase Cloud Messaging.
- *Ειδοποιήσεις SMS:* Για κρίσιμες περιπτώσεις, όπως η ανίχνευση κίνησης όταν ο χρήστης δεν έχει πρόσβασει σε διαδίκτυο, αποστέλλονται ειδοποιήσεις μέσω SMS χρησιμοποιώντας το API της Twilio για να εξασφαλιστεί η έγκαιρη ενημέρωση.

Βελτιστοποίηση επιδόσεων

- *Βελτιστοποίηση απόδοσης:* Χρησομοποιήθηκαν βελτιστοποιημένοι αλγόριθμοι για την αναγνώριση προσώπου και την ανίχνευση κίνησης, ώστε να εξασφαλίζεται ελάχιστη καθυστέρηση και υψηλή απόδοση.

4.5.2 Διεπαφή του Χρήστη

Η εφαρμογή FlameGuard περιλαμβάνει διάφορα *Activities* (10 συνολικά) και *Fragments* (11 συνολικά) που μαζί δημιουργούν ένα ολοκληρωμένο και φιλικό προς το χρήστη περιβάλλον.

Παρακάτω, κατηγοριοποιούνται και περιγράφονται κάθε ένα από αυτά:

4.5.2.1 Activities / Δραστηριότητες

- *MainActivity:* Χρησιμεύει ως ο κεντρικός κόμβος της εφαρμογής, παρέχοντας πρόσβαση σε διάφορες λειτουργίες όπως οι ρυθμίσεις.
- *SignInActivity:* Παρέχει τις λειτουργίες σύνδεσης των χρηστών, επιτρέποντας στους χρήστες να συνδεθούν με ασφάλεια στην εφαρμογή.
- *SignUpActivity:* Πραγματοποιεί την εγγραφή χρηστών, επιτρέποντας σε νέους χρήστες να δημιουργήσουν λογαριασμούς και να αποκτήσουν πρόσβαση στην εφαρμογή.
- *WelcomeActivity:* Η αρχική δραστηριότητα που καλωσορίζει τους νέους χρήστες και παρέχει μια εισαγωγή στην εφαρμογή.
- *PinActivity:* Χρησιμεύει για τις λειτουργίες που σχετίζονται με το PIN, συμπεριλαμβανομένου του καθορισμού, της επαλήθευσης και της αλλαγής του PIN που χρησιμοποιείται για πρόσθετη ασφάλεια.
- *FaceRecognitionActivity:* Ειδική δραστηριότητα που αναλαμβάνει τη διαχείριση εργασιών αναγνώρισης προσώπου, ξεχωριστά από την κύρια δραστηριότητα για τον εξορθολογισμό των εργασιών, συμπεριλαμβανομένου του καθορισμού, της επαλήθευσης και της αλλαγής του προσώπου.
- *AddFaceActivity:* Διευκολύνει την προσθήκη νέων προσώπων στη βάση δεδομένων.
- *FaceRecognizerMainActivity:* Η κύρια δραστηριότητα για τις λειτουργίες αναγνώρισης προσώπων. Χειρίζεται την έναρξη και τη διαχείριση της διαδικασίας αναγνώρισης προσώπου.

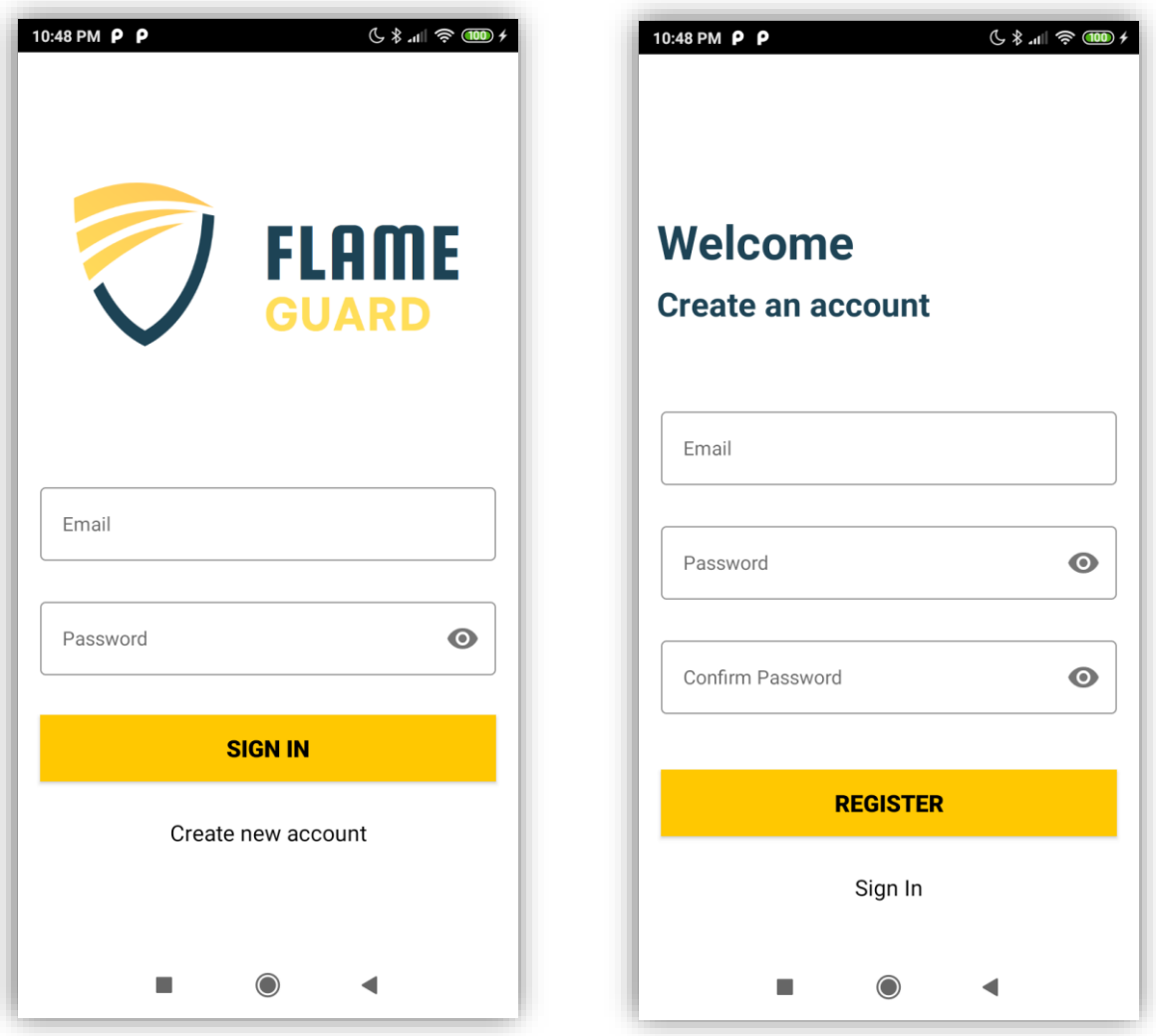
- *MotionDetectorMainActivity:* Διαχειρίζεται τις δραστηριότητες ανίχνευσης κίνησης. Αυτή η δραστηριότητα καταγράφει και επεξεργάζεται εικόνες για την ανίχνευση κίνησης και ειδοποιεί τον χρήστη όταν ανιχνεύεται κίνηση.
- *ResultActivity:* Εμφανίζει τα αποτελέσματα των διαδικασιών που πραγματοποιούνται, δείχνοντας αν οι λειτουργίες ήταν επιτυχείς ή όχι.

4.5.2.2 Fragments / Τμήματα

- *HomeFragment:* Το τμήμα της αρχικής οθόνης, που προσφέρει γρήγορη πρόσβαση στις κύριες λειτουργίες της εφαρμογής.
- *WelcomeFragment:* Μέρος της ακολουθίας καλωσορίσματος, αυτό το τμήμα εισάγει τους νέους χρήστες στα βασικά χαρακτηριστικά της εφαρμογής.
- *WelcomeFragment2:* Συνέχεια της ακολουθίας καλωσορίσματος, παρέχοντας πρόσθετες πληροφορίες ή βήματα ρύθμισης για τους νέους χρήστες.
- *MainPinFragment:* Το κύριο τμήμα για τη διαχείριση των δραστηριοτήτων που σχετίζονται με το PIN, ενσωματωμένο στη δραστηριότητα PIN.
- *AddPinFragment:* Διευκολύνει την προσθήκη ενός νέου PIN ασφαλείας για λογαριασμούς χρηστών.
- *EditPinFragment:* Επιτρέπει στους χρήστες να επεξεργάζονται το PIN ασφαλείας τους, βελτιώνοντας τις ρυθμίσεις ασφαλείας.
- *MainFaceRecognitionFragment:* Το κύριο τμήμα για τις εργασίες αναγνώρισης προσώπου, ενσωματωμένο στην κύρια δραστηριότητα για απρόσκοπτη λειτουργία.
- *AddFaceFragment:* Παρόμοιο με τη δραστηριότητα AddFaceActivity, αυτό το τμήμα επιτρέπει στους χρήστες να προσθέτουν νέα πρόσωπα στη βάση δεδομένων αναγνώρισης, αλλά χρησιμοποιείται σε διαφορετικό πλαίσιο.
- *RemoveFaceFragment:* Επιτρέπει στους χρήστες να αφαιρούν πρόσωπα που έχουν προστεθεί προηγουμένως από τη βάση δεδομένων αναγνώρισης.
- *ActivityLogsFragment:* Εμφανίζει τις καταγραφές όλων των δραστηριοτήτων, συμπεριλαμβανομένων των προσπαθειών αναγνώρισης προσώπου και των συμβάντων ανίχνευσης κίνησης, παρέχοντας στους χρήστες ένα ιστορικό όλων των λειτουργιών.

- *SettingsFragment:* Παρέχει πρόσβαση στις ρυθμίσεις της εφαρμογής, επιτρέποντας στους χρήστες να ρυθμίζουν τις παραμέτρους ασφαλείας.

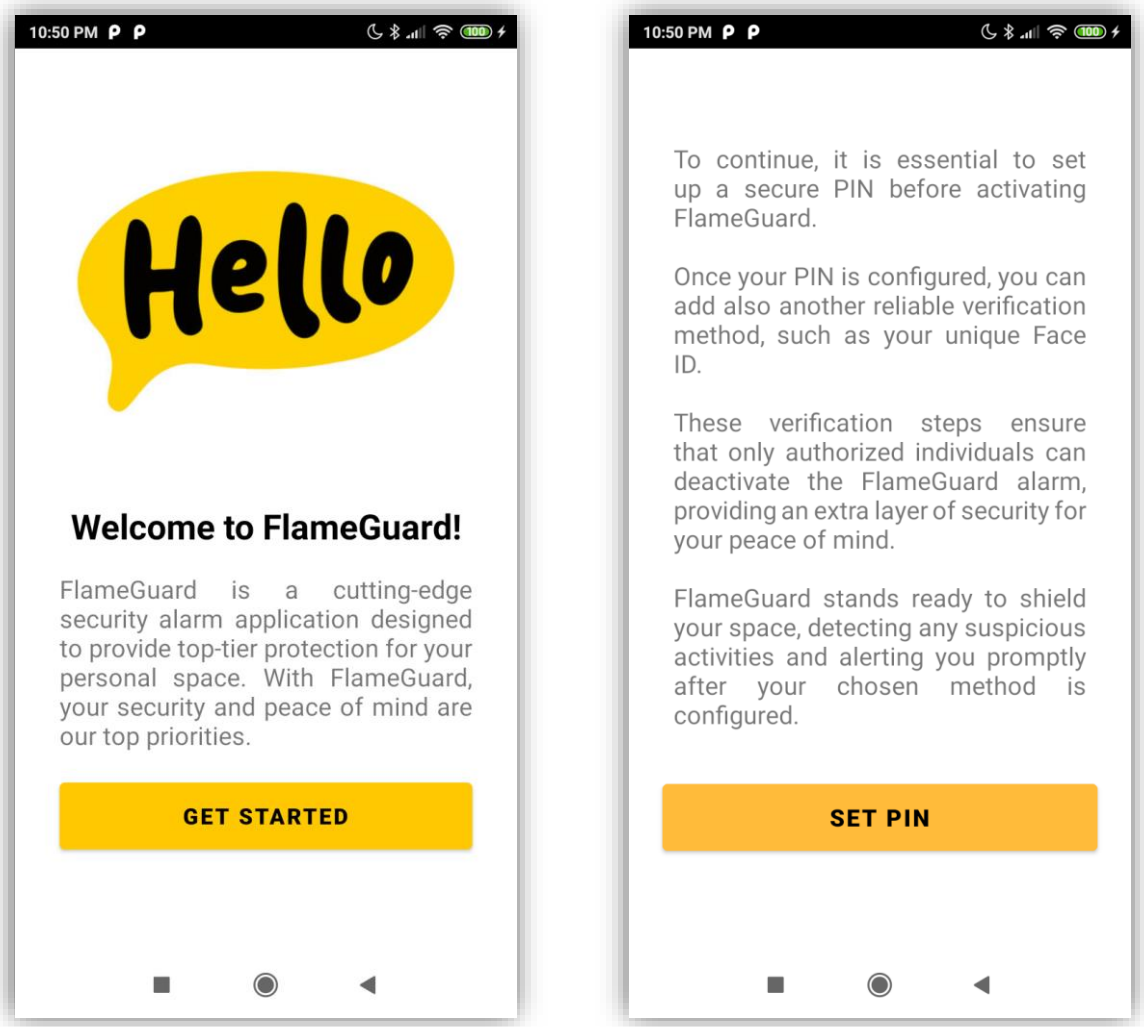
4.5.2.3 Στιγμιότυπα εφαρμογής



Εικόνα 42 – Σελίδα Σύνδεσης και Εγγραφής

Τα παραπάνω στιγμιότυπα δείχνουν δύο βασικές οθόνες της εφαρμογής για σύνδεση και εγγραγή χρήση. Η SignInActivity (αριστερά) είναι για τους υπάρχοντες χρήστες για να συνδεθούν με το email και τον κωδικό τους, με ένα εμφανές κουμπί *SIGN IN* και μια επιλογή για τη δημιουργία ενός νέου λογαριασμού. Αν ο χρήστης ήταν ήδη συνδεδεμένος στην τρέχουσα συσκευή, η εφαρμογή τον ανακατευθύνει αυτόματα

στην MainActivity κατά την εκκίνηση, χωρίς να εμφανίζεται η οθόνη σύνδεσης. Η SignUpActivity (δεξιά) επιτρέπει στους νέους χρήστες να εγγραφούν στην εφαρμογή εισάγοντας το email τους, τον κωδικό πρόσβασης και επιβεβαιώνοντας τον κωδικό πρόσβασης τους.

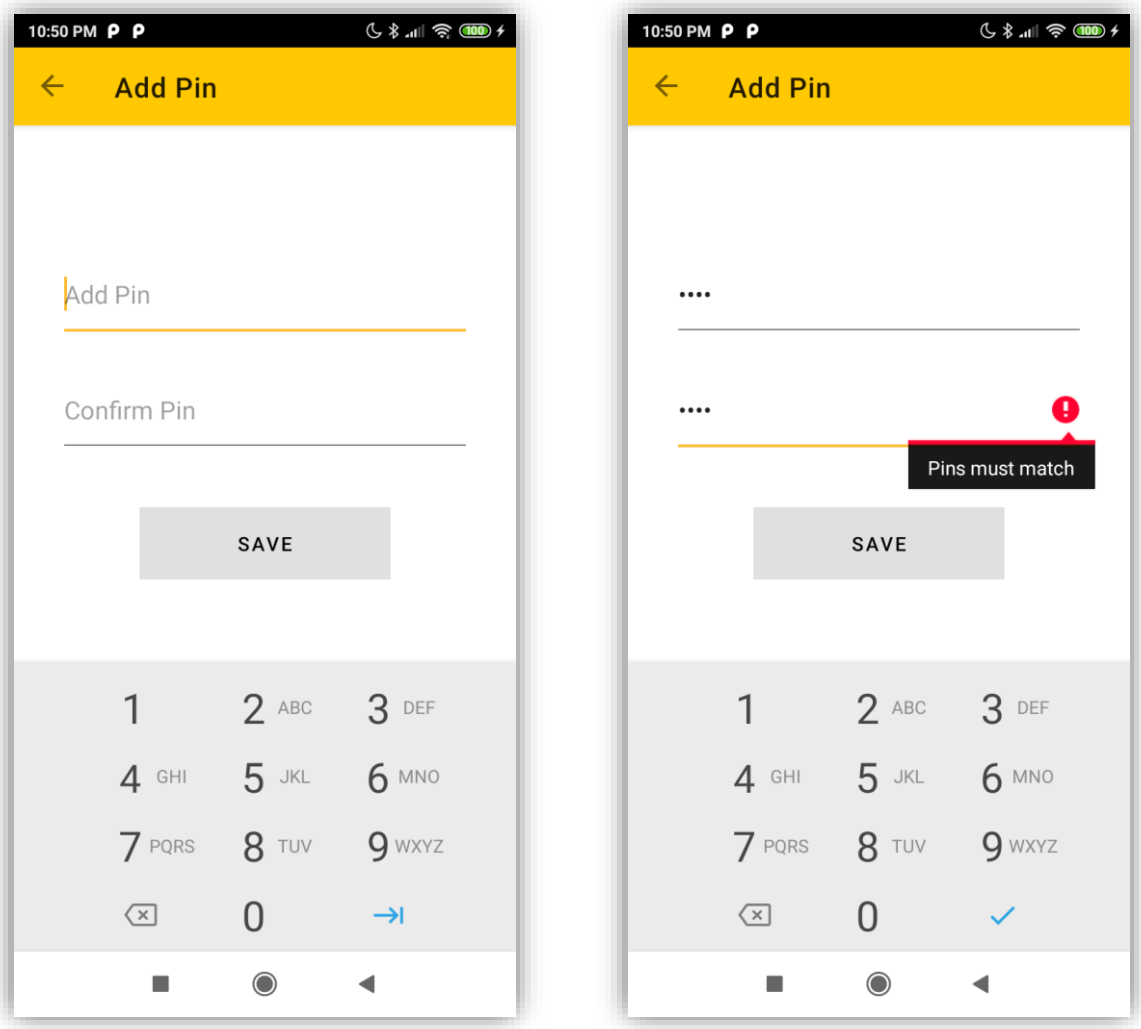


Εικόνα 43 - Καλωσόρισμα Νέων Χρηστών

Τα παραπάνω στιγμιότυπα εμφανίζουν τις οθόνες καλωσορίσματος της εφαρμογής Flame Guard για νέους χρήστες. Η πρώτη εικόνα αριστερά δείχνει ένα μήνυμα καλωσορίσματος με ένα γραφικό *Hello* και μια εισαγωγή στην εφαρμογή. Τονίζεται ότι η Flame Guard είναι μια εφαρμογή συναγερμού ασφαλείας που έχει σχεδιαστεί για να παρέχει κορυφαία προστασία για προσωπικούς χώρους δίνοντας έμφαση στην

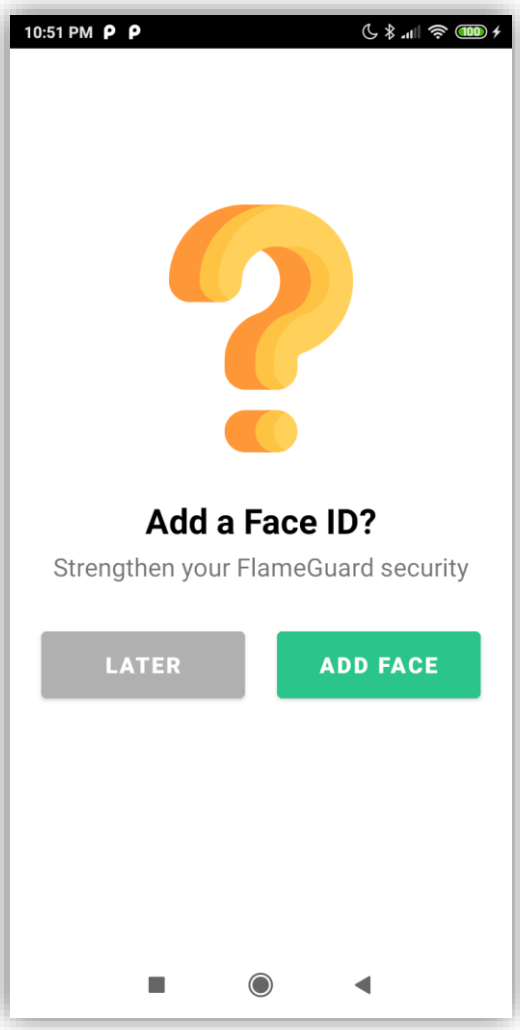
ασφάλεια. Η οθόνη περιλαμβάνει ένα εμφανές κουμπί *GET STARTED* για να συνεχίσει ο χρήστης παρακάτω.

Η δεύτερη εικόνα δεξιά περιγράφει το βασικό βήμα της δημιουργίας ενός ασφαλούς PIN πριν από την ενεργοποίηση της φύλαξης. Εξηγεί ότι οι χρήστες μπορούν να προσθέσουν μια άλλη μέθοδο επαλήθευσης προσώπου, διασφαλίζοντας ότι μόνο εξουσιοδοτημένα άτομα μπορούν να απενεργοποιήσουν τον συναγερμό, παρέχοντας ένα επιπλέον επίπεδο ασφάλειας. Η οθόνη διαβεβαιώνει τους χρήστες ότι η εφαρμογή θα προστατεύει το χώρο τους, θα ανιχνεύει ύποπτες δραστηριότητες και θα τους ειδοποιεί αμέσως. Ένα κουμπί *SET PIN* εμφανίζεται στο κάτω μέρος για εύκολη πρόσβαση του χρήστη για να δημιουργήσει ένα PIN ασφαλείας.



