Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Επαλήθευση της ταυτότητας ενός χρήστη με τη χρήση τεχνολογιών αναγνώρισης προσώπου** **Authentication of a user using facial recognition technologies**
Ονοματεπώνυμο Φοιτητή	**Δημήτριος Σταμουλακάτος**
Πατρώνυμο	**Χαρίδημος**
Αριθμός Μητρώου	**ΜΠΠΛ 19053**
Επιβλέπων	**Ευάγγελος Σακκόπουλος, Αναπληρωτής Καθηγητής**

Ιούνιος 2023

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Ευάγγελος Σακκόπουλος Αναπληρωτής Καθηγητής	Ευθύμιος Αλέπης Αναπληρωτής Καθηγητής	Διονύσιος Σωτηρόπουλος Επίκουρος Καθηγητής

Σύνοψη

Η τεχνολογία αναγνώρισης προσώπου**(facial recognition)** είναι ένας από τους πιο διαδεδομένους τρόπους επαλήθευσης της ταυτότητας. Η ανάπτυξη της τεχνητής νοημοσύνης καθώς και η ανάγκη για μεγαλύτερη ασφάλεια αλλά και ευκολία, έδωσε ώθηση σε ερευνητές αλλά και εταιρείες παροχής λογισμικού να αναπτύξουν νέους τρόπος για την επαλήθευση της ταυτότητα ενός ατόμου.

Στο διαδίκτυο μέχρι τις μέρες μας ο πιο διαδεδομένος τρόπος επαλήθευσης της ταυτότητας ενός χρήστη μιας εφαρμογής ήταν μέσω του προσωπικού αναγνωριστικού και του κωδικού πρόσβασής. Ένα από τα κύρια μειονεκτήματα αυτής της μεθόδου αφορούσε το κομμάτι της ασφάλειας καθώς ήταν πιθανό να παραβιαστούν σχετικά εύκολα οι προσωπικοί κωδικοί. Ακόμα, η επαλήθευση της ταυτότητας με την χρήση τεχνολογιών αναγνώρισης προσώπου διευκόλυνε σημαντικά την διαδικασία επαλήθευσης καθώς πλέον δεν απαιτούνταν προσωπικοί κωδικοί παρά μόνο μια φωτογραφία ή η ενεργοποίηση της κάμερες της συσκευής.

Η τεχνολογία αναγνώρισης προσώπου αναπτύσσεται με γρήγορους ρυθμούς τα τελευταία χρόνια. Μαζί της αναπτύσσονται και ερωτήματα που αφορούν την εφαρμογής της αλλά και το πως ενδέχεται να επηρεάσει θεμελιώδη δικαιώματα όπως της ιδιωτικότητας, της προστασίας των προσωπικών δεδομένων καθώς και τις πολιτικές ελευθερίες.

Η παρούσα διπλωματική εργασία παρουσιάζει μια λύση επαλήθευσης της ταυτότητας με την χρήση της τεχνολογίας αναγνώρισης προσώπου. Συγκεκριμένα χρησιμοποιεί την προσέγγιση που παρέχεται μέσω του SDK της FaceTec.

Η εφαρμογή αποτελείται από ένα authentication system που έχει ως προϋπόθεση ο χρήστης να έχει εγγραφεί στο σύστημα με την χρήση του προσώπου του έτσι ώστε να είναι δυνατή η επαλήθευση του. Η εφαρμογή συγκρίνει το πρόσωπο του χρήστη με την φωτογραφία που έχει αποθηκευτεί κατά την εγγραφή του χρήστη. Αν η επαλήθευση πραγματοποιηθεί επιτυχώς ο χρήστης πραγματοποιεί την είσοδο στην εφαρμογή.

Abstract

Facial recognition technology is one of the most widespread ways of verifying identity. The development of artificial intelligence and the need for greater security and convenience has prompted researchers and software companies to develop new ways of verifying a person's identity.

On the internet until nowadays the most common way of authenticating a user of an application was through personal ID and password. One of the main disadvantages of this method was related to the security aspect as it was possible to break personal passwords relatively easily. Still, authentication using facial recognition technologies greatly facilitated the verification process as no personal passwords were now required but only a photo or activation of the device's camera.

Facial recognition technology has been developing rapidly in recent years. Along with it, questions are developing regarding its implementation and how it may affect fundamental rights such as privacy, data protection and civil liberties.

This thesis presents an identity verification solution using facial recognition technology. Specifically, it uses the approach provided through FaceTec's SDK.

The application consists of an authentication system that requires the user to be registered in the system using his/her face so that the user can be verified. The application compares the user's face with the photo stored during the user's registration. If the verification is successfully performed the user is logged into the application.