Εικόνα 44 - Δημιουργία PIN Ασφαλείας

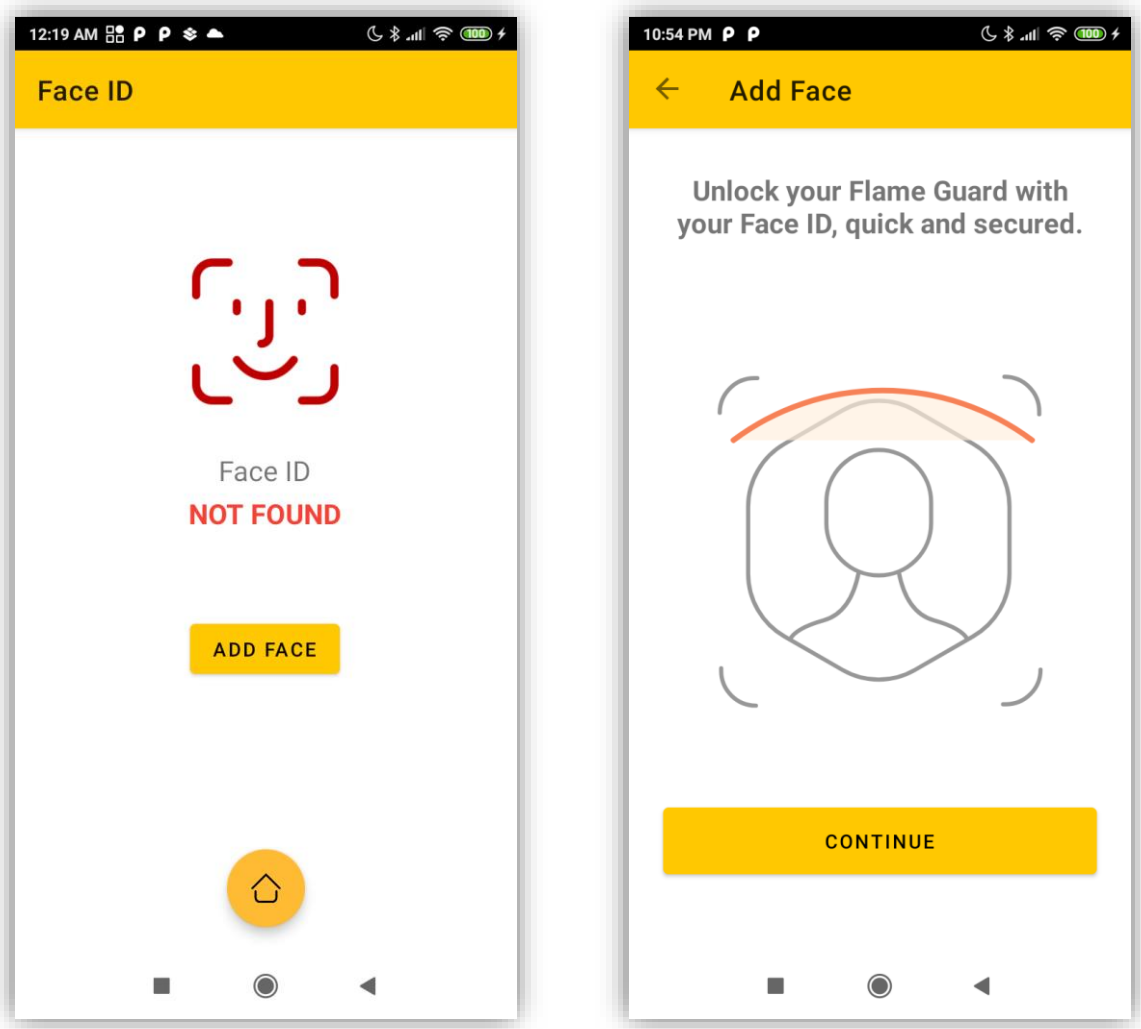
Οι παραπάνω εικόνες απεικονίζουν τη διαδικασία δημιουργίας PIN ασφαλείας στην εφαρμογή. Η πρώτη εικόνα αριστερά δείχνει το αρχικό βήμα όπου οι χρήστες καλούνται να προσθέσουν και να επιβεβαιώσουν το PIN τους. Η διεπαφή είναι απλή, με πεδία εισαγωγής για το PIN και ένα κουμπί *SAVE* για να προχωρήσουν. Η δεύτερη εικόνα δεξιά παρουσιάζει τη διαδικασία επαλήθευσης του PIN σε πραγματικό χρόνο. Εάν τα PIN που έχουν εισαχθεί δεν ταιριάζουν, ο χρήστης ενημερώνεται αμέσως με το ειδικό μήνυμα, το οποίο εμφανίζεται με κόκκινο χρώμα κάτω από το πεδίο επιβεβαίωσης.



Εικόνα 45 - Ερώτηση για Προσθήκη Μεθόδου Επαλήθευσης μέσω Προσώπου

Η *Εικόνα 45* δείχνει μια οθόνη από την εφαρμογή, η οποία ρωτάει τον χρήστη αν θέλει να προσθέσει ένα Face ID αφού ρυθμίσει το PIN του. Η οθόνη αυτή αποτελεί μέρος της διαδικασίας εισόδου των νέων χρηστών με στόχο την ενίσχυση της ασφάλειας.

Η οθόνη διαθέτει ένα εικονίδιο με ερωτηματικό στην κορυφή, ακολουθούμενο από την ερώτηση *«Add a Face ID?»* και το υποκείμενο *«Strengthen your FlameGuard security» (Ενισχύστε την ασφάλειά σας με τη FlameGuard)*. Στους χρήστες δίνονται δύο επιλογές, *LATER* που τους επιτρέπει να παραλείψουν αυτό το βήμα και να προσθέσουν το Face ID αργότερα, και *ADD FACE* που ξεκινά τη διαδικασία για την άμεση ρύθμιση του Face ID.

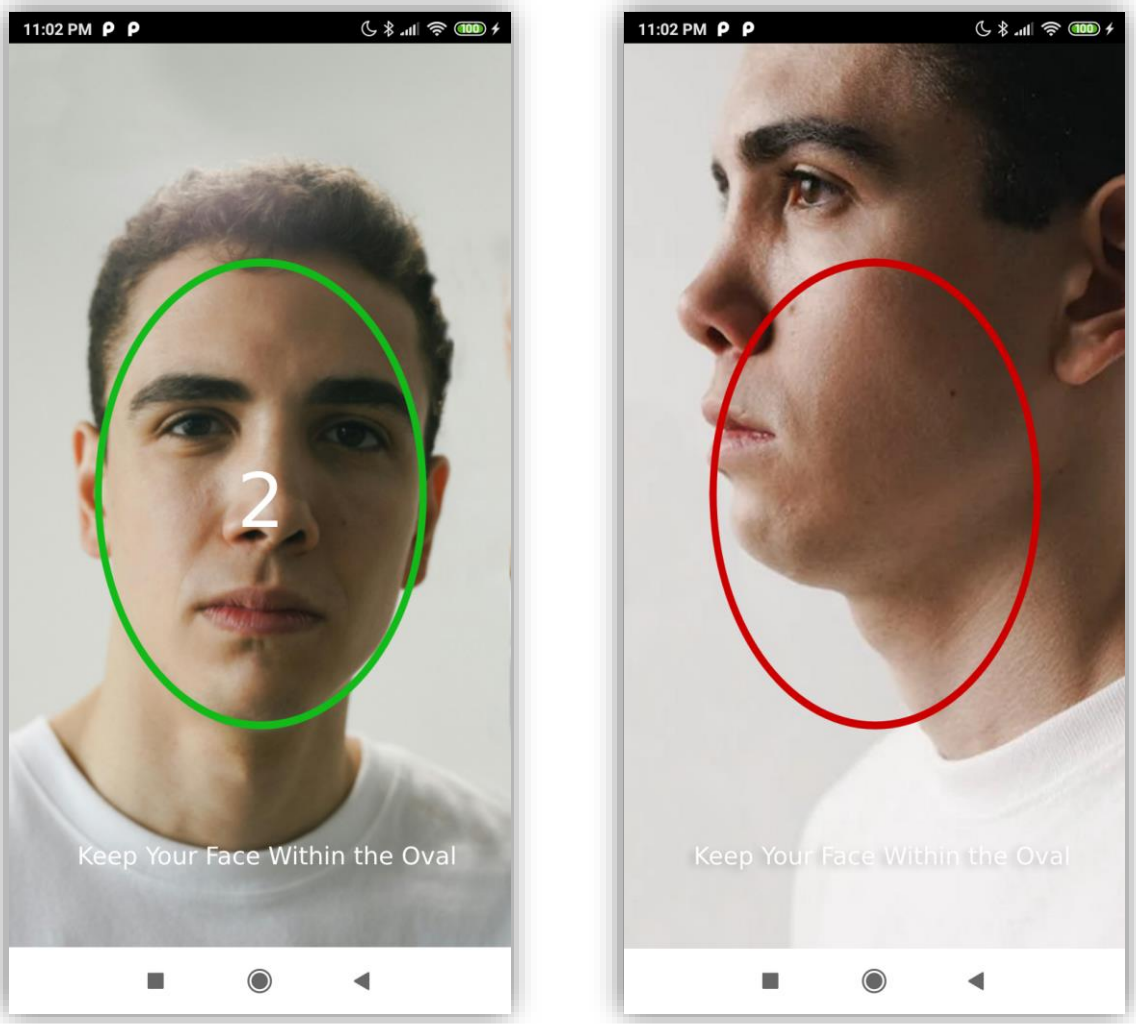


Εικόνα 46 - Διαχείριση Προσθήκης Προσώπου και Οδηγίες

Συνεχίζοντας με την προσθήκη προσώπου, η εφαρμογή συνεχίζει με την οθόνη διαχείρισης του Face ID εντός της εφαρμογής.

Στην πρώτη οθόνη αριστερά εμφανίζεται το μήνυμα *ότι δεν βρέθηκε αποθηκευμένο πρόσωπο επαλήθευσης,* το οποίο υποδεικνύει ότι ο χρήστης δεν έχει ακόμη ρυθμίσει το Face ID. Διαθέτει ένα κόκκινο εικονίδιο προσώπου και παρέχει ένα κουμπί *ADD FACE*, προτρέποντας τον χρήστη να προχωρήσει στη προσθήκη προσώπου.

Η δεύτερη οθόνη δεξιά είναι η διεπαφή προσθήκης προσώπου. Παρέχει οδηγίες στον χρήστη και περιλαμβάνει μια απεικόνιση ενός προσώπου που σαρώνεται και ένα κουμπί *CONTINUE*, καθοδηγώντας τον χρήστη στη διαδικασία προσθήκης προσώπου επαλήθευσης.

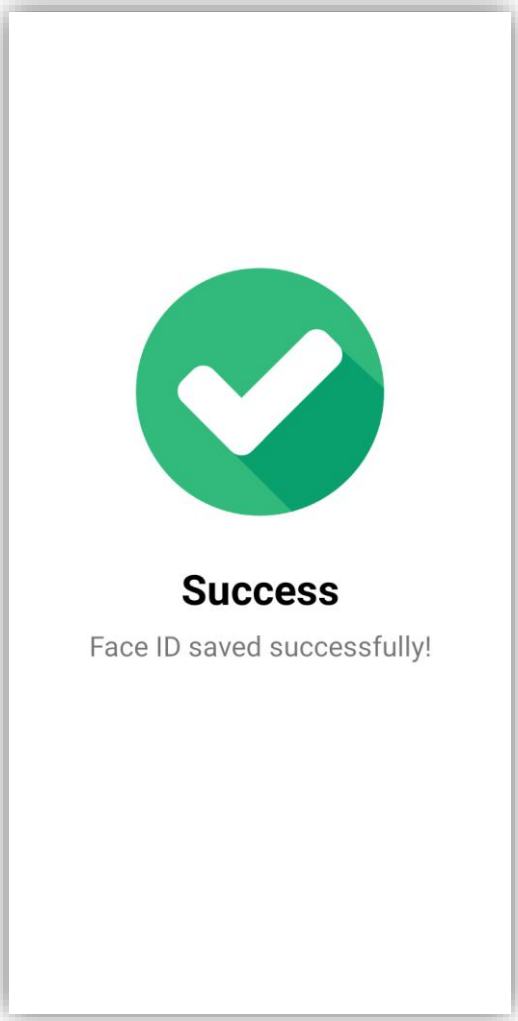


Εικόνα 47 - Προσθήκη Μεθόδου Επαλήθευσης μέσω Προσώπου

Οι παραπάνω εικόνες απεικονίζουν τη διαδικασία προσθήκης της αναγνώρισης προσώπου στην εφαρμογή.

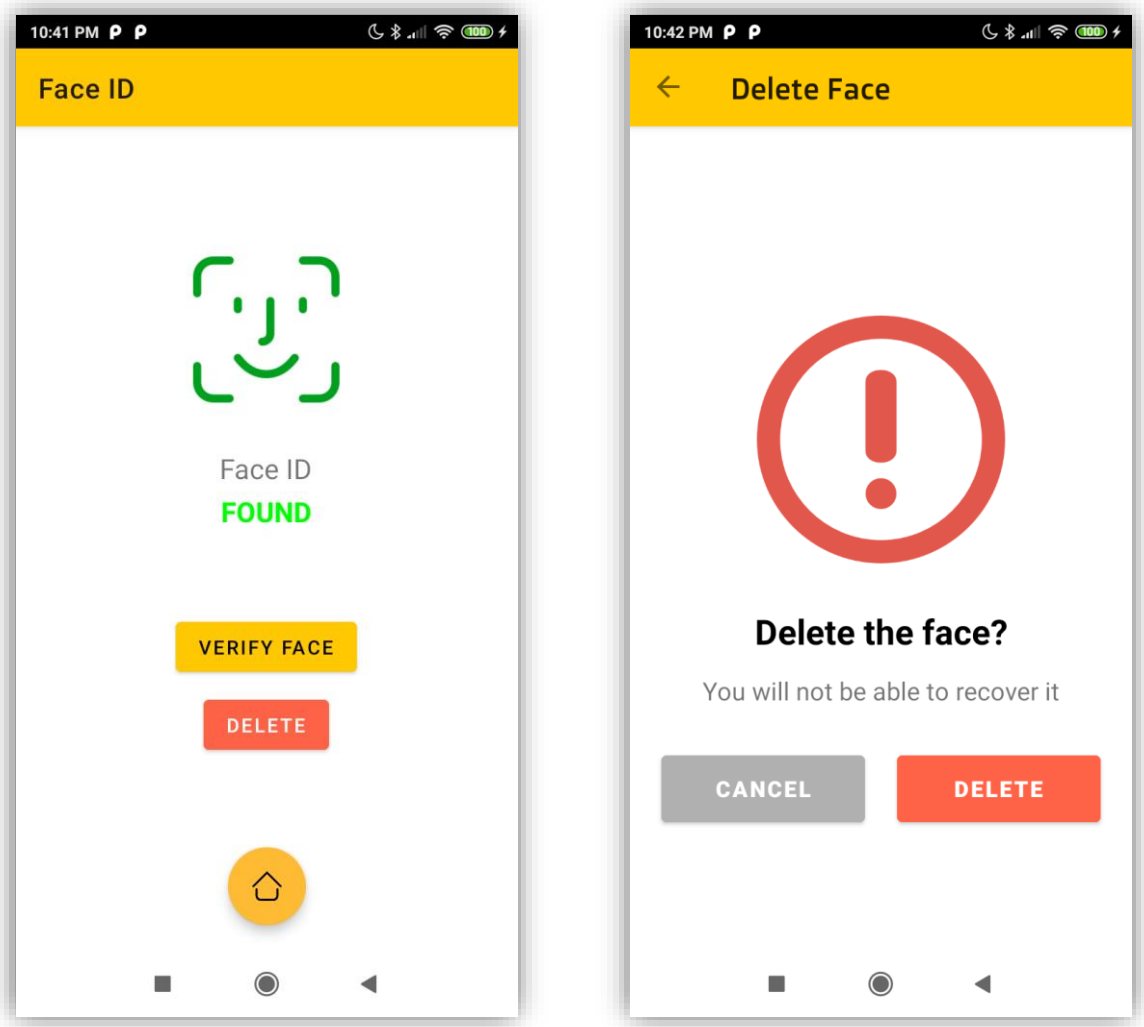
Η αριστερή εικόνα δείχνει ένα επιτυχημένο σενάριο αναγνώρισης προσώπου, όπου το πρόσωπο του χρήστη είναι σωστά τοποθετημένο μέσα στο οβάλ. Σε αυτή την περίπτωση, ο χρήστης πρέπει να διατηρήσει το πρόσωπό του μέσα στο οβάλ για 3 δευτερόλεπτα για να ολοκληρωθεί η διαδικασία αναγνώρισης και ανάλυσης του προσώπου. Αν ο χρήστης απομακρυνθεί από το οβάλ πριν ολοκληρωθεί η αντίστροφη μέτρηση, η διαδικασία θα διακοπεί και θα ξεκινήσει εκ νέου.

Η δεξιά εικόνα δείχνει μια λανθασμένη τοποθέτηση του προσώπου, που υποδεικνύεται από το κόκκινο οβάλ. Το οβάλ βοηθά τον χρήστη να κατευθύνει σωστά το πρόσωπό του για την επιτυχή αποθήκευση.



Εικόνα 48 - Επιτυχής Προσθήκη Μεθόδου Αναγνώρισης Προσώπου

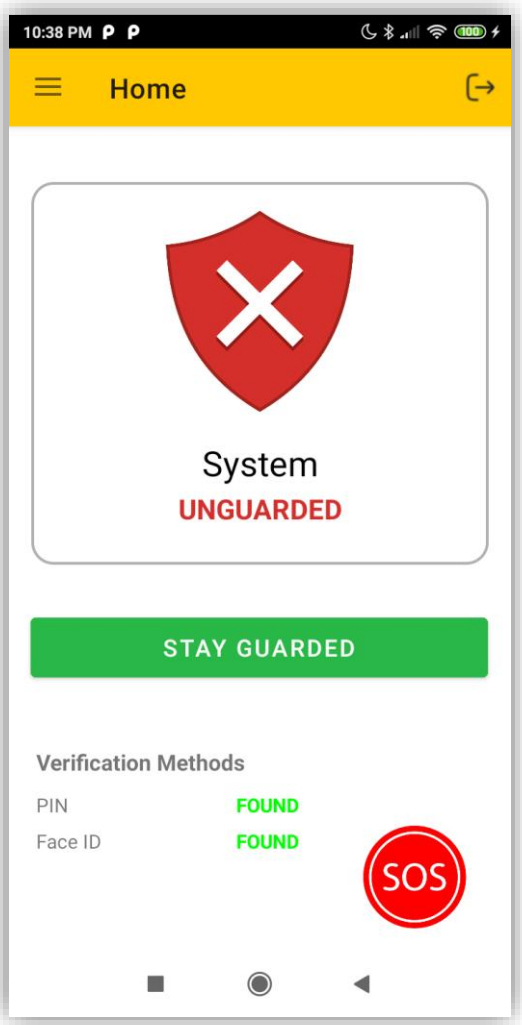
Η παραπάνω εικόνα παρουσιάζει την οθόνη επιβεβαίωσης της επιτυχίας εντός της εφαρμογής. Η συγκεκριμένη οθόνη εμφανίζεται αφού ο χρήστης έχει προσθέσει επιτυχώς την μέθοδο αναγνώρισης προσώπου. Διαθέτει ένα πράσινο εικονίδιο με σημάδι ελέγχου, που συμβολίζει την επιτυχία, και ένα μήνυμα που αναφέρει ότι το πρόσωπο του χρήστη προστέθηκε με επιτυχία. Αυτή η οθόνη παρέχεται μέσω της κλήσης του ResultActivity, διασφαλίζοντας ότι οι χρήστες λαμβάνουν άμεση και σαφή ενημέρωση σχετικά με το αποτέλεσμα της διαδικασίας που εκτελούν.



Εικόνα 49 - Μενού Διαχείρισης του Face ID και Περίπτωση Διαγραφής

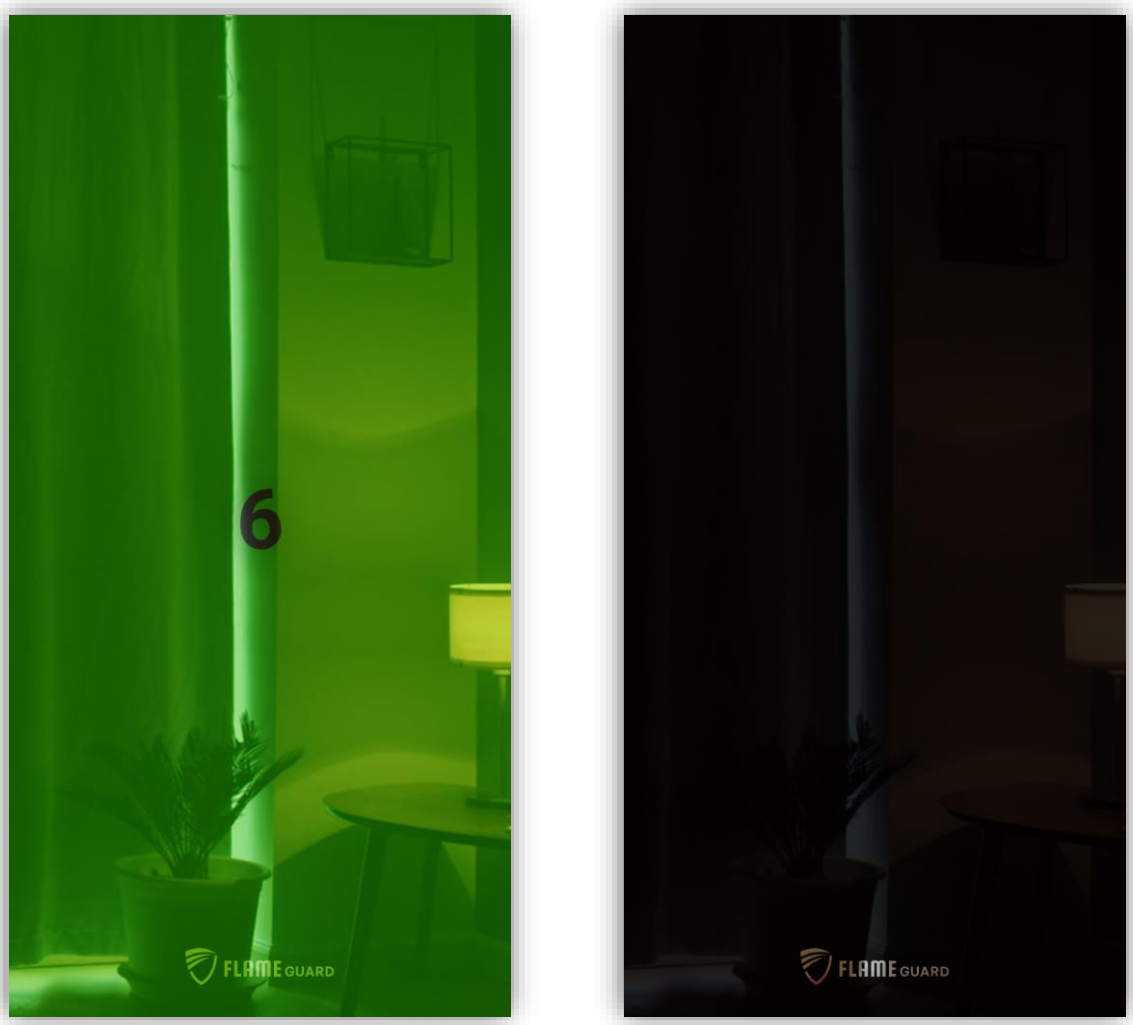
Μετά την προσθήκη του προσώπου, ο χρήστης μπορεί να έχει πρόσβαση στις ρυθμίσεις προσώπου μέσω του μενού διαχείρισης προσώπου. Αυτό το μενού επιτρέπει στον χρήστη είτε να επαληθεύσει το πρόσωπο του είτε να το διαγράψει για να προσθέσει ένα διαφορετικό πρόσωπο. Εάν ο χρήστης επιλέξει να διαγράψει το πρόσωπο, θα του ζητηθεί να επιβεβαιώσει τη διαγραφή, διασφαλίζοντας ότι γνωρίζει ότι αυτή η ενέργεια είναι μη αντιστρέψιμη.