Πίνακας Περιεχομένων

Κατάλογος Εικόνων:

Κατάλογος Πινάκων:

Κεφάλαιο 1

1. Εισαγωγή

Η παρούσα μεταπτυχιακή διατριβή έχει ως στόχο να παρουσιάσει έναν εναλλακτικό τρόπο επαλήθευσης της ταυτότητας ενός ατόμου με την χρήση της τεχνολογίας αναγνώρισης προσώπου. Μέσω του SDK που παρέχει η FaceTec και την κατάλληλη εξατομίκευση και παραμετροποίηση επιχειρείται να παρουσιαστεί η διαδικασία η οποία είναι αναγκαίο να ακολουθήσει ένα χρήστης προκείμενου να επαληθεύσει την ταυτότητα του έτσι ώστε να συνδεθεί στην εφαρμογή.

Η αξία των τεχνολογιών αναγνώρισης προσώπου είναι τεράστια. Καθημερινά, εκατομμύρια άνθρωποι χρησιμοποιούν συστήματα και εφαρμογές που έχουν ενσωματώσει την συγκεκριμένη τεχνολογία. Από τον προσωπικό μας υπολογιστή έως προηγμένα συστήματα ασφαλείας στη βιομηχανία ή σε χώρους που απαιτούνται υψηλά μέτρα ασφαλείας η επαλήθευση της ταυτότητας ενός ατόμου γίνεται με την χρήση εφαρμογών και συστημάτων που έχουν την ικανότητα μέσω βιομετρικών στοιχείων να πραγματοποιούν την επαλήθευση.

Όμως, οι παραπάνω εργασίες και τα αντίστοιχα συστήματα απαιτούν ασφάλεια και ακρίβεια. Ακόμα πρέπει να λάβουμε υπόψιν μας ότι η δημιουργία τους χρειάστηκε χρόνια ερευνών καθώς είναι μια επίπονη και πολύπλοκη διαδικασία. Η τεχνολογία αναγνώρισης προσώπου αποτελεί ένα μέρος ενός ευρύτερου κλάδου που μπήκε στην ζωή μας τα τελευταία χρόνια και εξελίσσεται συνεχώς, αυτού της τεχνητής νοημοσύνης. Η εξέλιξη του κλάδου που γίνεται με εντυπωσιακούς ρυθμούς είναι πιθανό να δώσει και απάντηση σε ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζει, όπως της ασφάλειας των συστημάτων και της ιδιωτικότητας των πολιτών.

Για να είναι πιο εύκολη η παρουσίαση της παραπάνω τεχνολογίας επιλέξαμε να γίνει με την χρήση του SDK της FaceTec έτσι ώστε μέσω ενός συστήματός που λειτουργεί να είναι πιο ξεκάθαρές οι δυνατότητες που παρέχουν τα λογισμικά που χρησιμοποιούν την τεχνολογία αναγνώρισης προσώπου για την επαλήθευση της ταυτότητας.

Στα κεφάλαιο 2 θα παρουσιάσουμε εν συντομία την ιστορική εξέλιξη του τομέα της αναγνώρισης προσώπου καθώς και κάποιες βασικές έννοιες που είναι απαραίτητες για την κατανόηση του πεδίου. Στο κεφάλαιο 3 θα αναλύσουμε τις βασικές τεχνολογίες που χρησιμοποιήθηκαν για την υλοποίηση. Στο κεφαλαίο 4 θα παρουσιάσουμε την ανάλυση αλλά και το σχεδιασμό του συστήματος μας. Στο κεφάλαιο 5 θα παρουσιάσουμε συγκεκριμένα κρίσιμα σημεία της υλοποίηση, ενώ στο κεφάλαιο 6 θα παρουσιάσουμε τα συμπεράσματα και πιθανές μελλοντικές επεκτάσεις.

1.2 Ανασκόπηση πεδίου - Σύντομη Περιγραφή

Ο τομέας ο οποίος ασχολείται με την έρευνα πάνω στην τεχνολογία αναγνώρισης προσώπου έχει αποκτήσει τεράστια δυναμική τα τελευταία χρόνια. Η τεχνολογία αυτή έχει τη δυνατότητα να εντοπίζει και να ταυτοποιεί άτομα από ζωντανό ή καταγεγραμμένο βίντεο ή φωτογραφίες χρησιμοποιώντας τα χαρακτηριστικά του προσώπου τους, καθιστώντας την απαραίτητο εργαλείο για σκοπούς ασφάλειας, ταυτοποίησης και αυθεντικοποίησης.

Η αυξανόμενη ζήτηση για προηγμένα συστήματα ταυτοποίησης της ταυτότητας με την χρήση βιομετρικών εργαλείων σε διάφορους κλάδους, όπως η βιομηχανία, οι δημόσιες υπηρεσίες, οι τραπεζικές και χρηματοπιστωτικές υπηρεσίες, καθώς και το λιανικό και ηλεκτρονικό εμπόριο, οδηγεί στην ολοένα και μεγαλύτερη ανάπτυξη της αγοράς εφαρμογών και συστημάτων αναγνώρισης προσώπου.