Τα βήματα για την επαλήθευση προσώπου θα παρουσιαστούν στα κεφάλαια που ακολουθούν, καθώς η μέθοδος επαλήθευσης προσώπου χειρίζεται στο πλαίσιο της ίδιας δραστηριότητας που χρησιμοποιείται για την αναγνώριση προσώπου για την απενεργοποίηση της φύλαξης.



Εικόνα 50 - Αρχική Οθόνη της Εφαρμογής

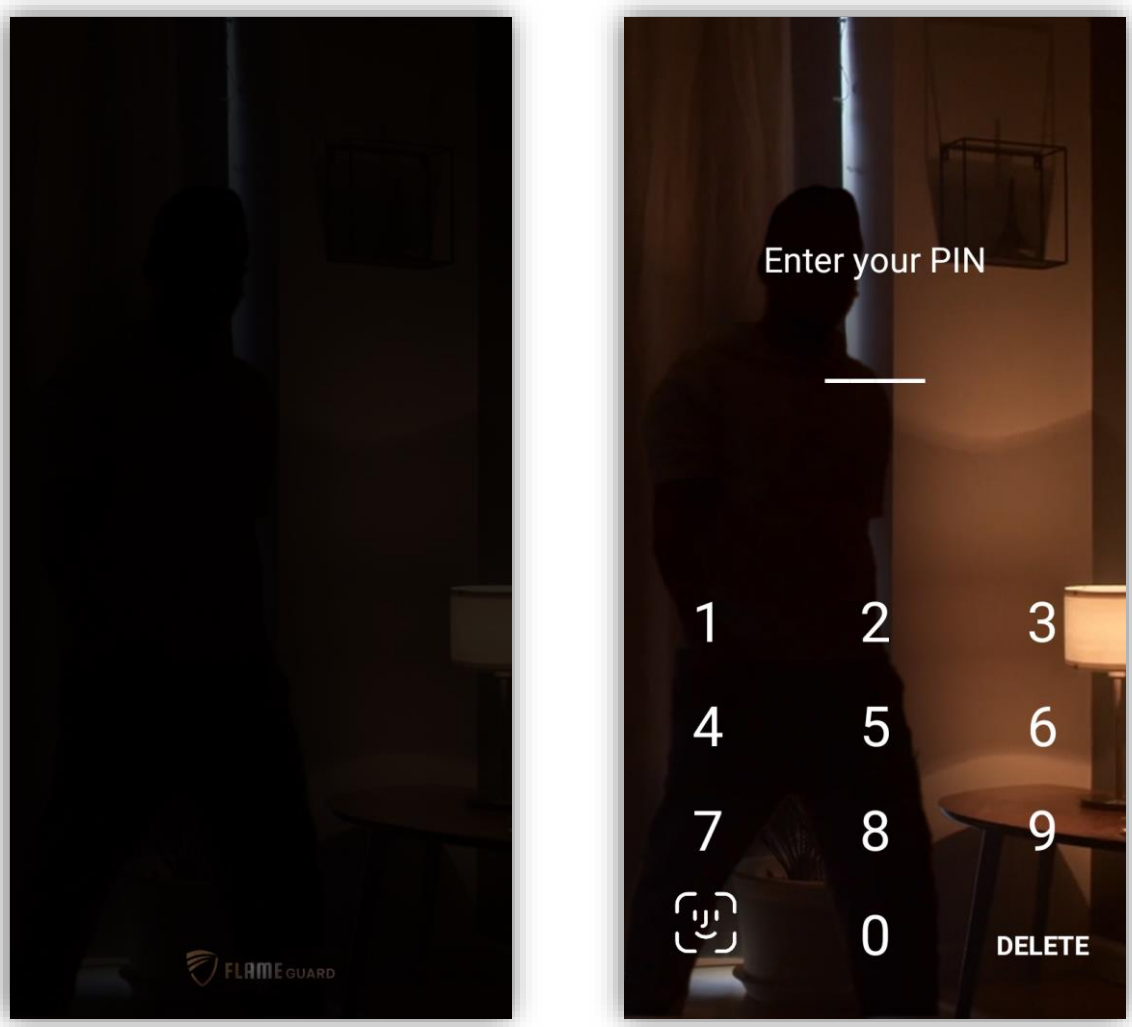
Η παραπάνω εικόνα εμφανίζει την αρχική οθόνη, δείχνοντας μια κόκκινη ασπίδα με Χ και επισημαίνοντας ότι το σύστημα είναι αφύλακτο. Οι χρήστες μπορούν να ενεργοποιήσουν το σύστημα φύλαξης πατώντας το πράσινο κουμπί *STAY GUARDED*. Κάτω από αυτό το κουμπί, η οθόνη εμφανίζει την κατάσταση των μεθόδων επαλήθευσης, υποδεικνύοντας ότι τόσο το PIN ασφαλαείας όσο και το Face ID έχουν βρεθεί και ρυθμιστεί για περιπτώσεις επαλήθευσης. Επιπλέον, υπάρχει και ένα κουμπί SOS για περιπτώσεις έκτακτης ανάγκης το οποίο βοηθάει την ενεργοποίηση του συναγερμού χειροκίνητα.



Εικόνα 51 - Ενεργοποίηση Φύλαξης

Όταν ο χρήστης επιλέξει *STAY GUARDED* στην αρχική οθόνη, ενεργοποιείται η φύλαξη και στην οθόνη μαζί με την προβολή της κάμερας ξεκινάει μια αντίστροφη μέτρηση. Αυτός ο χρονομετρητής, έχει προκαθοριστεί από τον χρήστη στις ρυθμίσεις και επιτρέπει στον χρήστη να απομακρυνθεί από τον χώρο πριν ενεργοποιηθεί η ανίχνευση κίνησης. Η δεξιά εικόνα απεικονίζει το σύστημα μετά τη λήξη της αντίστροφης μέτρησης και την ενεργοποίηση της ανίχνευσης κίνησης.

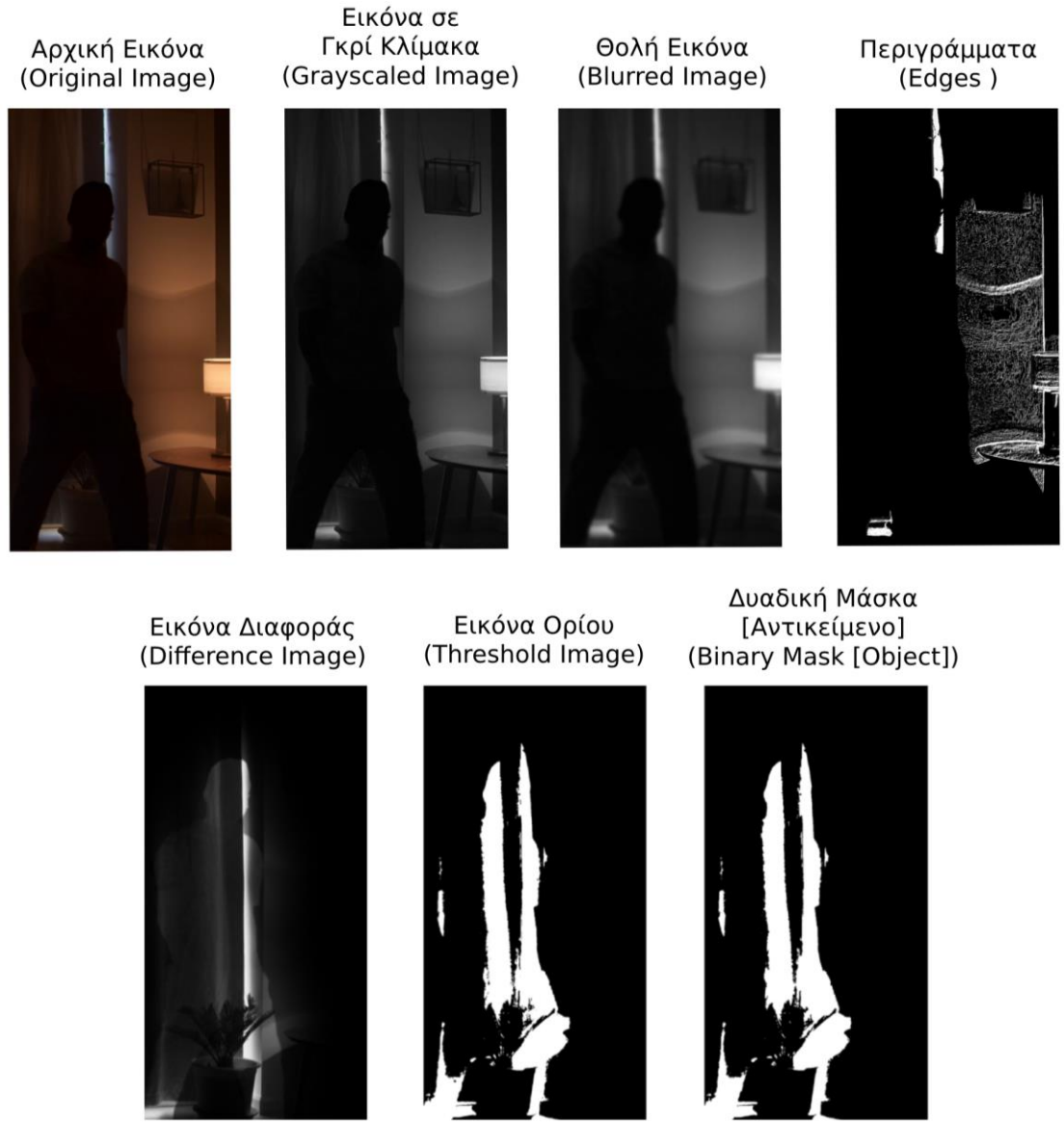
Για τη συντήρηση της χρήσης της μπαταρίας, η διαφάνεια της προβολής της κάμερας ρυθμίζεται χαμηλά κατά τη διάρκεια αυτής της περιόδου. Αυτή η λειτουργία διασφαλίζει ότι το σύστημα παραμένει αποδοτικό ως προς την κατανάλωση ενέργειας, ενώ παράλληλα παρέχει και τις απαραίτητες λειτουργίες ασφαλείας.



Εικόνα 52 - Ανίχνευση Κίνησης στη Φύλαξη

Όταν η φύλαξη είναι ενεργοποιημένη και ανιχνευθεί κίνηση, η διαφάνεια της προβολής κάμερας επιστρέφει στο προεπιλεγμένο επίπεδό της. Μόλις ανιχνευθεί κίνηση, εμφανίζεται το PinPad για την εισαγώγη PIN ασφαλείας μαζί με την εναλλακτική επιλογή επαλήθευσης μέσω αναγνώριση προσώπου.

Με την ανίχνευση κίνησης, ξεκινά επίσης μια αντίστροφη μέτρηση στο backend, η οποία κατά τη διάρκεια αυτής της περίπτωσης, το σύστημα πρέπει να επαληθευτεί είτε με το σωστό PIN ασφαλείας είτε μέσω αναγνώρισης προσώπου. Επιπλέον, ο χρήστης ειδοποιείται μέσω SMS για την ανιχνευμένη κίνηση, παρέχοντας άμεση ειδοποίηση και ενισχύοντας την αντίδραση ασφαλείας. Για την περαιτέρω ενίσχυση της ασφάλειας και την αποτροπή μη εξουσιοδοτημένων ενεργειών, η κάτω γραμμή πλοήγησης απενεργοποιείται, ώστε να αποφευχθεί το κλείσιμο της εφαρμογής σε περιπτώσεις έκτακτης ανάγκης.



Εικόνα 53 - Βήματα της Διαδικασίας Ανίχνευσης Κίνησης με Παράδειγμα

Η *Εικόνα 53* απεικονίζει τα βήματα που πραγματοποιούνται στη διαδικασία ανίχνευσης κίνησης στην συγκεκριμένη περίπτωση.

Η διαδικασία ανίχνευσης κίνησης ξεκινά με τη λήψη μιας αρχικής εικόνας όταν βρεθεί διαφορά πάνω από τον όριο με την προηγούμενη λήψη. Το σύστημα καταγράφει συνεχώς εικόνες και τις επεξεργάζεται μέσω των βημάτων που περιγράφονται παραπάνω. Όταν ανιχνεύεται μια σημαντική αλλαγή μεταξύ των εικόνων, η οποία υποδεικνύεται από την εικόνα διαφοράς και τη δυαδική μάσκα, το σύστημα αναγνωρίζει ότι έχει ανιχνευθεί κίνηση.

Αρχική Εικόνα (Original Image)

Αρχική λήψη από την κάμερα που δείχνει τη σκηνή με ένα άτομο να βρίσκεται στον χώρο φύλαξης. Χρησιμεύει ως βάση για την ανίχνευση αλλαγών στο περιβάλλον.

*Εικόνα σε Γκρί Κλίμακα (*Grayscaled Image*)*

Η εικόνα μετατρέπεται σε κλίμακα του γκρι για την απλοποίηση των δεδομένων και τη μείωση της υπολογιστικής πολυπλοκότητας, εστιάζοντας στην ένταση του φωτός για την ανάδειξη των αντιθέσεων.

Θολή Εικόνα (Blurred Image):

Εφαρμόζεται θόλωση για την μείωση των λεπτομερειών και του θορύβου, βοηθώντας στην εστίαση σε σημαντικές αλλαγές που υποδηλώνουν κίνηση.

Περιγράμματα (Edges):

Η ανίχνευση περιγραμμάτων προσδιορίζει τα όρια των αντικειμένων, δίνοντας έμφαση στις περιγραφές και τα περιεχόμενα για τον εντοπισμό σημαντικών αλλαγών μεταξύ των εικόνων.

Εικόνα Διαφοράς (Difference Image):

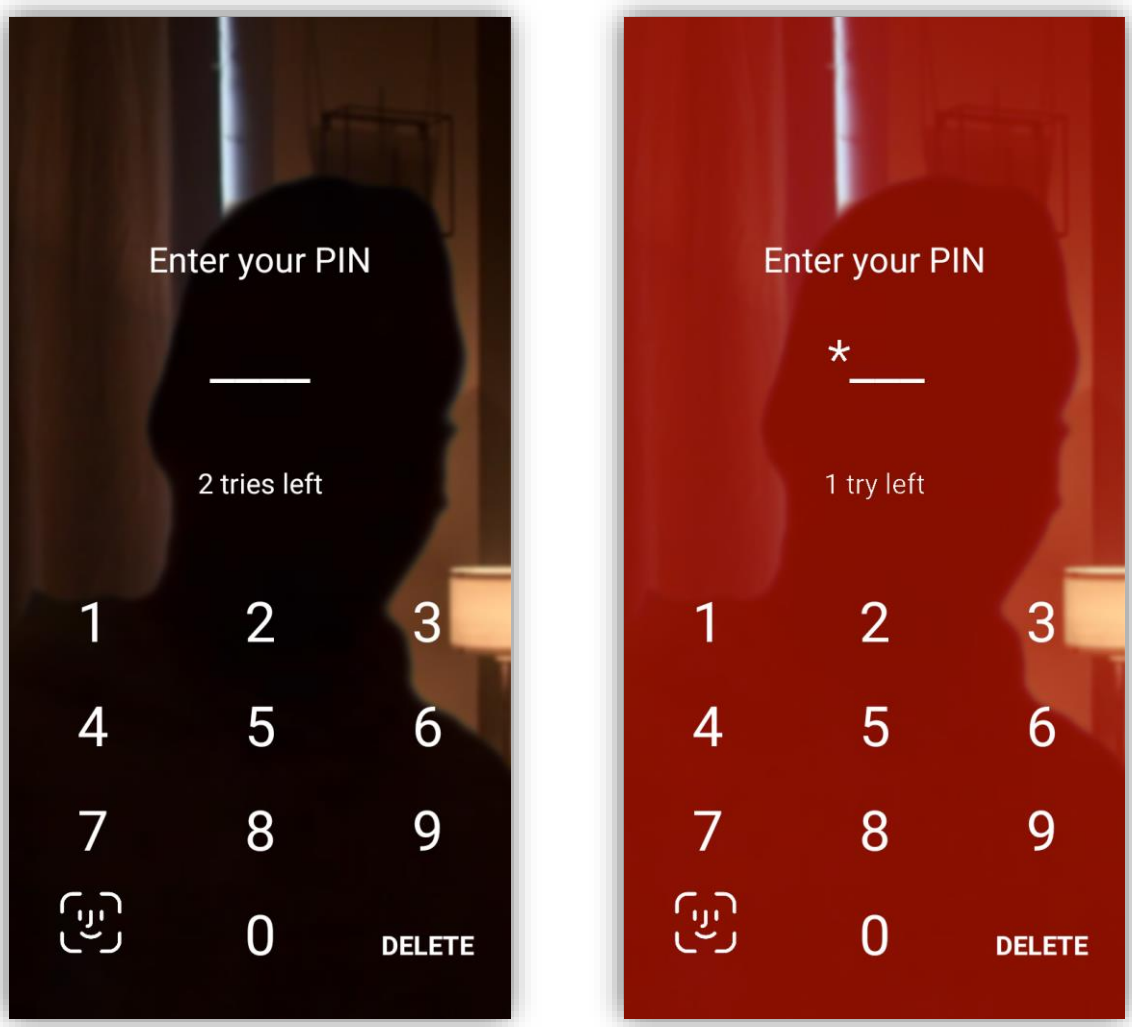
Υπολογίζεται με την εύρεση της απόλυτης διαφοράς μεταξύ του τρέχουσας εικόνας σε κλίμακα του γκρι και μιας εικόνας αναφοράς, αναδεικνύοντας τις περιοχές όπου έχουν σημειωθεί αλλαγές.

Εικόνα Ορίου (Threshold Image):

Ένα δυαδικό όριο εφαρμόζεται στην εικόνα διαφοράς, δημιουργώντας έναν χάρτη όπου οι σημαντικές αλλαγές επισημαίνονται με λευκό χρώμα, διαχωρίζοντας τα κινούμενα αντικείμενα από το φόντο.

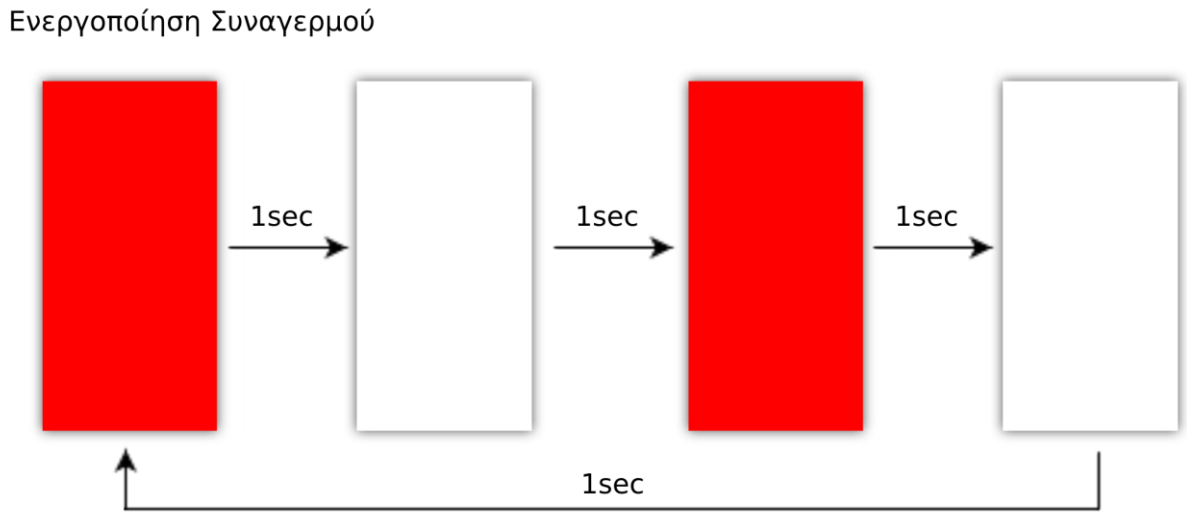
Δυαδική Μάσκα [Αντικείμενο] (Binary Mask [Object]):

Η τελική δυαδική μάσκα απομονώνει το κινούμενο αντικείμενο, αναπαριστώντας το με λευκό χρώμα σε μαύρο φόντο, που χρησιμοποιείται για την παρακολούθηση της κίνησης



Εικόνα 54 - Εισαγωγή PIN Ασφαλείας

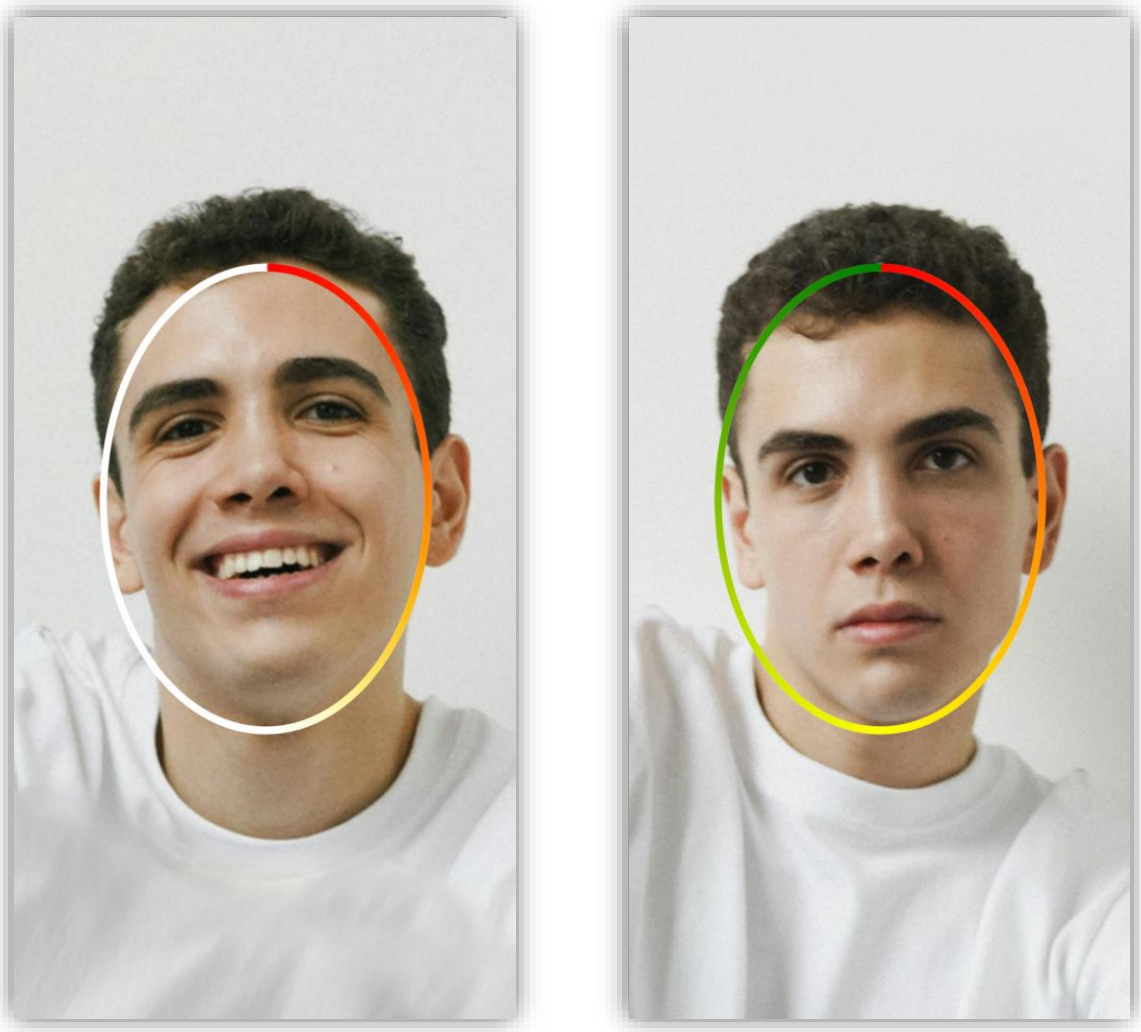
Για την απενεργοποίηση της φύλαξης, ο χρήστης πρέπει να πληκτρολογήσει σωστά το PIN ασφαλείας εντός του προκαθορισμένου χρόνου και εντός τριών προσπαθειών, όπως φαίνεται στις παραπάνω εικόνες. Όταν εισάγεται ένα ψηφίο, αυτό εμφανίζεται ως αστερίσκος (*) στην οθόνη για λόγους ασφαλείας. Όταν το PIN ταιριάζει με το PIN του χρήστη, η φύλαξη απενεργοποιείται αυτόματα. Εάν το σωστό PIN δεν εισαχθεί εντός τριών προσπαθειών ή πριν από τη λήξη του προκαθορισμένου χρόνου, η οθόνη γίνεται κόκκινη και ενεργοποιείται ο συναγερμός. Επιπλέον, στέλνεται SMS στον χρήστη στην κύρια του συσκευή, το οποίο τον ενημερώνει για την ενεργοποίηση του συναγερμού. Η λεπτομερής ροή της διαδικασίας ενεργοποίησης του συναγερμού περιγράφεται στην *Εικόνα 55*.



Εικόνα 55 - Λογική Ροή Οπτικής Αναπαράστασης του Συναγερμού

Με την ενεργοποίηση του συναγερμού, η οθόνη ξεκινά μια επανάληψη που εναλλάσσεται μεταξύ κόκκινου και λευκού χρώματος, όπως φαίνεται στην *Εικόνα 55*. Κάθε χρώμα εμφανίζεται για 1 δευτερόλεπτο, δημιουργώντας μια οπτική ροή που μοιάζει με τα φώτα που αναβοσβήνουν στις σειρήνες έκτακτης ανάγκης. Ταυτόχρονα, ένας δυνατός ήχος σειρήνας αναπαράγεται στο περιβάλλον, παρέχοντας ένα ακουστικό σήμα που συμπληρώνει τον οπτικό συναγερμό. Αυτός ο συνδυασμός ηχητικών και οπτικών ειδοποιήσεων έχει σχεδιαστεί για να τραβήξει την άμεση προσοχή στην κατάσταση έκτακτης ανάγκης και συνεχίζεται για 15 λεπτά, ώστε να διασφαλιστεί ότι ο συναγερμός γίνεται αντιληπτός και κοινοποιείται αποτελεσματικά σε όποιον βρίσκεται κοντά.

Κατά τη διάρκεια αυτής της περιόδου, η κάτω γραμμή πλοήγησης παραμένει απενεργοποιημένη για να αποτρέψει τυχόν προσπάθειες κλεισίματος της εφαρμογής ή παράκαμψης του συναγερμού. Αυτή η λειτουργία είναι σημαντική για τη διατήρηση της αξιοπιστίας του συστήματος ασφαλείας, καθώς διασφαλίζει ότι ο συναγερμός δεν μπορεί εύκολα να αγνοηθεί. Ο συνεχιζόμενος οπτικοακουστικός συναγερμός, σε συνδυασμό με την απενεργοποιημένη πλοήγηση, παρέχει μια ισχυρή λύση σε ενδεχόμενες απειλές για την ασφάλεια, διασφαλίζοντας ότι ο χρήστης και οι άλλοι που βρίσκονται στην περιοχή γνωρίζουν την κατάσταση έκτακτης ανάγκης και μπορούν να λάβουν τα κατάλληλα μέτρα.

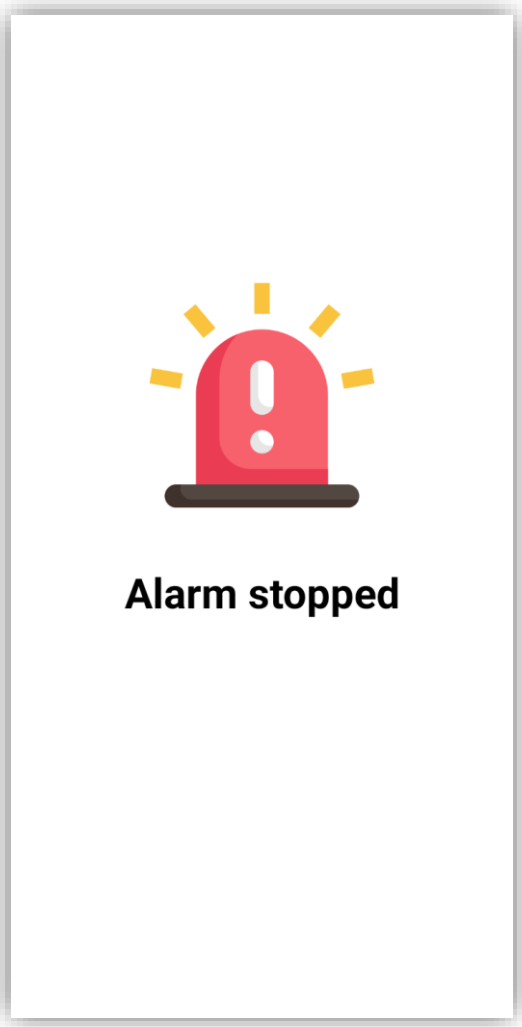


Εικόνα 56 - Απενεργοποίηση της Φύλαξης μέσω Αναγνώριση Προσώπου

Στην κατάσταση ανίχνευσης κίνησης, αν ο χρήστης επιλέξει το εικονίδιο Face ID που βρίσκεται στην κάτω αριστερή γωνία του PinPad, το σύστημα θα αρχίσει να αναλύει τις τρέχουσες εικόνες της προβολής για την ανίχνευση προσώπου. Αυτή η διαδικασία περιλαμβάνει τη σύγκριση των εικόνων από την προβολή της κάμερα σε απευθείας σύνδεση με τα αποθηκευμένα δεδομένα προσώπου για την αναγνώριση των εξουσιοδοτημένων χρηστών.

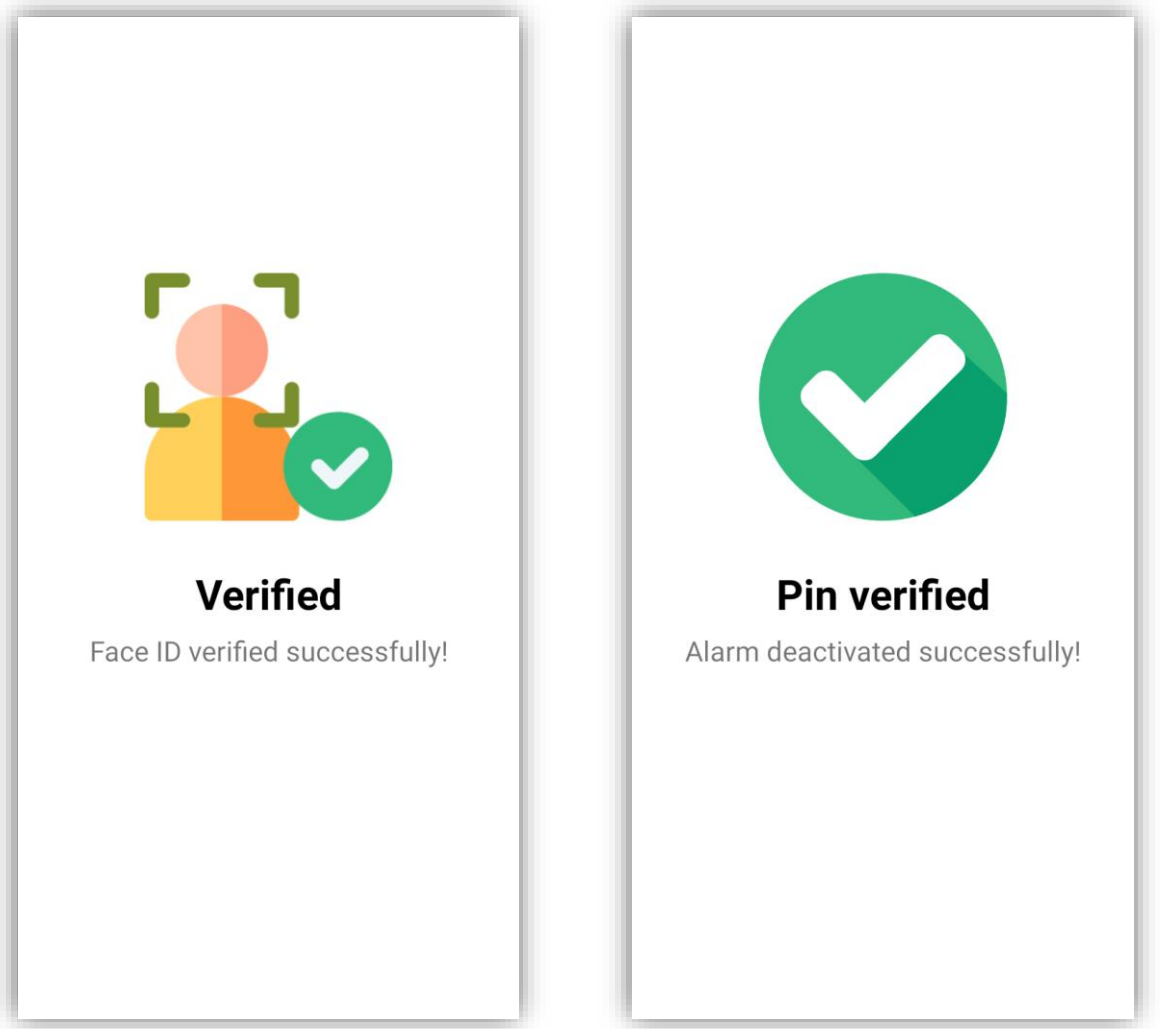
Για την επιτυχή αναγνώριση, ο χρήστης πρέπει να διατηρεί το πρόσωπο του εντός του οβάλ που εμφανίζεται στην οθόνη. Καθώς το σύστημα αναλύει το πρόσωπο, το οβάλ αλλάζει χρώμα από κόκκινο σε πράσινο, υποδεικνύοντας την πρόοδο και την ευθυγράμμιση. Η μετάβαση από το κόκκινο στο πράσινο γίνεται ομαλά, καθοδηγώντας τον χρήστη να τοποθετήσει σωστά το πρόσωπό του για ακριβή αναγνώριση.

Η διαδικασία ανάλυσης των εικόνων για την αναγνώριση προσώπου περιλαμβάνει διάφορα βήματα, όπως περιγράφεται στα παρεχόμενα διαγράμματα ροής στην *Εικόνα 37* και *Εικόνα 39*. Αρχικά, το σύστημα καλεί για αναγνώριση προσώπου και ενσωματώνεται με την Firebase για έλεγχο ταυτότητας και αποθήκευσης. Η κάμερα ενεργοποιείται και η ανάλυση της εικόνας αρχίζει σχεδόν αμέσως. Οι εικόνες που καταγράφονται από την κάμερα υποβάλλονται σε επεξεργασία για την ανίχνευση προσώπων με τη χρήση του FaceNetModel. Αν εντοπιστεί πρόσωπο, αυτό συγκρίνεται με τα αποθηκευμένα δεδομένα προσώπων. Αν το πρόσωπο αναγνωριστεί με επιτυχία, η φύλαξη απενεργοποιείται. Αν όχι, και η διαδικασία υπερβεί το χρονικό όριο, η εφαρμογή θα προχωρήσει στην ενεργοποίηση του συναγερμού με τον ίδιο τρόπο που περιγράφεται στην *Εικόνα 55*, ο οποίος περιλαμβάνει τις οπτικές και ακουστικές ειδοποιήσεις για να σηματοδοτήσει την κατάσταση έκτακτης ανάγκης.



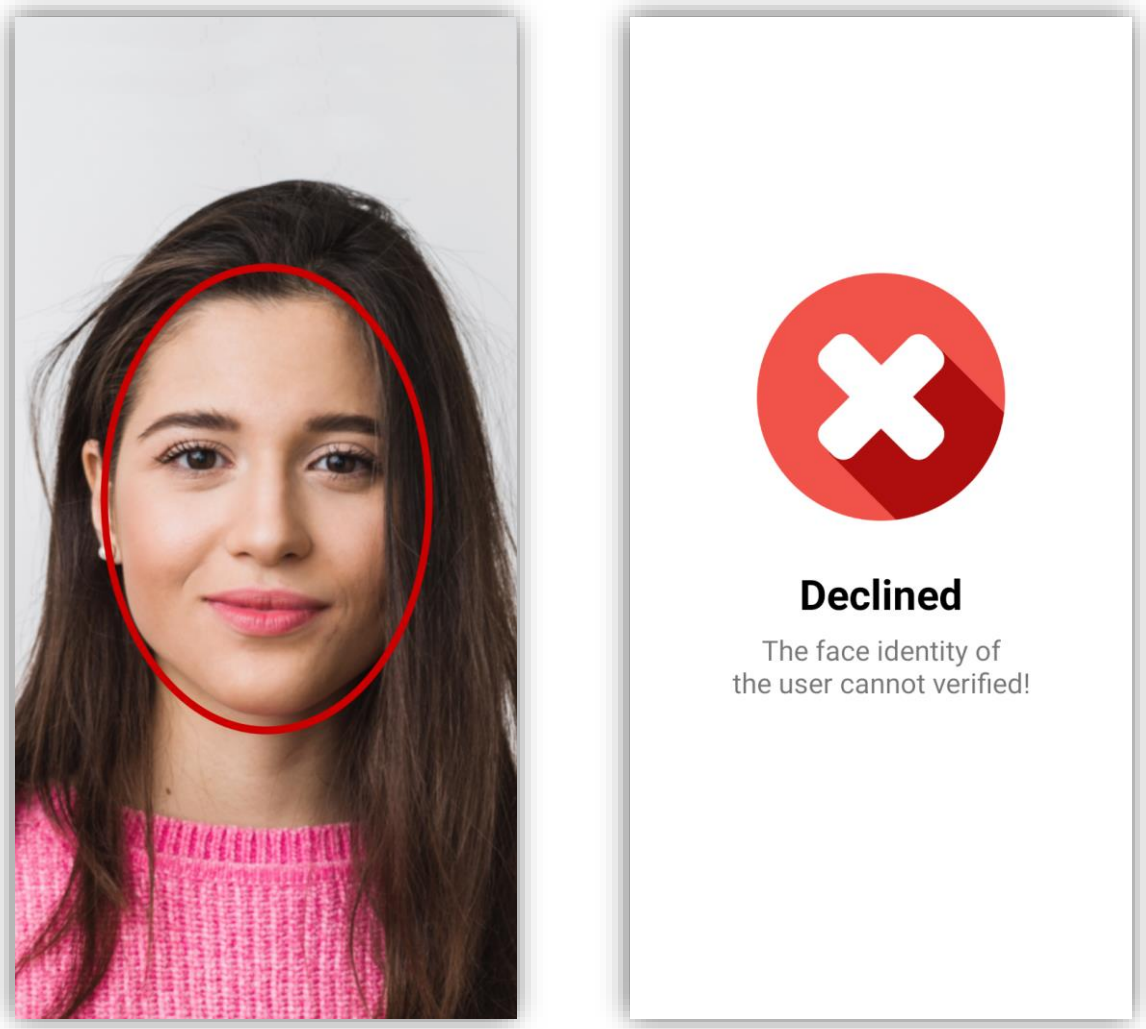
Εικόνα 57 - Ενημέρωση για Διακοπή του Συναγερμού

Μετά την ενεργοποίηση του συναγερμού και την ολοκλήρωση του συνδυασμού ηχητικών και οπτικών ειδοποιήσεων συναγερμού μετά από 15 λεπτά, η εφαρμογή εμφανίζει ένα ενημερωτικό μήνυμα που υποδεικνύει ότι η λειτουργία του συναγερμού έχει σταματήσει. Αυτό το μήνυμα διασφαλίζει ότι ο χρήστης γνωρίζει ότι ο συναγερμός έχει απενεργοποιηθεί και ότι η ειδοποίηση έκτακτης ανάγκης έχει ολοκληρωθεί.



Εικόνα 58 - Οθόνες Ενημέρωσης Επιτυχής Απενεργοποίησης της Φύλαξης

Όταν το σύστημα επαληθεύεται επιτυχώς είτε με PIN ασφαλείας είτε με την αναγνώριση προσώπου, θα εμφανιστεί ένα ενημερωτικό μήνυμα ανάλογα με τη μέθοδο επαλήθευσης που χρησιμοποιήθηκε. Δηλαδή, αν η επαλήθευση επιτευχθεί μέσω αναγνώρισης προσώπου, θα εμφανιστεί οθόνη που θα υποδεικνύει την επιτυχή επαλήθευση της αναγνώρισης προσώπου. Αν η επαλήθευση πραγματοποιείται με τη χρήση του PIN ασφαλείας, τότε η οθόνη θα ενημερώνει τον χρήστη για την επιτυχή επαλήθευση του PIN και την απενεργοποίηση του συναγερμού. Μετά από αυτές τις οθόνες πληροφοριών, η εφαρμογή θα συνεχίσει στην αρχική οθόνη.



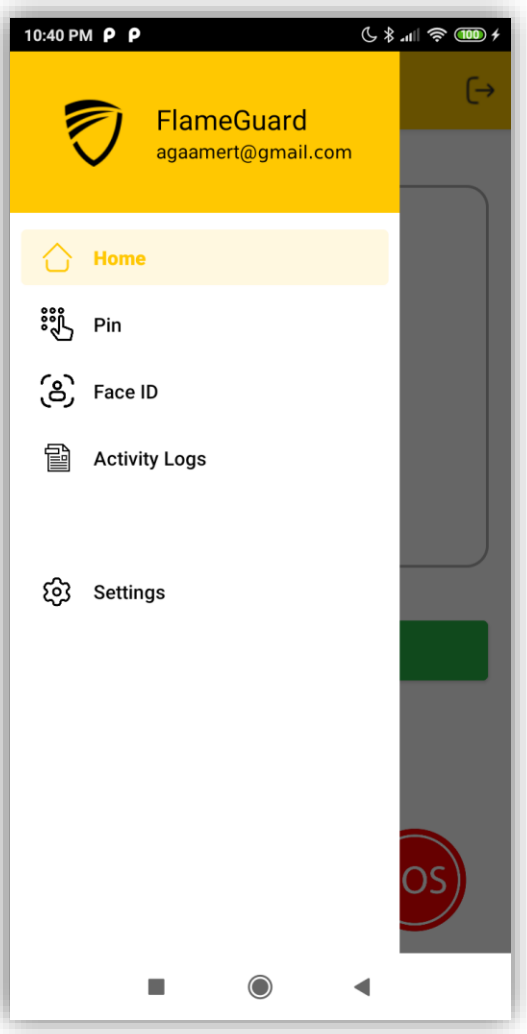
Εικόνα 59 - Ενημέρωση για Ανεπιτυχής Επαλήθευση Προσώπου

Για να μειωθεί η πολυπλοκότητα του συστήματος, η επαλήθευση προσώπου από το μενού διαχείρισης αναγνώρισης προσώπου και η επαλήθευση προσώπου από τη φύλαξη εκτελούνται μέσω της ίδιας δραστηριότητας. Πραγματοποιείται έλεγχος για να διαπιστωθεί αν η κλάση κλήθηκε μέσω του μενού ή μέσω της φύλαξης, και η ανεπιτυχής επαλήθευση προσώπου αντιμετωπίζεται διαφορετικά στις δύο περιπτώσεις.

Εάν η επαλήθευση προσώπου έχει κληθεί από το μενού διαχείρισης αναγνώρισης προσώπου, τότε η ανεπιτυχής επαλήθευση οδηγεί σε ενημέρωση του χρήστη που αναφέρει ότι η επαλήθευση προσώπου δεν ολοκληρώθηκε επιτυχώς και απορρίφθηκε. Στην περίπτωση της φύλαξης, αν η επαλήθευση προσώπου αποτύχει,

το σύστημα ενεργοποιεί απευθείας τον συναγερμό αντί να εμφανίζει απλώς μια ενημέρωση.

Επιπλέον, σε περίπτωση ανεπιτυχής αναγνώρισης, το οβάλ θα γίνει εντελώς κόκκινο, παρέχοντας μια σαφή οπτική ένδειξη της αποτυχημένης προσπάθειας επαλήθευσης.



Εικόνα 60 - Επιλογές του Μενού της Αρχικής Οθόνης

Παραπάνω είναι οι επιλογές του μενού που είναι προσβάσιμες από τις τρεις γραμμές στην επάνω αριστερή πλευρά της αρχικής οθόνης.