Οι προκλήσεις που αντιμετωπίζει το πεδίο της αναγνώρισης προσώπου είναι πολλές. Πέρα από αυτήν της ασφάλειας που προαναφέρθηκε μια δεύτερη είναι αυτή της ακρίβειας. Αν και η τεχνολογία έχει βελτιωθεί σημαντικά τα τελευταία χρόνια, εξακολουθεί να είναι επιρρεπής σε σφάλματα. Η ακρίβεια των αλγορίθμων αναγνώρισης προσώπου μπορεί να επηρεαστεί από παράγοντες όπως ο φωτισμός, η πόζα και οι εκφράσεις του προσώπου του ατόμου. Αυτό μπορεί να οδηγήσει σε ψευδείς επαληθεύσεις. Οι λανθασμένες ταυτίσεις μπορεί να έχουν σοβαρές συνέπειες, που αφορούν από τα προσωπικά δεδομένα έως θέματα ασφάλειας κρατών.

Παρόλα αυτά είναι σημαντικό να τονίσουμε ότι η ανάπτυξη της τεχνολογίας αναγνώρισης προσώπου βρίσκεται ακόμη σε πρώιμο στάδιο και υπάρχουν πολλές προκλήσεις που πρέπει να αντιμετωπιστούν προτού η τεχνολογία υιοθετηθεί ευρέως. Η ακρίβεια, η μεροληψία, η προστασία της ιδιωτικής ζωής, η νομική ρύθμιση και οι ηθικές ανησυχίες αποτελούν σημαντικές προκλήσεις που πρέπει να ξεπεραστούν. Οι οργανισμοί, τα ερευνητικά κέντρα και οι εταιρείες που εργάζονται σε αυτόν τον τομέα, ερευνούν και αναπτύσσουν τεχνολογίες και συστήματα είναι αναγκαίο να δίνουν προτεραιότητα σε ηθικά ζητήματα και ζητήματα που αφορούν τα προσωπικά δεδομένα καθώς επίσης είναι σημαντικό να υπόκεινται σε συνέχεις ελέγχους.

1.3 Βασικές έννοιες

Αναγνώριση προσώπου: Η αναγνώριση προσώπου είναι μια βιομετρική τεχνολογία που χρησιμοποιεί χαρακτηριστικά του προσώπου για την αναγνώριση ή την επαλήθευση της ταυτότητας ενός ατόμου. Η τεχνολογία αυτή αναλύει τα χαρακτηριστικά του προσώπου, όπως η απόσταση μεταξύ των ματιών, το σχήμα της μύτης και το μέγεθος του στόματος, για να δημιουργήσει ένα πρότυπο προσώπου.

Βιομετρική πιστοποίηση ταυτότητας: Ο βιομετρικός έλεγχος ταυτότητας είναι μια διαδικασία ασφαλείας που χρησιμοποιεί βιομετρικά δεδομένα, όπως αναγνώριση προσώπου ή τα δακτυλικά αποτυπώματα , για την επαλήθευση της ταυτότητας ενός ατόμου.

Ανίχνευση ζωντάνιας: Η ανίχνευση ζωντάνιας είναι μια τεχνολογία που χρησιμοποιείται για την πρόληψη της απάτης στη βιομετρική πιστοποίηση ταυτότητας. Η τεχνολογία αυτή διασφαλίζει ότι το άτομο που παρέχει βιομετρικά δεδομένα είναι ένας πραγματικός άνθρωπος και όχι μια στατική εικόνα ή μια μάσκα.

FaceTec: Η FaceTec είναι μια εταιρεία ανάπτυξης λογισμικού που ειδικεύεται στην τεχνολογία αναγνώρισης προσώπου. Προσφέρει προηγμένα χαρακτηριστικά ασφαλείας, όπως η τρισδιάστατη ανίχνευση ζωντάνιας και η προστασία από την πλαστογράφηση.

1.4 Ιστορική εξέλιξη της τεχνολογίας αναγώρισης προσώπου

Η τεχνολογία αναγνώρισης προσώπου έχει σημειώσει αξιοσημείωτη εξέλιξη τα τελευταία χρόνια, αλλάζοντας τον τρόπο με τον οποίο μπορεί να γίνει πλέον η επαλήθευση της ταυτότητας ενός ατόμου καθώς επίσης και την ασφάλεια με την όποια αυτή μπορεί να πραγματοποιηθεί. Με τη χρήση εξελιγμένων αλγορίθμων και της τεχνητής νοημοσύνης, η τεχνολογία αυτή μπορεί να αναγνωρίζει και να πιστοποιεί άτομα με βάση τα μοναδικά χαρακτηριστικά του προσώπου τους πράγμα το οποίο προσφέρει τόσο ασφάλεια όσο και ευκολία στην διαδικασία επαλήθευσης της ταυτότητας ενός ατόμου.