Το μενού περιλαμβάνει επιλογές για:

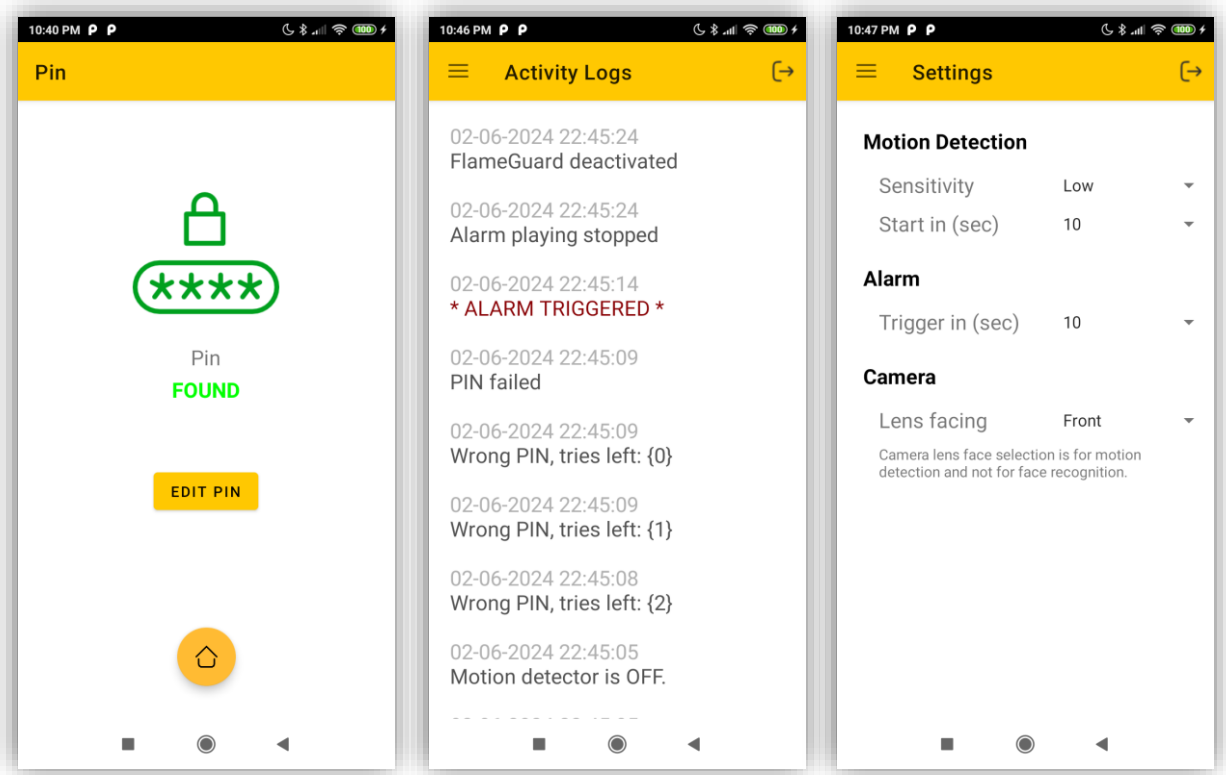
Αρχική σελίδα (Home): Επιστροφή στην αρχική οθόνη.

PIN: Διαχείριση των ρυθμίσεων PIN.

Face ID: Διαχείριση ρυθμίσεων αναγνώρισης προσώπου.

Αρχεία καταγραφής δραστηριοτήτων (Activity Logs): Προβολή αρχείων καταγραφής των δραστηριοτήτων από τις προηγούμενες ενεργοποίησεις φύλαξης.

Ρυθμίσεις (Settings): Πρόσβαση στις γενικές ρυθμίσεις της εφαρμογής που σχετίζονται κυρίως με την φύλαξη.



Εικόνα 61 - Οθόνες των Επιλογών του Μενού της Αρχικής Οθόνης

Η αριστερή εικόνα δείχνει τη διαχείριση του PIN, όπου οι χρήστες μπορούν να διαχειριστούν τις ρυθμίσεις του PIN ασφαλεία τους. Αυτή η οθόνη επιτρέπει στους χρήστες να ελέγχουν την κατάσταση του PIN τους και να το επεξεργάζονται, αν είναι απαραίτητο.

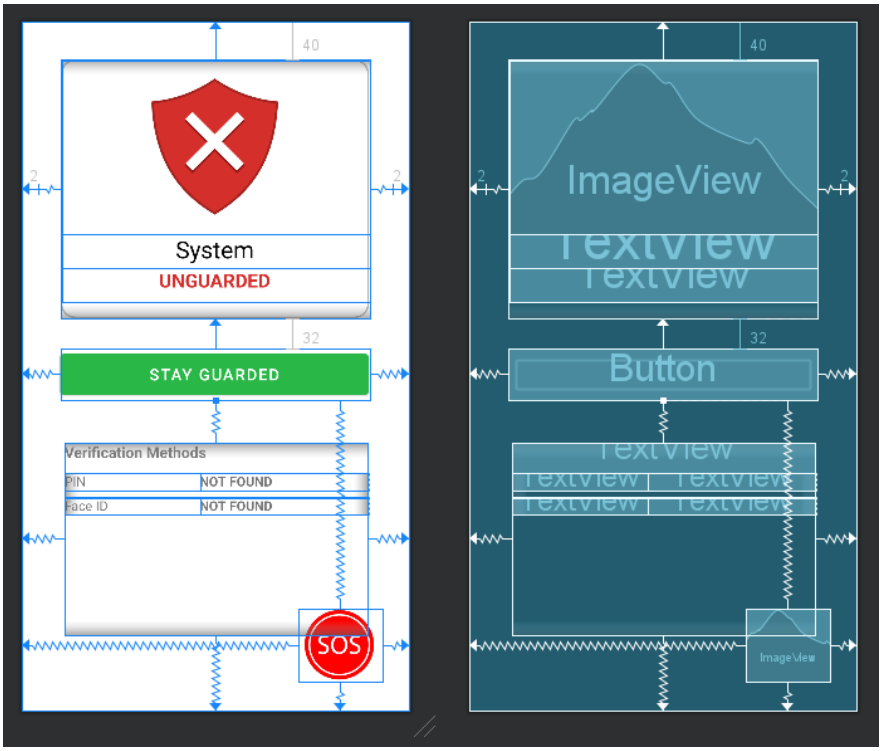
Στην κεντρική εικόνα εμφανίζεται το αρχείο καταγραφής δραστηριοτήτων, το οποίο διατηρεί αρχείο προηγούμενων ενεργειών ασφαλείας. Αυτό το αρχείο καταγραφής παρέχει λεπτομερείς πληροφορίες σχετικά με συμβάντα, όπως ενεργοποιήσεις συναγερμών, προσπάθειες εισαγωγής PIN, προσπάθειες αναγνώρισης προσώπου, κατάσταση για τη φύλαξη και απενεργοποιήσεις του συστήματος, επιτρέποντας στους χρήστες να επανεξετάζουν και να παρακολουθούν τις δραστηριότητες ασφαλείας.

Στη δεξιά εικόνα παρουσιάζονται οι ρυθμίσεις της εφαρμογής που σχετίζονται με τη φύλαξη. Αυτή η οθόνη περιλαμβάνει επιλογές για την προσαρμογή της ευαισθησίας ανίχνευσης κίνησης, τη ρύθμιση της ώρας έναρξης και της ώρας ενεργοποίησης του συναγερμού και τη διαμόρφωση των ρυθμίσεων της κάμερας. Αυτές οι ρυθμίσεις επιτρέπουν στους χρήστες να προσαρμόζουν τις λειτουργίες ασφαλείας της εφαρμογής στις προτιμήσεις και τις ανάγκες τους.

4.5.3 Σχεδιασμός Διάταξης και Πηγές Αρχείων XML

Ο σχεδιασμός προσαρμοστικών διεπαφών και η αποτελεσματική χρήση των πόρων XML παίζουν καθοριστικό ρόλο στην ανάπτυξη μιας εφαρμογής με τη χρήση του Android Studio. Κατανοώντας τις αρχές και τις τεχνικές, δημιουγήθηκαν οπτικά ελκυστικές και φιλικές προς το χρήστη διεπαφές που προσαρμόζονται απρόσκοπτα σε διάφορα μεγέθη και προσανατολισμούς οθόνης.

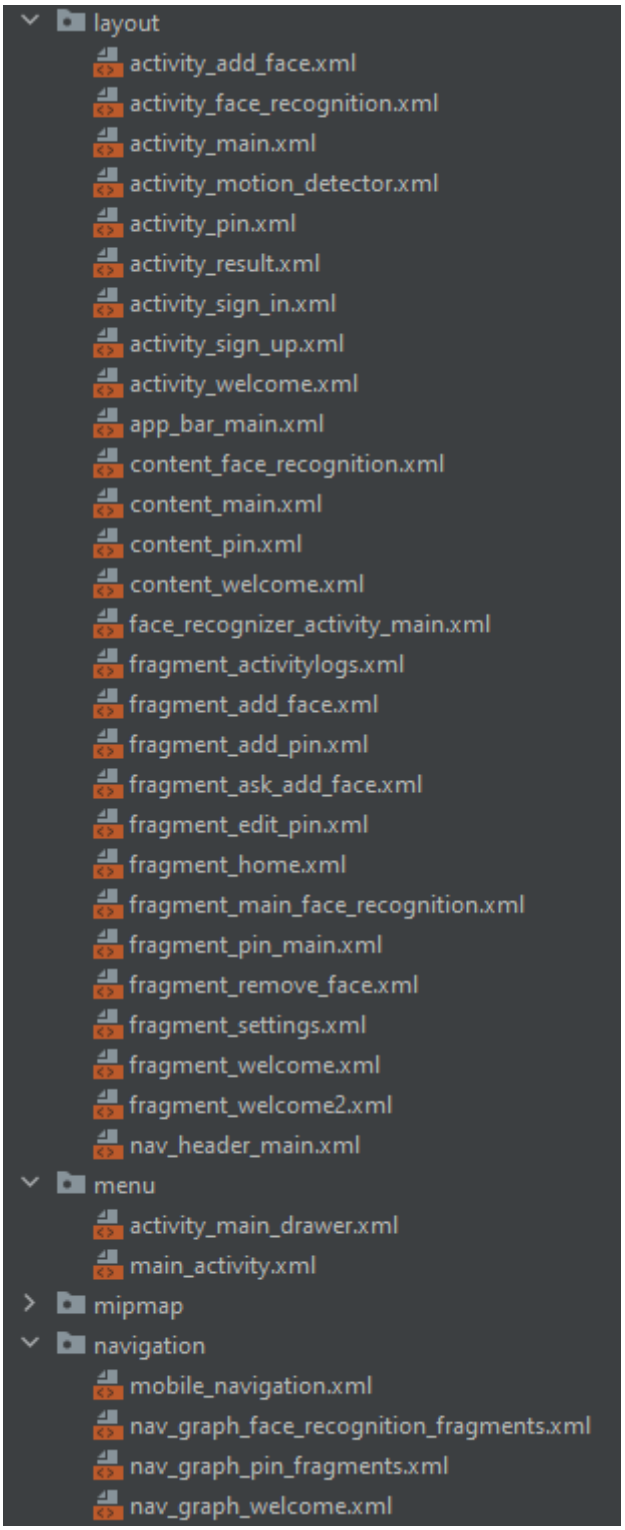
Χρησιμοποιώντας τις ιδιότητες του XML, καθοριστήκαν οι συμπεριφορές, οι εφμανίσεις και οι θέσεις του κάθε στοιχείου UI. Αυτή η μέθοδος εξασφαλίζει σαφή διαχωρισμό μεταξύ του επιπέδου παρουσίασης και της λογικής της εφαρμογής, απλοποιώντας τη διαχείριση και τη συντήρηση του κώδικα.



Εικόνα 62 - Περιορισμοί και Οδηγίες Διάταξης των Στοιχείων στο XML Layout

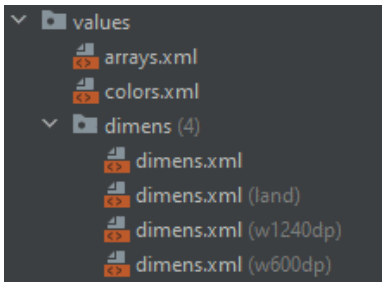
Η δημιουργία ευέλικτων διατάξεων απαιτεί προσεκτική εξέταση των διαφορετικών μεγεθών και προσανατολισμών οθόνης που θα συναντήσει η εφαρμογή. Η εφαρμογή περιορισμών και οδηγιών διάταξης βοηθά στην επίτευξη ενός προσαρμοστικού σχεδιασμού. Οι περιορισμοί επιτρέπουν στα στοιχεία του UI να προσαρμόζονται και να διατηρούν τις σχετικές θέσεις τους καθώς αλλάζει το μέγεθος της οθόνης, εξασφαλίζοντας μια συνεπή διάταξη σε διάφορες συσκευές. Οι οδηγίες διάταξης

παρέχουν οπτικές αναφορές για την ευθυγράμμιση και την τοποθέτηση των στοιχείων UI, βοηθώντας στη διατήρηση ενός ισορροπημένου και αρμονικού σχεδιασμού.



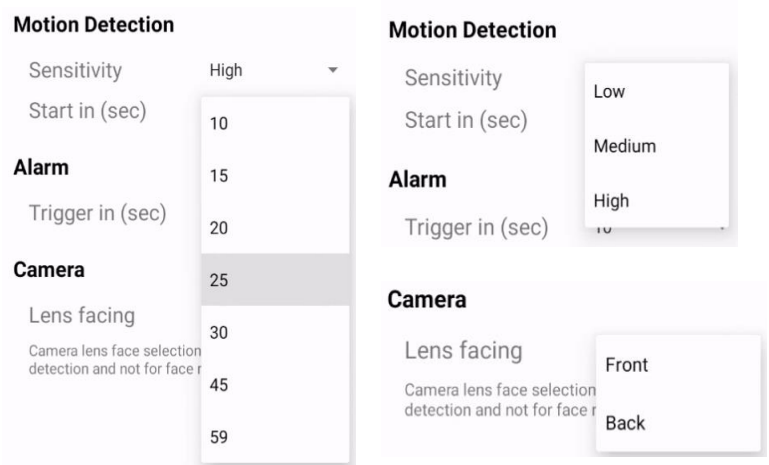
Εικόνα 63 - XML Αρχεία της Εφαρμογής στο Android Studio

Επιπλέον, η διαχείριση διαφορετικών μεγεθών συσκευών και των διαφορετικών πυκνοτήτων εικονοστοιχείων είναι σημαντική για τη δημιουργία ενός προσαρμοστικού σχεδιασμού UI. Οι συσκευές Android διαφέρουν σημαντικά ως προς την πυκνότητα εικονοστοιχείων, που κυμαίνεται από χαμηλή έως πολύ υψηλή. Για την αντιμετώπιση αυτού του ζητήματος, δόθηκε έμφαση στην υλοποίηση της εφαρμογής Flame Guard, ώστε να παρέχει πολλαπλές εκδόσεις για κάθε επίπεδο πυκνότητας εικονοστοιχείων. Αυτή η πρακτική διασφαλίζει ότι τα περιεχόμενα και τα εικονίδια στις οθόνες των διαφορετικών συσκευών παραμένουν ίδιες, ευκρινείς και καθαρές, αποφεύγοντας προβλήματα. Με την εφαρμογή πόρων που αφορούν την πυκνότητα, η εφαρμογή διατηρεί την οπτική συνοχή σε όλες τις συσκευές, παρέχοντας μια συνεκτική και υψηλής ποιότητας εμπειρία χρήστη ανεξάρτητα από το μέγεθος της οθόνης.



Εικόνα 64 - Αρχεία Διαφορετικών Διαστάσεων

Στο πλαίσιο της ανάπτυξης μιας εφαρμογής, το αρχείο *arrays.xml* χρησιμοποιείται για τον ορισμό μεταβλητών που έχουν πολλαπλές επιλογές. Στην υλοποίηση της εφαρμογής FlameGuard, αυτή η υποστήριξη χρησιμοποιείται στην οθόνη ρυθμίσεων και στα αρχεία καταγραφής δραστηριοτήτων. Αυτοί οι πίνακες επιτρέπουν στους χρήστες να φιλτράρουν κατηγορίες καταγραφής και να επιλέγουν από πολλαπλές προκαθορισμένες επιλογές. Αυτή η προσέγγιση παρέχει τόσο ευελιξία όσο και συνέπεια, επιτρέποντας στην εφαρμογή να παρουσιάζει στον χρήστη μια ποικιλία στατικών τιμών με οργανωμένο τρόπο.



Εικόνα 65 - Παραδείγματα Επιλογών Ρυθμίσεων

4.6 Διασφάλιση Ποιότητας της Εφαρμοφής

Η διασφάλιση ποιότητας στην ανάπτυξη λογισμικού διασφαλίζει ότι τα προϊόντα πληρούν τις καθορισμένες απαιτήσεις και λειτουργούν σωστά. Περιλαμβάνει συστηματικές δραστηριότητες με στόχο τη βελτίωση της διαδικασίας ανάπτυξης και την πρόληψη των ελαττωμάτων. Η διασφάλιση ποιότητας είναι απαραίτητη για την παροχή λογισμικού υψηλής ποιότητας, την ενίσχυση της ικανοποίησης των χρηστών, τη μείωση του κόστους και τη διασφάλιση της συμμόρφωσης με πρότυπα και κανονισμούς. Εντοπίζοντας και διορθώνοντας προβλήματα νωρίς στον κύκλο ανάπτυξης, η ποιότητα ελέγχου ελαχιστοποιεί τον κίνδυνο ελαττωμάτων μετά την έκδοση, οδηγώντας σε εξοικονόμηση κόστους και βελτίωση της αξιοπιστίας του λογισμικού [77].

Η διασφάλιση ποιότητας στην ανάπτυξη λογισμικού χρησιμοποιεί τόσο αυτοματοποιημένες όσο και χειροκίνητες τεχνικές δοκιμών για να διασφαλίσει ότι οι εφαρμογές πληρούν τις καθορισμένες απαιτήσεις και λειτουργούν σωστά. Οι αυτοματοποιημένες δοκιμές, συμπεριλαμβανομένων των δοκιμών μονάδας (unit tests), επαληθεύουν γρήγορα και επανειλημμένα μεμονωμένα στοιχεία του κώδικα, ενισχύοντας την αποδοτικότητα και επιτρέποντας τη συνεχή ολοκλήρωση. Οι χειροκίνητες δοκιμές περιλαμβάνουν την εκτέλεση δοκιμών χωρίς εργαλεία αυτοματοποίησης, καθιστώντας την απαραίτητη για διερευνητικές δοκιμές και δοκιμές ευχρηστίας. Η χειροκίνητη δοκιμή επιτρέπει στους ελεγκτές να αξιολογήσουν τη συμπεριφορά της εφαρμογής από την οπτική γωνία του χρήστη, εξασφαλίζοντας μια ολοκληρωμένη αξιολόγηση της λειτουργικότητας και της εμπειρίας του χρήστη.

Τα παρακάτω σενάρια δοκιμών στον *Πίνακας 1* απεικονίζουν την εκτέλεση των προτύπων χειροκίνητων σεναρίων για την εφαρμογή Flame Guard.

Πίνακας 1 - Διασφάλιση Ποιότητας στην Ανάπτυξη Εφαρμογής

ID	Σενάριο Δοκιμής	Προϋποθέσεις	Βήματα Δοκιμής	Αναμενόμενο Αποτέλεσμα	Αποτέλεσμα
TC01	Εγγραφή Χρήστη	Ο χρήστης βρίσκεται στην οθόνη εγγραφής. Υπάρχει διαθέσιμη σύνδεση στο διαδίκτυο.	1. Εισάγετε έγκυρη διεύθυνση email. 2. Εισάγετε κωδικό πρόσβασης. 3. Επιβεβαιώστε τον κωδικό πρόσβασης. 4. Πατήστε το κουμπί "Register".	Ο χρήστης λαμβάνει μήνυμα επιβεβαίωσης και ανακατευθύνεται στο SignInActivity.	Επιτυχής
TC02	Σύνδεση Χρήστη	Ο χρήστης έχει λογαριασμό και βρίσκεται στην οθόνη σύνδεσης.	1. Εισάγετε την εγγεγραμμένη διεύθυνση email. 2. Εισάγετε τον σωστό κωδικό πρόσβασης. 3. Πατήστε το κουμπί "Sign In".	Ο χρήστης συνδέεται επιτυχώς και ανακατευθύνεται στο MainActivity.	Επιτυχής
TC03	Ενεργοποίηση Ανίχνευσης Κίνησης	Ο χρήστης είναι συνδεδεμένος και βρίσκεται στο MainActivity. Οι ρυθμίσεις ανίχνευσης κίνησης είναι ρυθμισμένες.	1. Ενεργοποιήστε τον συναγερμό από το MainActivity 2. Βεβαιωθείτε ότι η κάμερα της συσκευής λειτουργεί.	Η ανίχνευση κίνησης ενεργοποιείται και η συσκευή ξεκινά την παρακολούθηση για κίνηση.	Επιτυχής
TC04	Επαλήθευση με PIN	Η ανίχνευση κίνησης ενεργοποιείται. Ο χρήστης καλείται να εισάγει το PIN.	1. Εισάγετε το σωστό PIN.	Ο χρήστης επαληθεύει επιτυχώς την ταυτότητά του και ο συναγερμός απενεργοποιείται εάν το PIN είναι σωστό.	Επιτυχής
TC05	Εσφαλμένη Εισαγωγή PIN	Η ανίχνευση κίνησης ενεργοποιείται. Ο χρήστης καλείται να εισάγει το PIN.	1. Εισάγετε εσφαλμένο PIN. 2. Επαναλάβετε την εσφαλμένη εισαγωγή PIN έως ότου εξαντληθούν οι προσπάθειες.	Ο χρήστης λαμβάνει μήνυμα σφάλματος για κάθε εσφαλμένη προσπάθεια και ο συναγερμός ενεργοποιείται μετά τη μέγιστη προσπάθεια.	Επιτυχής
TC06	Επαλήθευση με Αναγνώριση Προσώπου	Η ανίχνευση κίνησης ενεργοποιείται.	1. Χρησιμοποιήστε την εμπρόσθια κάμερα για να σαρώσετε το πρόσωπο του χρήστη.	Ο χρήστης επαληθεύει επιτυχώς την ταυτότητά του εάν το πρόσωπο αναγνωριστεί και ο συναγερμός απενεργοποιείται.	Επιτυχής

TC07	Ειδοποίηση Συναγερμού	Η ανίχνευση κίνησης ενεργοποιείται και η επαλήθευση αποτυγχάνει.	1. Ενεργοποιήστε τον συναγερμό αποτυγχάνοντας την επαλήθευση ταυτότητας.	Ο χρήστης λαμβάνει άμεση ειδοποίηση μέσω SMS ή μέσω εφαρμογής σε άλλη συσκευή με λεπτομέρειες της ύποπτης δραστηριότητας.	Επιτυχής
TC08	Λειτουργία Κουμπιού SOS	Ο χρήστης βρίσκεται στο MainActivity.	1. Πατήστε το κουμπί SOS.	Ο συναγερμός SOS ενεργοποιείται αμέσως.	Επιτυχής
TC09	Πλοήγηση μέσω του Μενού	Ο χρήστης είναι συνδεδεμένος και βρίσκεται στο MainActivity.	1. Ανοίξτε το μενού 2. Επιλέξτε "Home". 3. Επιλέξτε "PIN". 4. Επιλέξτε "Face ID" 5. Επιλέξτε "Activity Logs". 6. Επιλέξτε "Settings"	Ο χρήστης πλοηγείται στις αντίστοιχες οθόνες και κάθε οθόνη εμφανίζει το σωστό περιεχόμενο που σχετίζεται με το επιλεγμένο στοιχείο μενού.	Επιτυχής
TC10	Επεξεργασία Ρυθμίσεων Χρήστη	Ο χρήστης είναι συνδεδεμένος και βρίσκεται στην οθόνη Ρυθμίσεων.	1. Αλλάξτε τον χρόνο ενεργοποίησης του συναγερμού. 2. Αλλάξτε την ευαισθησία κίνησης.	Οι ρυθμίσεις ενημερώνονται επιτυχώς και αποθηκεύονται στη βάση δεδομένων.	Επιτυχής
TC11	Προβολή Καταγραφών Δραστηριότητας	Ο χρήστης είναι συνδεδεμένος και βρίσκεται στο MainActivity.	1. Πλοηγηθείτε στην οθόνη Activity Logs από το μενού.	Ο χρήστης μπορεί να δει μια λίστα με όλες τις καταγραφές δραστηριότητας, συμπερ/μένων των ενεργοποιήσεων συναγερμών και των προσπαθειών επαλήθευσης.	Επιτυχής

Ο *Πίνακας 1* επισημαίνει τις βασικές περιπτώσεις χειροκίνητων δοκιμών και τα αποτελέσματα που εκτελέστηκαν για την εφαρμογή Flame Guard. Οι δοκιμές περιλαμβάνουν την επαλήθευση των διαδικασιών σύνδεσης και εγγραφής του χρήστη, την ανίχνευση και την απόκριση κίνησης, την αναγνώριση PIN και προσώπου για την απενεργοποίηση του συναγερμού και την πλοήγηση στο κύριο μενού και στα μενού ρυθμίσεων. Κάθε δοκιμή σχεδιάστηκε για να διασφαλίσει ότι η εφαρμογή πληροί τις απαιτήσεις της και λειτουργεί αξιόπιστα. Όλες οι περιπτώσεις δοκιμών πραγματοποιήθηκαν και πέρασαν με επιτυχία, επιβεβαιώνοντας την ευστάθεια και την αξιοπιστία της εφαρμογής.

4.7 Διαχείριση Έργου και Μοντέλο Ανάπτυξης Εφαρμογής

4.7.1 Συνοπτική Επισκόπηση Διαχείρισης Έργου

Η αποτελεσματικότητα της εφαρμογής Flame Guard βασίζεται σε μια δομημένη προσέγγιση στη διαχείριση του έργου. Η μεθοδολογία που ακολουθείται διασφαλίζει ότι όλες οι φάσεις του έργου, από την έναρξη έως την ανάπτυξη, είναι καλοσχεδιασμένες και εκτελεσμένες. Αυτό περιλαμβάνει τον καθορισμό σαφών στόχων, τον καθορισμό χρονοδιαγραμμάτων, την ανάθεση καθηκόντων και την παρακολούθηση της προόδου για να διασφαλιστεί η έγκαιρη υλοποίηση.

4.7.1.1 Κύκλος Ζωής Ανάπτυξης Λογισμικού

Η υλοποίηση της εφαρμογής ακολουθεί το μοντέλο κύκλου ζωής ανάπτυξης λογισμικού (Software Development Life Cycle - SDLC).

Οι φάσεις του SDLC περιλαμβάνουν:

Ανάλυση απαιτήσεων: Συγκέντρωση και ανάλυση των απαιτήσεων από τα ενδιαφερόμενα μέρη.

Σχεδιασμός: Δημιουργία της αρχιτεκτονικής του συστήματος και των προδιαγραφών σχεδιασμού.

Υλοποίηση: Υλοποίηση της εφαρμογής με βάση τις προδιαγραφές σχεδιασμού.

Δοκιμές: Επικύρωση της λειτουργικότητας, της απόδοσης και της ασφάλειας της εφαρμογής.

Συντήρηση: Παροχή συνεχούς υποστήριξης και ενημερώσεων μετά την ανάπτυξη.

4.7.2 Συνοπτική Επισκόπηση Μοντέλου Ανάπτυξης Εφαρμογής

4.7.2.1 Μεθοδολογία Agile

Για την προσαρμογή στις μεταβαλλόμενες απαιτήσεις και τη διασφάλιση της συνεχούς βελτίωση της εφαρμογής, χρησιμοποιείται η μεθοδολογία Agile η οποία παρέχει μια ευέλικτη και επαναληπτική προσέγγιση στη διαχείριση του έργου.

Οι βασικές Agile πρακτικές περιλαμβάνουν:

Σχεδιασμός: Καθορισμός στόχων για κάθε κύκλο ζωής ανάπτυξης .

Ανασκοπήσεις : Αξιολόγηση των αποτελεσμάτων κάθε στόχων.

Επαναληπτικές προοπτικές: Αναδρομή στους στόχους για τον εντοπισμό σημείων βελτίωσης.

4.7.3 Εργαλεία Διαχείρισης Έργου

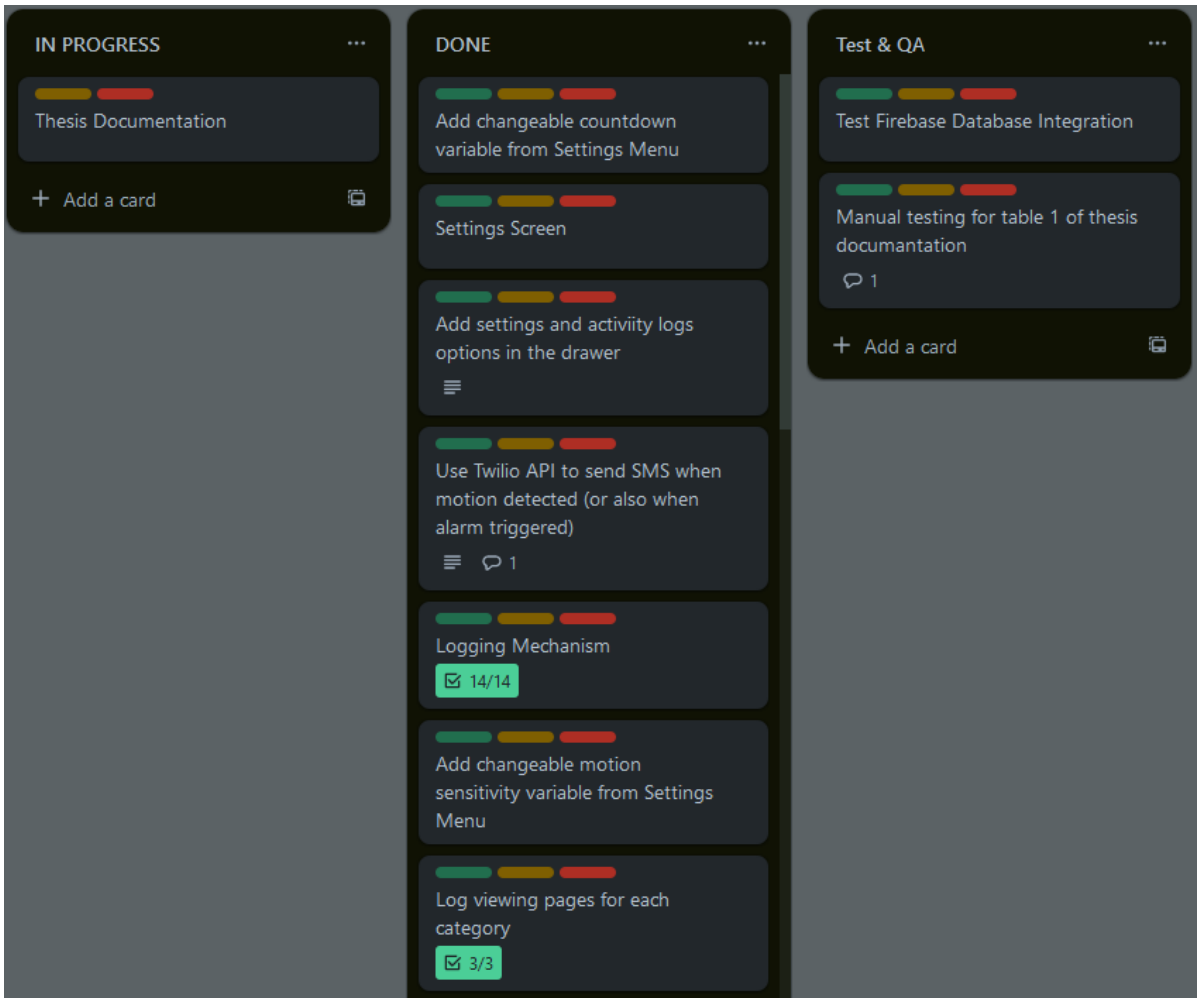
Για την αποτελεσματική διαχείριση του έργου και την ανάπτυξη της εφαρμογής Flame Guard, χρησιμοποιήθηκαν διάφορα βασικά εργαλεία και πρακτικές, τα οποία παίζουν σημαντικό ρόλο στη διασφάλιση της επιτυχίας της εργασίας.

Στην διαχείριση του έργου αξιοποιήθηκαν τα εργαλεία όπως το Trello και το Clockify για την παρακολούθηση εργασιών και τη διαχείριση του χρόνου. Το Trello παρέχει μια οπτική διεπαφή με το σύστημα που βασίζεται σε κάρτες, επιτρέποντας την παρακολούθηση εργασίας σε διάφορα στάδια ολοκλήρωσης. Υποστηρίζει χαρακτηριστικά όπως η ιεράρχηση εργασιών, οι προθεσμίες και τα συνεργατικά σχόλια, τα οποία ενισχύουν την τρέχουσα κατάσταση της εργασίας. Το Clockify βοηθάει στην παρακολούθηση του χρόνου που δαπανάται για τις εργασίες και διασφαλίση της ακριβής καταγραφής του χρόνου. Αυτή η διπλή προσέγγιση διασφαλίζει ότι τόσο η διαχείριση εργασιών όσο και η παρακολούθηση του χρόνου αντιμετωπίζονται αποτελεσματικά.

Στην εφαρμογή χρησιμοποιήθηκε επιπλέον το GitHub για τον έλεγχο εκδόσεων. Το GitHub διευκολύνει την παρακολούθηση των αλλαγών στον κώδικα, τη δημιουργία πολλών branches για νέα χαρακτηριστικά και την απρόσκοπτη συγχώνευση αυτών

των αλλαγών πίσω στην κύρια βάση κώδικα. Με τα commits, κάθε αλλαγή κώδικα καταγράφεται, οπότε είναι εύκολη η επαναφορά σε προηγούμενες εκδόσεις αν κάτι πάει στραβά. Αυτό το σύστημα επιτρέπει πολλαπλές συνεισφορές στον κώδικα ταυτόχρονα χωρίς να υπάρχουν συγκρούσεις, καθιστώντας τον αποτελεσματικό. Το GitHub προσφέρει επίσης χρήσιμες λειτουργίες, όπως τα pull requests για την αναθεώρηση των αλλαγών, την παρακολούθηση προβλημάτων για τη διαχείριση εργασιών.

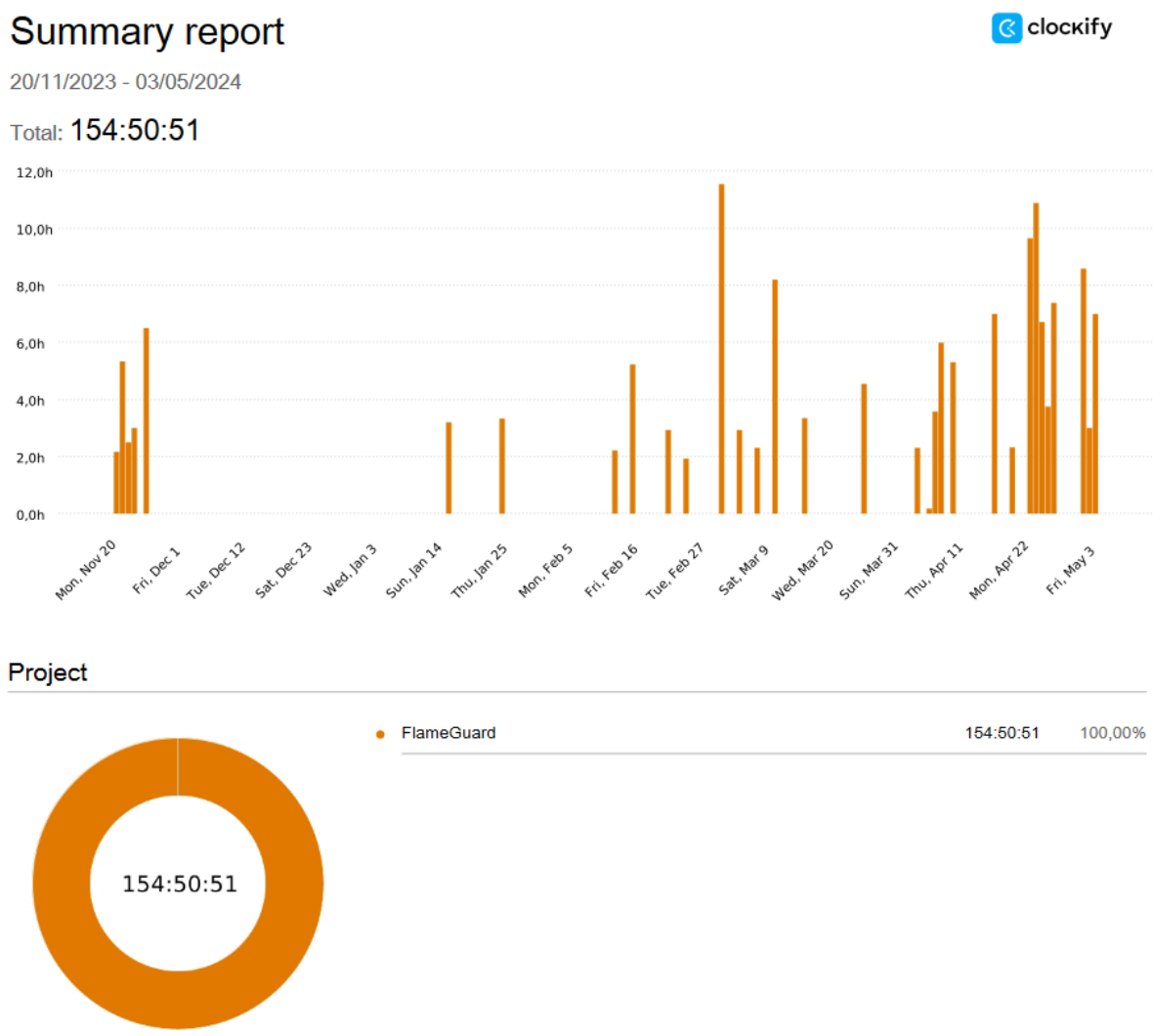
Παραδείγματα χρήσης όλων των εργαλείων



Εικόνα 66 - Παράδειγμα από τον Πίνακα Kanban για τη Διαχείριση της Εργασίας (Trello)

Το παράδειγμα του πίνακα Kanban απεικονίζει τη διαδικασία διαχείρισης έργων με τη χρήση του Trello. Οι εργασίες οργανώνονται σε στήλες που αντιπροσωπεύουν διαφορετικά στάδια προόδου. Κάθε κάρτα αντιπροσωπεύει μια συγκεκριμένη διαδικασία, αναφέροντας λεπτομερώς την κατάσταση της και τυχόν σχετικά σχόλια ή

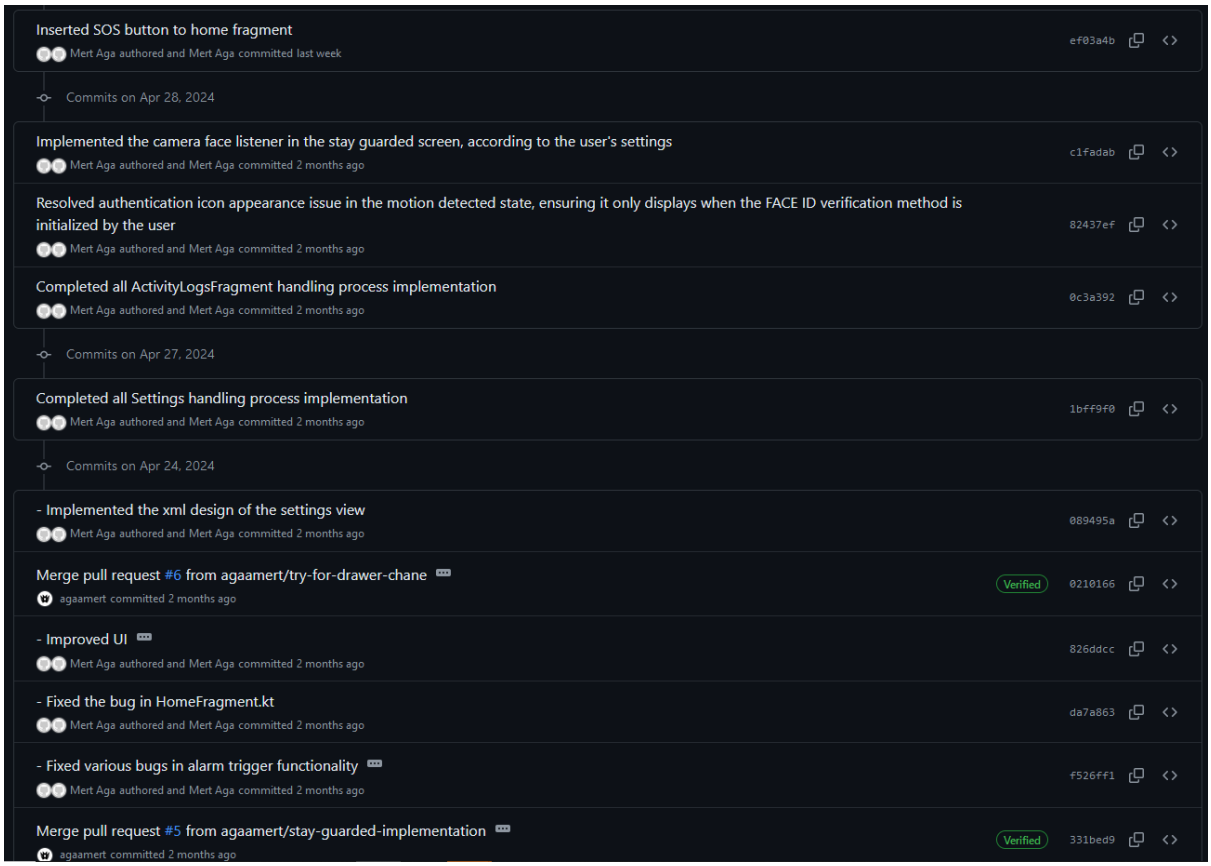
λίστες ελέγχου, διευκολύνοντας την αποτελεσματική παρακολούθηση και διαχείριση της ροής εργασιών του έργου. Ο πίνακας Kanban είναι ένα οπτικό εργαλείο που χρησιμοποιείται στη διαχείριση έργων για την αναπαράσταση εργασιών σε διάφορα στάδια μιας διαδικασίας, βοηθώντας την απικόνηση της πρόοδου.



Εικόνα 67 - Συνοπτική Αναφορά για την Διαχείριση Έργου (Clockify)

Η ολοκλήρωση της εργασίας Flame Guard, η οποία ξεκίνησε από τις 20 Νοεμβρίου 2023 έως τις 3 Μαΐου 2024, διήρκεσε συνολικά 154 ώρες, 50 λεπτά και 51 δευτερόλεπτα, δηλαδή περίπου 20 ανθρωποημέρες. Κατά την αρχική φάση, από τις 20 Νοεμβρίου έως τις 5 Δεκεμβρίου 2023, αφιερώθηκαν περίπου 10 ώρες στον προγραμματισμό του σχεδίου, στην ανάλυση απαιτήσεων και στον αρχικό σχεδιασμό. Στη συνέχεια έγινε η υλοποίηση της εφαρμογής και τις τελευταίες εβδομάδες

επικεντρώθηκαν στις δοκιμές, ώστε να διασφαλιστεί ότι η εφαρμογή ήταν αξιόπιστη και αποτελεσματική πριν από την παράδοση της στους χρήστες.



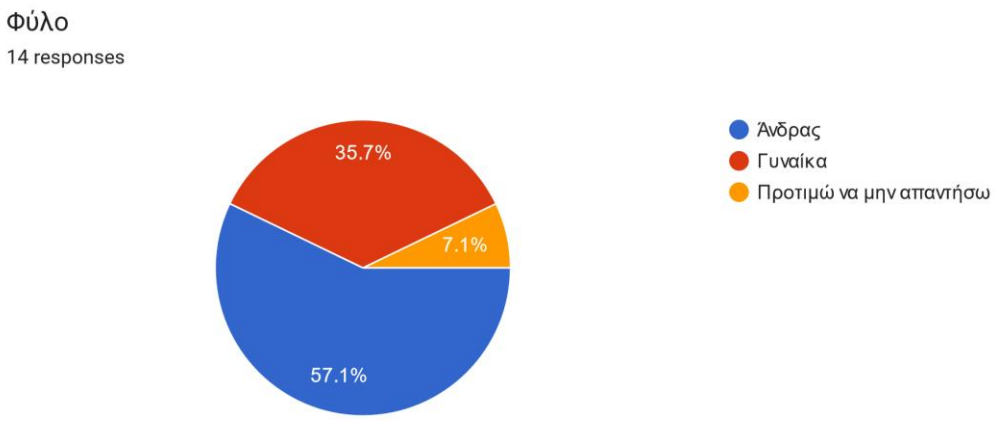
Εικόνα 68 - Παράδειγμα από τα commits στο repository (GitHub)

Η παραπάνω εικόνα είναι ένα παράδειγμα των commits και των pull requests από το repository της εργασίας FlameGuard στο GitHub. Παρουσιάζει διάφορες ενημερώσεις και βελτιώσεις που έγιναν στην εργασία.

5. Αξιολογήσεις Χρηστών

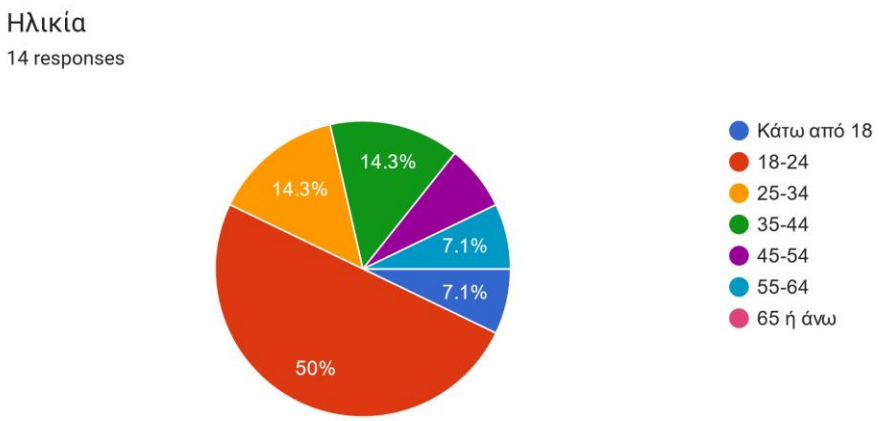
Οι αξιολογήσεις χρηστών αποτελούν κρίσιμο στοιχείο για την αξιολόγηση και τη βελτίωση της εφαρμογής Flame Guard. Μέσω των αξιολογήσεων και των σχολίων από τους χρήστες, μπορεί να κατανοηθεί καλύτερα η εμπειρία χρήσης, να εντοπιστούν τυχόν προβλήματα. Οι αξιολογήσεις παρέχουν πολύτιμες πληροφορίες σχετικά με την απόδοση των λειτουργιών, την ευχρηστία του UI και την αποτελεσματικότητα των μηχανισμών ασφαλείας. Αυτή η ενότητα παρουσιάζει τα αποτελέσματα των αξιολογήσεων που συλλέχθηκαν μέσω ενός ερωτηματολογίου που διανεμήθηκε σε ένα ευρύ φάσμα χρηστών της εφαρμογής για την αξιολόγηση της απόδοσής της και την ικανοποίηση των χρηστών.

Ακολουθεί η αξιολόγηση της εφαρμογής Flame Guard.

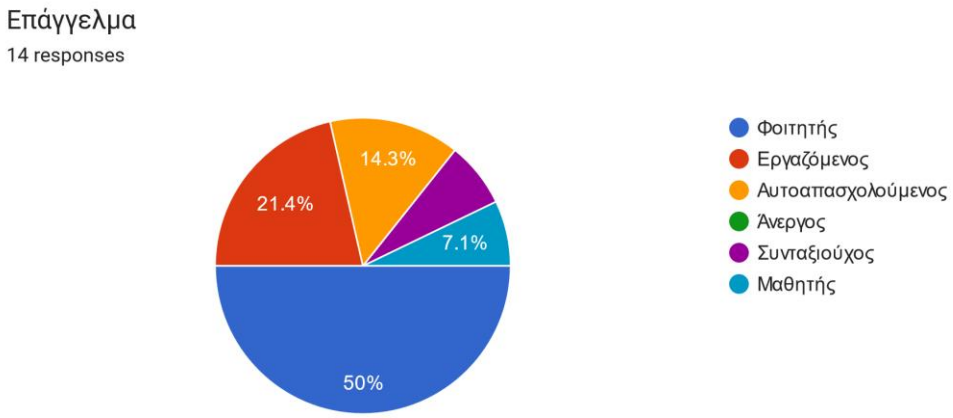


Γράφημα 1 - Κατανομή Φύλου

Το παραπάνω γράφημα παρουσιάζει την κατανομή του φύλου των συμμετεχόντων στην έρευνα αξιολόγησης της εφαρμογής Flame Guard. Από τις 14 απαντήσεις, το 57,1% ήταν άνδρες, το 35,7% γυναίκες, ενώ το 7,1% προτίμησε να μην απαντήσει στην ερώτηση για το φύλο. Αυτή η κατανομή παρέχει μια επισκόπηση της δημογραφικής σύνθεσης των χρηστών που συμμετείχαν στην αξιολόγηση.

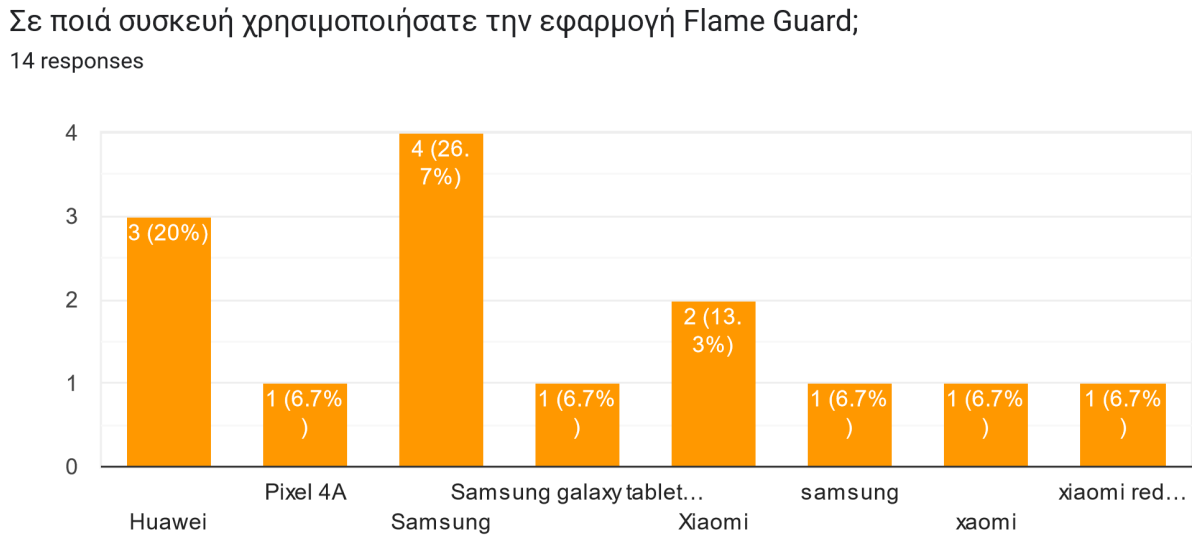


Γράφημα 2 - Κατανομή Ηλικίας



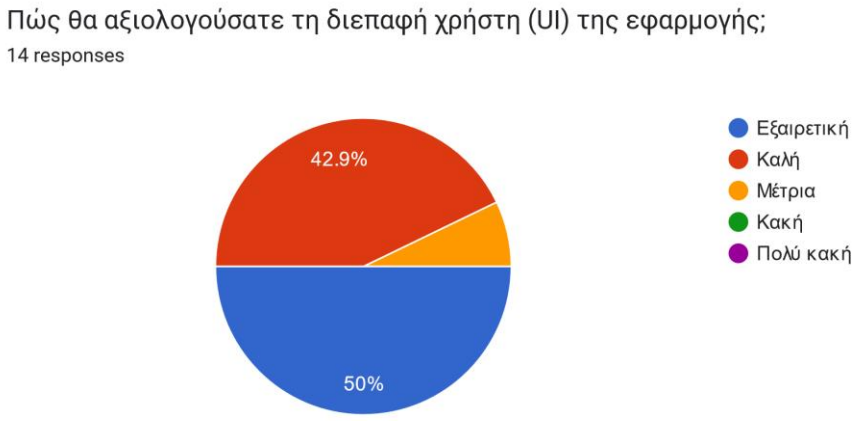
Γράφημα 3 - Κατανομή Επαγγέλματος

Το *Γράφημα 2* και *Γράφημα 3* παρουσιάζουν την κατανομή της ηλικίας και επαγγελματικών καταστάσεων των συμμετεχόντων στην έρευνα αξιολόγησης της εφαρμογής.



Γράφημα 4 - Συσκευές Χρήσης της Εφαρμογής

Το *Γράφημα 4* παρουσιάζει την κατανομή των συσκευών που χρησιμοποιήθηκε η εφαρμογή. Οι συσκευές Samsung αντιπροσωπεύουν το μεγαλύτερο ποσοστό με 33.4% όταν συνυπολογιστούν και οι γενικές συσκευές Samsung. Οι συσκευές Xiaomi, συμπεριλαμβανομένων των Redmi, κατέχουν επίσης ένα σημαντικό ποσοστό της τάξης του 26.7%. Οι συσκευές Huawei καταλαμβάνουν το 20%, ενώ οι συσκευές Pixel 4A καταλαμβάνουν το 6.7%.



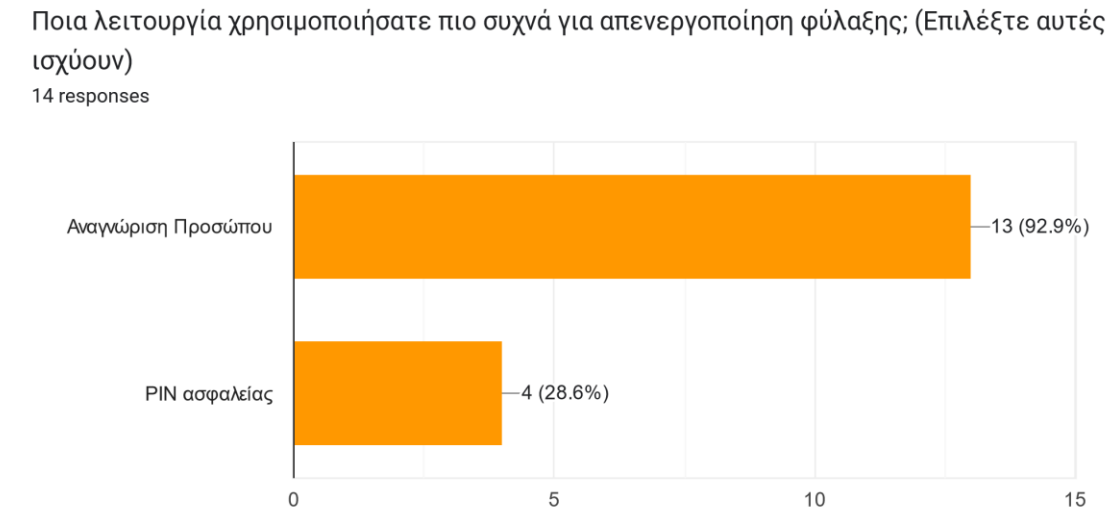
Γράφημα 5 - Αξιολόγηση της Διεπαφή Χρήστη (UI) της Εφαρμογής

Συνολικά, οι απόψεις για το UI είναι ιδιαίτερα θετικές. Η απουσία αρνητικών αξιολογήσεων, όπως «Κακή» ή «Πολύ κακή», υπογραμμίζει περαιτέρω την επιτυχία της εφαρμογής στην παροχή μιας φιλικής προς το χρήστη και οπτικά ελκυστική διεπαφή.

Γράφημα 6 - Χρήση Λειτουργιών της Εφαρμογής

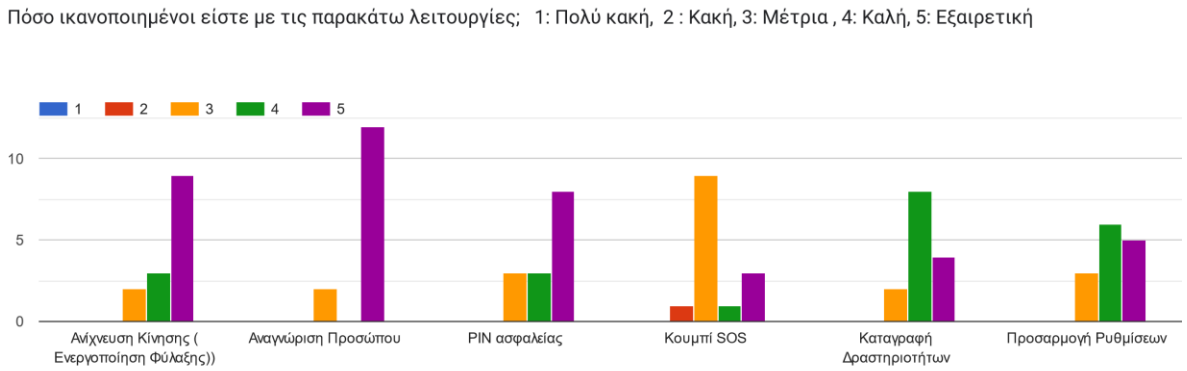
Η πιο συχνά χρησιμοποιούμενη λειτουργία είναι η ανίχνευση κίνησης, με το 92,9% των χρηστών να ενεργοποιεί αυτή τη λειτουργία. Αμέσως μετά, οι λειτουργίες αναγνώρισης προσώπου και PIN ασφαλείας χρησιμοποιήθηκαν από το 85,7% των συμμετεχόντων, υποδεικνύοντας τη σημασία τους στους χρήστες.

Συνολικά, το διάγραμμα αποτυπώνει ένα υψηλό ποσοστό υιοθέτησης των βασικών χαρακτηριστικών ασφαλείας, ενώ οι λειτουργίες προσαρμογής και ρύθμισης παρουσιάζουν διαφορετικά επίπεδα δέσμευσης μεταξύ των χρηστών.



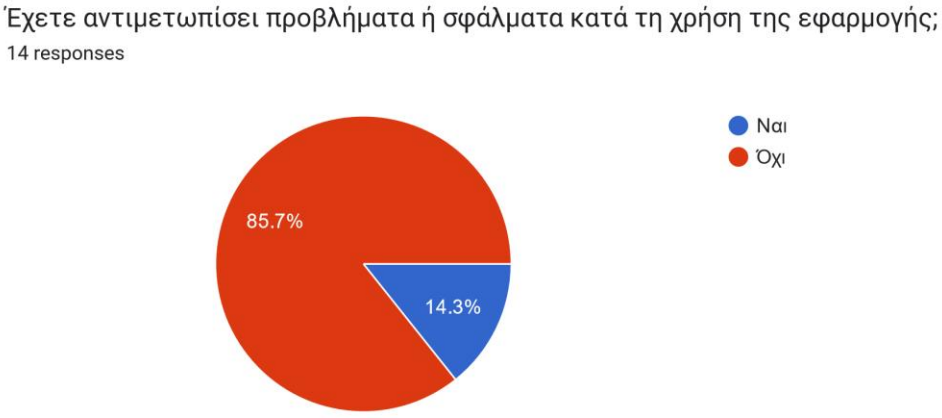
Γράφημα 7 - Χρήση Λειτουργιών για Απενεργοποίηση Φύλαξης

Το *Γράφημα 7* αποτυπώνει ότι οι χρήστες προτιμούν περισσότερο τη χρήση της αναγνώρισης προσώπου για την απενεργοποίηση της φύλαξης στην εφαρμογή, ενώ μικρότερο ποσοστό επιλέγει την απενεργοποίηση μέσω εισαγωγής το PIN ασφαλείας.



Γράφημα 8 - Ικανοποίηση Χρηστών με τις Λειτουργίες της Εφαρμογής

Τα επίπεδα ικανοποίησης για τα διάφορα χαρακτηριστικά της εφαρμογής Flame Guard απεικονίζονται στο *Γράφημα 8*. Οι λειτουργίες αναγνώρισης προσώπου και PIN ασφαλείας έλαβαν τις υψηλότερες βαθμολογίες ικανοποίησης, με την πλειοψηφία των χρηστών να τις βαθμολογεί με «5: Εξαιρετική». Συνολικά, το γράφημα υπογραμμίζει ότι ενώ οι περισσότεροι χρήστες είναι ικανοποιημένοι με τις λειτουργίες της εφαρμογής, υπάρχουν περιθώρια βελτίωσης σε ορισμένους τομείς για να ανταποκριθούν καλύτερα στις προσδοκίες των χρηστών.

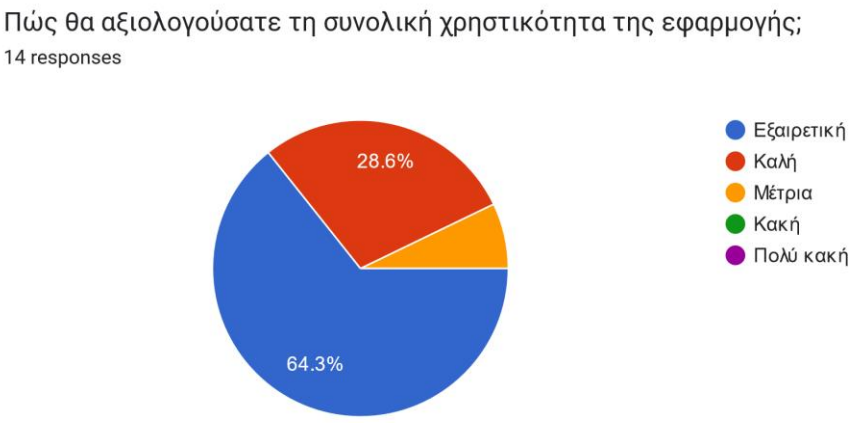


Γράφημα 9 - Ερώτηση για Τυχόν Προβλήματα κατά τη Χρήση της Εφαρμογής

Γράφημα 10 - Περιγραφή Προβλημάτων από Χρήστες

Στο *Γράφημα 9* και *Γράφημα 10* παρουσιάζονται οι απαντήσεις των χρηστών σχετικά με το αν αντιμετώπισαν προβλήματα ή σφάλματα κατά τη χρήση της εφαρμογής. Η πλειοψηφία των χρηστών, ανέφεραν ότι δεν αντιμετώπισαν κανένα πρόβλημα κατά τη χρήση της εφαρμογής. Ωστόσο, το 14,3% των χρηστών ανέφεραν ότι αντιμετώπισαν προβλήματα.

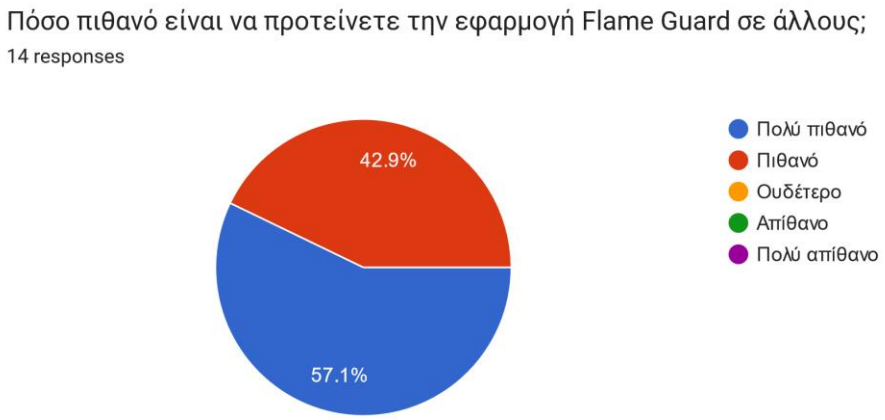
Τα σχόλια των χρηστών περιλαμβάνουν ζητήματα όπως η απουσία επιλογής γλώσσας για Ελληνικά, η επιθυμία για απομακρυσμένη απενεργοποίηση της φύλαξης από την κύρια συσκευή, και διαφορές στην εμπειρία χρήσης μεταξύ τάμπλετ και κινητού. Αυτά τα σχόλια παρέχουν πολύτιμη ανατροφοδότηση για μελλοντικές βελτιώσεις της εφαρμογής.



Γράφημα 11 - Συνολική Αξιολόγηση Χρηστικότητας της Εφαρμογής

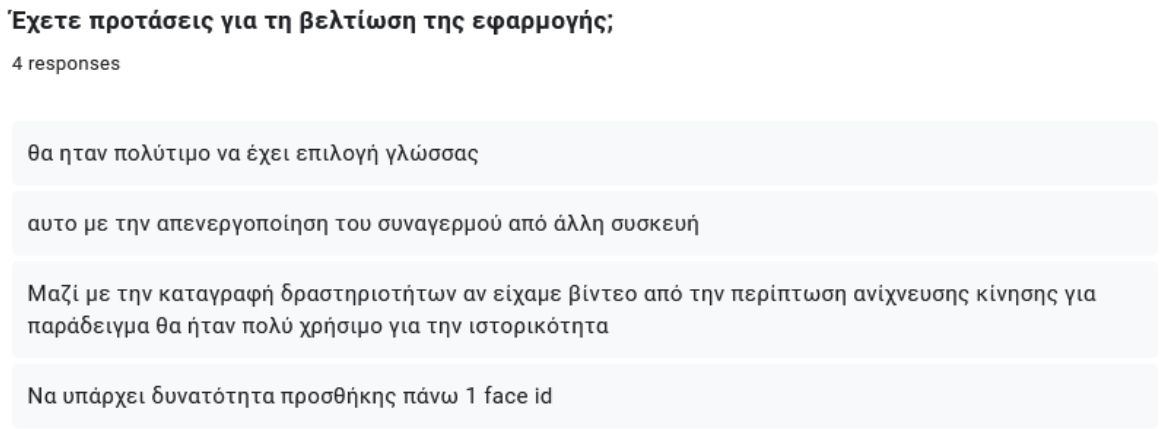
Οι περισσότεροι χρήστες (64.3%) αξιολόγησαν τη χρηστικότητα της εφαρμογής ως εξαιρετική, ενώ το 28.6% την αξιολόγησε ως καλή. Ένα μικρό ποσοστό (7.1%) την χαρακτήρισε ως μέτρια. Αυτές οι αξιολογήσεις δείχνουν ότι η πλειονότητα των

χρηστών είναι πολύ ικανοποιημένοι με την ευκολία χρήσης και την εμπειρία που προσφέρει η εφαρμογή.



Γράφημα 12 - Πιθανότητα Πρότασης της Εφαρμογής σε Άλλους

Η πλειοψηφία των χρηστών δήλωσε ότι είναι πολύ πιθανό να προτείνει την εφαρμογή, ενώ το 42.9% δήλωσε ότι είναι πιθανό να το κάνει. Τα αποτελέσματα αυτά δείχνουν μια υψηλή βαθμολογία ικανοποίησης και εμπιστοσύνης προς την εφαρμογή, ενισχύοντας την αξιοπιστία και την αποδοχή της στους χρήστες.



Γράφημα 13 - Προτάσεις για τη Βελτίωση της Εφαρμογής

Οι χρήστες έχουν προτείνει την προσθήκη δυνατότητας επιλογής γλώσσας για την υποστήριξη πολλών γλωσσών. Επίσης, εξέφρασαν την επιθυμία να μπορούν να απενεργοποιούν τον συναγερμό από διαφορετική συσκευή. Επιπλέον, δόθηκε η ιδέα για την ενσωμάτωση δυνατότητας καταγραφής βίντεο κατά τη διάρκεια ανίχνευσης

κίνησης για την βελτίωση της ιστορικότητας. Τέλος, οι χρήστες πρότειναν την επιλογή προσθήκης περισσότερων από ένα πρόσωπο για την αναγνώριση τους σε περίπτωση ανίχνευσης κίνησης.

Συμπεράσματα Αξιολογήσεων

Τα σχόλια και οι αξιολογήσεις που συγκεντρώθηκαν από τους χρήστες παρέχουν σημαντικές πληροφορίες σχετικά με την απόδοση και τη χρηστικότητα της εφαρμογής Flame Guard. Η πλειοψηφία των χρηστών ανέφερε θετική εμπειρία, με υψηλά επίπεδα ικανοποίησης για βασικά χαρακτηριστικά όπως η ανίχνευση κίνησης, η αναγνώριση προσώπου και οι λειτουργίες PIN ασφαλείας.

Οι χρήστες τόνισαν την ευκολία χρήσης και την αποτελεσματικότητα της εφαρμογής, με την πλειονότητα να βρίσκει διαισθητική τη διεπαφή χρήστη και αξιόπιστες τις λειτουργίες ασφαλείας. Παρά τη συνολική θετική υποδοχή, ορισμένοι χρήστες επεσήμαναν τομείς προς βελτίωση, όπως η προσθήκη υποστήριξης πολλαπλών γλωσσών, η δυνατότητα απομακρυσμένης απενεργοποίησης του συναγερμού και η παροχή δυνατότητας προσθήκης πολλαπλών αναγνωριστικών προσώπου. Αυτές οι προτάσεις είναι πολύτιμες για την καθοδήγηση μελλοντικών βελτιώσεων και τη διασφάλιση ότι η εφαρμογή θα συνεχίσει να ανταποκρίνεται αποτελεσματικά στις ανάγκες των χρηστών.

Συνολικά, οι αξιολογήσεις καταδεικνύουν ότι η Flame Guard είναι μια στιβαρή και φιλική προς το χρήστη εφαρμογή ασφαλείας που ανταποκρίνεται αποτελεσματικά στις ανάγκες των χρηστών, ενώ παρέχει υψηλό επίπεδο ικανοποίησης και αξιοπιστίας. Η αξιολόγηση που συγκεντρώθηκε θα συμβάλει καθοριστικά στην προώθηση περαιτέρω βελτιώσεων και στη διατήρηση των υψηλών προδιαγραφών της εφαρμογής.

6. Συμπεράσματα

Η παρούσα διπλωματική εργασία είχε ως στόχο τον σχεδιασμό, την υλοποίηση και την αξιοπιστία μίας εφαρμογής ψηφιακού συστήματος συναγερμού ασφαλείας για περιπτώσεις κινδύνου, με έμφαση στην αναγνώριση προσώπου, την ανίχνευση κίνησης και τη χρήση της τεχνητής νοημοσύνης. Μέσω της ενσωμάτωσης προηγμένων τεχνολογιών όπως η μηχανική μάθηση και η όραση υπολογιστών, επιτεύχθηκε η δημιουργία μιας εφαρμογής που παρέχει σημαντικές δυνατότητες για την ενίσχυση της προσωπικής και οικιακής ασφάλειας.

Η ανάπτυξη της εφαρμογής επιβεβαίωσε τη δυνατότητα των κινητών τηλεφώνων να λειτουργούν ως πολύτιμα εργαλεία ασφαλείας. Η εφαρμογή, μέσω της χρήσης αλγορίθμων μηχανικής μάθησης, επιδεικνύει υψηλή ακρίβεια στην ανίχνευση και αναγνώριση προσώπων, μειώνοντας τους ψευδείς συναγερμούς και βελτιώνοντας την ασφάλεια των χρηστών.

Κατά τη διάρκεια της ανάπτυξης, αξιολογήθηκαν διάφορα μοντέλα κινητών τηλεφώνων για να διαπιστωθεί η αποτελεσματικότητα της εφαρμογής σε διαφορετικές συσκευές και συνθήκες. Τα αποτελέσματα έδειξαν ότι η εφαρμογή είναι λειτουργική και αποδοτική σε ένα ευρύ φάσμα συσκευών, αν και η απόδοση της αναγνώρισης προσώπου και της ανίχνευσης κίνησης επηρεάζεται από τις συνθήκες φωτισμού και την ποιότητα της κάμερας του κινητού τηλεφώνου.

Η συνολική αξιολόγηση της εφαρμογής από τους χρήστες ήταν θετική, με υψηλά επίπεδα ικανοποίησης και αναγνώριση της αξίας των βασικών λειτουργιών της. Η εφαρμογή έδειξε ότι μπορεί να παρέχει αποτελεσματική και αξιόπιστη προστασία, βελτιώνοντας την προσωπική και οικιακή ασφάλεια μέσω της αξιοποίησης των σύγχρονων τεχνολογιών.

Αυτές οι προτάσεις και τα αποτελέσματα της εργασίας προσφέρουν μια ισχυρή βάση για τη συνεχή ανάπτυξη και βελτίωση της εφαρμογής, διασφαλίζοντας ότι θα συνεχίσει να ανταποκρίνεται αποτελεσματικά στις ανάγκες των χρηστών και θα παρέχει υψηλά επίπεδα ασφάλειας και προστασίας.

6.1 Περιορισμοί

Ένας από τους κύριους περιορισμούς της εφαρμογής είναι η ευαισθησία της σε περιβαλλοντικές συνθήκες. Η απόδοση των αλγορίθμων αναγνώρισης προσώπου και ανίχνευσης κίνησης μπορεί να μειωθεί σε συνθήκες χαμηλού φωτισμού ή σε περιπτώσεις όπου τα πρόσωπα είναι μερικώς καλυμμένα. Επιπλέον, η εφαρμογή απαιτεί σημαντικούς υπολογιστικούς πόρους, γεγονός που μπορεί να περιορίσει τη χρήση της σε παλαιότερες ή λιγότερο ισχυρές συσκευές. Η διαχείριση της ιδιωτικότητας και της ασφάλειας των δεδομένων είναι επίσης κρίσιμη, καθώς η χρήση της τεχνολογίας αναγνώρισης προσώπου και ανίχνευσης κίνησης μέσω κάμερας, δημιουργούν ζητήματα προστασίας προσωπικών δεδομένων που πρέπει να αντιμετωπιστούν με αυστηρά πρωτόκολλα ασφαλείας και συμμόρφωση με τις διεθνείς κανονιστικές απαιτήσεις.

Επιπρόσθετα, λόγω του γεγονότος ότι τα κινητά τηλέφωνα έχουν το κουμπί ενεργοποίησης ενσωματωμένο στη συσκευή, αυτό δημιουργεί ένα αρνητικό στοιχείο για τη συνολική λειτουργικότητα της εφαρμογής. Η χρήση του κουμπιού μπορεί να οδηγήσει σε απενεργοποίηση της εφαρμογής ή της συσκευής, κάτι που αποτελεί σοβαρό εμπόδιο για τη συνεχή παρακολούθηση και προστασία. Αυτή η αδυναμία μπορεί να υπονομεύσει την αξιοπιστία της εφαρμογής σε κρίσιμες στιγμές, όπου η συνεχής λειτουργία είναι απαραίτητη. Για να αντιμετωπιστεί αυτό το πρόβλημα, η χρήση πλαισίων ή βάσεων στήριξης για τα κινητά τηλέφωνα θα ήταν χρήσιμα. Αυτά τα πλαίσια θα μπορούσαν να σχεδιαστούν με τρόπο που να αποτρέπει το πάτημα του κουμπιού ενεργοποίησης, διασφαλίζοντας ότι η συσκευή παραμένει ενεργή και η εφαρμογή λειτουργεί καθ' όλη τη διάρκεια της χρήσης. Επιπλέον, η χρήση τέτοιων βάσεων θα μπορούσε να συμβάλει στη σταθερή τοποθέτηση της συσκευής, βελτιώνοντας την ακρίβεια της ανίχνευσης κίνησης και προσώπων, καθώς και την αξιοπιστία της συνολικής παρακολούθησης. Έτσι, η εφαρμογή θα μπορεί να παρέχει πιο αξιόπιστες και συνεχείς υπηρεσίες ασφαλείας στους χρήστες.

6.2 Μελλοντικές Επεκτάσεις

Θα μπορούσαν να γίνουν αρκετές επεκτάσεις σε διαφορετικά επίπεδα της εφαρμογής, όπως την ασφάλεια δεδομένων, προσβασιμότητα από πολλές συσκευές και τις δυνατότητες της σχετικά με την καλύτερη δυνατή απόδοση της.

Πρώτον, θα ήταν αξιόπιστο να διερευνηθούν και να ενσωματωθούν πιο προηγμένοι αλγόριθμοι μηχανικής μάθησης και βαθιάς μάθησης, με στόχο τη βελτίωση της ακρίβειας και της ταχύτητας αναγνώρισης προσώπων και ανίχνευσης κίνησης. Οι υπάρχοντες αλγόριθμοι μπορούν να αναβαθμιστούν μέσω της χρήσης πιο εξελιγμένων τεχνικών όπως τα νευρωνικά δίκτυα και τα συστήματα ενισχυτικής μάθησης, τα οποία θα επιτρέψουν την ταχύτερη και ακριβέστερη επεξεργασία δεδομένων. Με αυτόν τον τρόπο, η εφαρμογή θα μπορεί να αναγνωρίζει πρόσωπα και κινήσεις με μεγαλύτερη ακρίβεια, μειώνοντας τους ψευδείς συναγερμούς και αυξάνοντας την αξιοπιστία της σε διάφορες συνθήκες. Επίσης, η εκπαίδευση των αλγορίθμων με μεγαλύτερα και πιο ποικιλόμορφα σύνολα δεδομένων μπορεί να συμβάλει τη βελτίωση της απόδοσης και της προσαρμοστικότητας της εφαρμογής σε διάφορα περιβάλλοντα και καταστάσεις.

Δεύτερον, η προσθήκη επιπλέον Internet of Things (IoT) συσκευών θα μπορούσε να ενισχύσει σημαντικά τη λειτουργικότητα και την ευελιξία της εφαρμογής. Η ενσωμάτωση εξωτερικών IP καμερών θα επιτρέψει την επέκταση του πεδίου παρακολούθησης, παρέχοντας περισσότερες γωνίες για την προβολή. Επιπλέον, η χρήση αισθητήρων PIR μπορούν να βελτιώσουν την ακρίβεια της ανίχνευσης κίνησης, ειδικά σε συνθήκες χαμηλού φωτισμού. Η χρήση αισθητήρων για τους πόρτες επίσης μπορούν να επιτρέψουν στους χρήστες να λαμβάνουν ειδοποιήσεις όταν ανοίγονται ή κλείνουν οι πόρτες, αυξάνοντας την ασφάλεια των χώρων τους. Αυτές οι επεκτάσεις θα επιτρέψουν στην εφαρμογή να γίνει ένας ολοκληρωμένος κόμβος ασφαλείας, προσφέροντας ολοκληρωμένες λύσεις μέσω της διασύνδεσης με πολλαπλές συσκευές, ενισχύοντας έτσι την προστασία και την ειδοποίηση σε πραγματικό χρόνο. Ωστόσο, το αρνητικό είναι ότι η αγορά και η εγκατάσταση αυτών των πρόσθετων συσκευών μπορεί να αποτελέσει επιπλέον κόστος για τους χρήστες, γεγονός που θα μπορούσε να έχει αρνητική επίδραση στην αποδοχή της εφαρμογής.

Η ανάπτυξη ελαφρύτερων εκδόσεων της εφαρμογής είναι σημαντική για να διασφαλιστεί η λειτουργικότητά της σε παλαιότερα ή λιγότερο ισχυρά κινητά τηλέφωνα. Αυτό μπορεί να επιτευχθεί μέσω της βελτιστοποίησης του κώδικα και της μείωσης των απαιτήσεων υπολογιστικής ισχύος, διατηρώντας παράλληλα την αποτελεσματικότητα των λειτουργιών της εφαρμογής. Οι χρήστες με παλαιότερα μοντέλα τηλεφώνων θα μπορούν να απολαμβάνουν τα ίδια επίπεδα ασφαλείας χωρίς να χρειάζεται να αναβαθμίσουν τις συσκευές τους. Επιπλέον, η ανάπτυξη μιας εφαρμογής που μπορεί να λειτουργήσει αποδοτικά σε διαφορετικές πλατφόρμες και λειτουργικά συστήματα θα αυξήσει την προσβασιμότητα και την αποδοχή της εφαρμογής από ένα ευρύτερο κοινό.

Η προστασία των δεδομένων των χρηστών επίσης είναι μια από τις σημαντικότερες προκλήσεις για κάθε εφαρμογή που χειρίζεται ευαίσθητες πληροφορίες. Η εφαρμογή αυστηρότερων πρωτοκόλλων ασφαλείας, όπως η κρυπτογράφηση δεδομένων των προσωπικών πληροφοριών, είναι απαραίτητη για την προστασία των δεδομένων των χρηστών. Επιπλέον, η συμμόρφωση με τις διεθνείς προδιαγραφές και κανονισμούς για την ιδιωτικότητα θα ενισχύσει την εμπιστοσύνη των χρηστών και θα διασφαλίσει ότι η εφαρμογή πληροί τις απαιτήσεις για την προστασία των προσωπικών δεδομένων.

Η βελτίωση της ακρίβειας της αναγνώρισης προσώπων σε πολυπολιτισμικά περιβάλλοντα είναι μια άλλη κρίσιμη κατεύθυνση για μελλοντικές επεκτάσεις. Η εκπαίδευση των αλγορίθμων με πιο ποικιλόμορφα σύνολα δεδομένων θα επιτρέψει στην εφαρμογή να αναγνωρίζει με ακρίβεια πρόσωπα από διάφορες εθνικότητες και πολιτισμικά υπόβαθρα. Αυτό θα ενισχύσει την αξιοπιστία της εφαρμογής σε παγκόσμιο επίπεδο, καθιστώντας την πιο προσαρμόσιμη και χρήσιμη για χρήστες από διαφορετικές κουλτούρες και περιοχές. Επιπλέον, η ανάπτυξη δυνατοτήτων πολυγλωσσικής υποστήριξης θα βελτιώσει την εμπειρία χρήσης για τους διεθνείς χρήστες, καθιστώντας την εφαρμογή πιο προσβάσιμη και φιλική προς το χρήστη.

Η προσθήκη νέων λειτουργιών, όπως η ανίχνευση αντικειμένων και η ανάλυση συμπεριφοράς, μπορεί να προσφέρει πιο ολοκληρωμένες λύσεις ασφαλείας. Η ανίχνευση αντικειμένων θα μπορούσε να χρησιμοποιηθεί για τον εντοπισμό ύποπτων αντικειμένων ή αποσκευών, ενώ η ανάλυση συμπεριφοράς θα μπορούσε να βοηθήσει στην αναγνώριση ασυνήθιστων ή ύποπτων κινήσεων.

Αυτές οι λειτουργίες θα μπορούσαν να αυξήσουν την αποτελεσματικότητα της εφαρμογής στην πρόληψη και αντιμετώπιση πιθανών απειλών, προσφέροντας στους χρήστες πιο ολοκληρωμένη και προληπτική προστασία. Η συνεχιζόμενη ανάπτυξη και επέκταση των δυνατοτήτων της εφαρμογής θα διασφαλίσει ότι παραμένει πρωτοπόρος στην παροχή καινοτόμων λύσεων ασφαλείας για κινητές συσκευές.

7. Βιβλιογραφία

[1] anonymos, "Η σημασία των συστημάτων συναγερμού για την προστασία του σπιτιού μας," 28 4 2024. [Online]. Available: http://housealarms24hrs.blogspot.com/.

[2] B. Wu, H. Peng and C. Chen, "A Practical Home Security System via Mobile Phones," 2006.

[3] L. Silver, "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally," Pew Research Center, 2019.

[4] A. Dennon, "What You Need to Know About Facial Recognition Home Security Cameras," Reviews, 2021.

[5] J. H. Nair, P. J. McCullagh and I. Cleland, "Face Recognition and Actuation to Promote Smart Home Security," Springer, 2023.

[6] A. Supe, K. Tajne, A. Bakade, N. Mali and R. Kubal, "Design and Implementation of Smart Home Security System based on GSM Technology," International Journal of Computer Sciences and Engineering, 2018.

[7] I. F. M. &. N. R. A.-D. C. Sarker, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," Springer, 2021.

[8] A. M. TURING, "I.—COMPUTING MACHINERY AND INTELLIGENCE," 1950.

[9] J. McCarthy, M. L. Minsky, N. Rochester and C. E. Shannon, "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence," 1955.

[10] L. Floridi, "AI and Its New Winter: from Myths to Realities," 2020.

[11] M. Campbell, A. H. Jr. and F.-h. Hsu, "Deep Blue," *Artificial Intelligence,* pp. 57-83, 2002.

[12] Y. LeCun, Y. Bengio and G. E. Hinton, "Deep Learning," *nature,* pp. 436-444, 2015.

[13] S. Russell and P. Norvig, "Artificial Intelligence: A Modern Approach, Third Edition," *Elsevier,* 2011.

[14] I. Goodfellow, Y. Bengio and A. Courville, Deep Learning, MIT Press, 2016.

[15] D. G. Lowe, "Object Recognition from Local Scale-Invariant Features," 1999.

[16] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Elsevier,* vol. 51, no. 12, pp. 3448-3470, 2007.

[17] A. S. Ashoor and S. Gore, "Importance of Intrusion Detection System (IDS)," *International Journal of Scientific and Engineering Research,* vol. 2, no. 1, 2011.

[18] S. Z. Li and A. K. Jain, Handbook of Face Recognition, Springer London, 2011.

[19] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," IEEE, 2001.

[20] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition,* pp. 886-893, 2005.

[21] D. Amodei, C. Olah, J. Steinhardt, P. Christiano, J. Schulman and D. Man, "Concrete Problems in AI Safety," 2016. [Online]. Available: https://arxiv.org/pdf/1606.06565. [Accessed 2024].

[22] W. S. McCulloch and W. Pitts, "A Logical Calculus of the Ideas Immanent in Nervous Activity," *Bulletin of Mathematical Biophysics,* vol. 5, no. 4, pp. 115-133, 1943.

[23] D. Rumelhart, G. E. Hinton and R. J. Williams, "Learning Representations by Back-Propagating Errors," *Nature,* pp. 533-536, 1986.

[24] [Online]. Available: https://www.geeksforgeeks.org/artificial-neural-networks-and-its-applications/.

[25] S. Haykin, Neural Networks and Learning Machines, Pearson, 2009.

[26] [Online]. Available: https://www.v7labs.com/blog/convolutional-neural-networks-guide.

[27] K. He, X. Zhang, S. Ren and J. Sun, "Deep Residual Learning for Image Recognition," IEEE, 2016.

[28] [Online]. Available: https://www.v7labs.com/blog/recurrent-neural-networks-guide.

[29] A. L. Samuel, "Some Studies in Machine Learning Using the Game of Checkers," *IBM Journal of Research and Development,* vol. 3, no. 3, pp. 210-229, 1959.

[30] F. Rosenblatt, "The perceptron: A probabilistic model for information storage and organization in the brain.," *Psychological Review,* vol. 65, no. 6, p. 386–408, 1958.

[31] T. H. T. Friedman, The Elements of Statistical Learning, Springer, 2009.

[32] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Timeline_of_machine_learning.

[33] D. Gunning, "Explainable Artificial Intelligence (XAI)," DARPA.

[34] B. D. Lucas and T. Kanade, "An Iterative Image Registration Technique with an Application to Stereo Vision," in *Proceedings of the 7th International Joint Conference on Artificial Intelligence*, 1981.

[35] R. C. Gonzalez and R. E. Woods, Digital Image Processing, Pearson, 2018.

[36] J. Shi and C. Tomasi, "Good Features to Track," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 1994.

[37] H. Aghajan and A. Cavallaro, Multi-Camera Networks: Principles and Applications, Academic Press, 2009.

[38] A. Geiger, P. Lenz and R. Urtasun, "Are We Ready for Autonomous Driving? The KITTI Vision Benchmark Suite," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2012.

[39] [Online]. Available: https://www.nvidia.com/en-gb/glossary/computer-vision/.

[40] M. Satyanarayanan, "The Emergence of Edge Computing," *Computer,* vol. 50, no. 1, pp. 30-39, 2017.

[41] C. Hochreutiner, "The History of Facial Recognition Technologies: How Image Recognition Got So Advanced," Any Connect Academy, 2019.

[42] A. P. Matthew Turk, "Eigenfaces for recognition," MIT Press, 1991.

[43] "ML | Face Recognition Using Eigenfaces (PCA Algorithm)," 24 10 2021. [Online]. Available: https://www.geeksforgeeks.org/ml-face-recognition-using-eigenfaces-pca-algorithm/.

[44] R. Gupta, "Breaking Down Facial Recognition: The Viola-Jones Algorithm," Towards Data Science, 2019.

[45] C. W. Bong, P. Y. Xian and J. Thomas, "Face Recognition and Detection Using Haars Features with Template Matching Algorithm," Springer, 2019.

[46] O. Taban, "Viola Jones Algoritması ile Yüz Tespiti," patron-labs, 2020.

[47] Y.-Q. Wang, "An Analysis of the Viola-Jones Face Detection Algorithm," IPOL Journal - Image Processing On Line, 2013.

[48] A. D. Egorov, A. N. Shtanko and P. E. Minin, "Selection of Viola–Jones algorithm parameters for specific conditions," Springer, 2015.

[49] F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015.

[50] C. Ding and D. Tao, "Robust Face Recognition via Multimodal Deep," IEEE, 2015.

[51] Y. Taigman, M. Yang, M. Ranzato and L. Wolf, "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2014.

[52] K. A. Wahab, L. W. Yew and J. N. Amizam, "Online Attendance System Using Face Recognition," *Engineering Agriculture Science and Technology Journal,* 2022.

[53] G. Guo and N. Zhang, "A survey on deep learning based face recognition," *Computer Vision and Image Understanding,* 2019.

[54] O. M. Parkhi, A. Vedaldi and A. Zisserman, "Deep Face Recognition".

[55] A. K. Jain, L. Hong and S. Pankanti, "Biometric Identification," *Communications of the ACM,* vol. 43, no. 2, pp. 90-98, 2000.

[56] J. Daugman, "igh confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 15, no. 11, pp. 1148-1161, 1993.

[57] P. N. Belhumeur, Joao, P. Hespanha and D. J. Kriegma, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 19, no. 7, 1997.

[58] R. Chellappa, C. L. Wilson and S. Sirohey, "Human and machine recognition of faces: A survey," in *Proceedings of the IEEE*, 1995.

[59] C. Stauffer and W. Grimson, "Adaptive background mixture models for real-time tracking," in *Conference on Computer Vision and Pattern Recognition (CVPR)* , 1999.

[60] A. Fauzi and S. Madenda, "The Motion Detection on Video Surveillance by Using Background Subtraction," *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* 2021.

[61] A. Krizhevsky, I. Sutskever and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," Advances in Neural Information Processing Systems, 2012.

[62] M. Banzi and M. Shiloh, Getting Started with Arduino, Maker Media, 2014.

[63] S. Monk, Programming the Raspberry Pi - Getting Started with Python, Mc Graw Hill Education, 2016.

[64] "AlfredCamera-Features," Alfred Systems Inc., [Online]. Available: https://alfred.camera/features. [Accessed 2024].

[65] "safesmartliving," [Online]. Available: https://www.safesmartliving.com/alfred-camera-review/.

[66] "AtHome Camera," iChano Incorporation, [Online]. Available: https://www.ichano.com/function.html?session_id=undefined.

[67] "Haven: Keep Watch," [Online]. Available: https://guardianproject.github.io/haven/#install.

[68] "Android Studio IDE," Android, [Online]. Available: https://developer.android.com/studio.

[69] "Android Developers Blog," [Online]. Available: https://android-developers.googleblog.com/2023/05/android-studio-io-23-announcing-studio-bot.html.

[70] M. Kumar, "Kotlin vs Java: A Comprehensive Comparison," Medium, 2023.

[71] N. d. Hoog, "Why Sketch is the perfect design tool for developers," Medium, 2014.

[72] "Firebase," Google, [Online]. Available: https://firebase.google.com/. [Accessed 2024].

[73] "TensorFlow Lite," [Online]. Available: https://www.tensorflow.org/lite.

[74] "ML Kit Face detection," Google, [Online]. Available: https://developers.google.com/ml-kit/vision/face-detection.

[75] "CameraX," Jetpack, [Online]. Available: https://developer.android.com/media/camera/camerax.

[76] "Our API: the basics," Twilio, [Online]. Available: https://www.twilio.com/docs/iam/api.

[77] "IEEE Standard for Software Quality," *IEEE Computer Society,* 2026.

[78] N. Singla, "Motion Detection Based on Frame Difference Method," *International Journal of Information & Computation Technology,* vol. 4, no. 15, pp. 1559-1565, 2014.