Η απαρχή της τεχνολογίας αναγνώρισης προσώπου χρονολογείται από τα μέσα της δεκαετίας του 1960, όταν οι ερευνητές άρχισαν να ερευνούν τρόπους για την αναγνώριση προσώπου μέσω υπολογιστή. Αρχικά, τα συστήματα αυτά βασίζονταν στη χειροκίνητη κωδικοποίηση των χαρακτηριστικών του προσώπου, με αποτέλεσμα την περιορισμένη ακρίβεια και αποτελεσματικότητα. Οι πρώτες μέθοδοι χρησιμοποιούσαν απλά γεωμετρικά μοντέλα και τεχνικές αντιστοίχισης προτύπων, θέτοντας τα θεμέλια για τις μετέπειτα εξελίξεις.

Τη δεκαετία του 1980 σημειώθηκε μια σημαντική ανακάλυψη με τις αυτοματοποιημένες τεχνικές εξαγωγής χαρακτηριστικών προσώπου. Προσεγγίσεις όπως η μέθοδος eigenface, η οποία χρησιμοποίησε την ανάλυση κύριων συνιστωσών (PCA), επέτρεψε την εξαγωγή και αναπαράσταση των βασικών χαρακτηριστικών του προσώπου ως διανύσματα. Αυτές οι τεχνικές έθεσαν τις βάσεις για πιο ισχυρά και ακριβή συστήματα αναγνώρισης προσώπου.

Στα τέλη της δεκαετίας του 1990 και στις αρχές της δεκαετίας του 2000, τα νευρωνικά δίκτυα ενσωματώθηκαν στους αλγορίθμους αναγνώρισης προσώπων, φέρνοντας επανάσταση στον τομέα. Τα συνελικτικά νευρωνικά δίκτυα (CNN) έπαιξαν καθοριστικό ρόλο διευκολύνοντας την αυτοματοποιημένη εκμάθηση χαρακτηριστικών. Τα μοντέλα αναγνώρισης προσώπου που βασίζονται σε CNN επέδειξαν ανώτερες επιδόσεις στο χειρισμό των διακυμάνσεων στις συνθήκες φωτισμού, τη στάση και τις εκφράσεις του προσώπου.

Οι εξελίξεις στη μηχανική μάθηση και τους αλγορίθμους βαθιάς μάθησης βελτίωσαν σημαντικά τις δυνατότητες των συστημάτων αναγνώρισης προσώπου. Η διαθεσιμότητα δεδομένων μεγάλης κλίμακας, όπως το LFW (Labeled Faces in the Wild) και το MegaFace, διευκόλυνε την εκπαίδευση μοντέλων βαθιάς μάθησης, με αποτέλεσμα σημαντικές βελτιώσεις στην ακρίβεια και την ανθεκτικότητα. Αρχιτεκτονικές τελευταίας τεχνολογίας, όπως το VGGNet, το ResNet και το FaceNet, έσπρωξαν περαιτέρω τα όρια της τεχνολογίας αναγνώρισης προσώπων.

Για να ξεπεραστούν οι περιορισμοί των παραδοσιακών συστημάτων αναγνώρισης προσώπου 2D, οι ερευνητές ανέπτυξαν την τεχνολογία αναγνώρισης προσώπου 3D. Αυτά τα συστήματα συλλαμβάνουν πληροφορίες βάθους είτε μέσω εξειδικευμένων αισθητήρων είτε με την ανακατασκευή τρισδιάστατων μοντέλων από πολλαπλές εικόνες 2D. Με την ενσωμάτωση των νέων τεχνολογιών, η τρισδιάστατη αναγνώριση προσώπου πέτυχε μεγαλύτερη ακρίβεια, ιδίως σε πολύπλοκες καταστάσεις. Ακόμα προσέφερε μεγαλύτερη ασφάλεια αλλά και πλήθος νέων εφαρμογών ιδιαίτερα στο τομέα της ασφάλειας.

Οι εφαρμογές της τεχνολογίας αναγνώρισης προσώπου στην ασφάλεια είναι τεράστιες. Έχει φέρει επανάσταση στα συστήματα ελέγχου πρόσβασης, επιτρέποντας την ασφαλή και εύκολη πιστοποίηση ταυτότητας σε διάφορα περιβάλλοντα. Τα αεροδρόμια, τα κινητά τηλέφωνα, οι τράπεζες καθώς και περιοχές υψηλής ασφάλειας χρησιμοποιούν την αναγνώριση προσώπου για να ενισχύσουν την ασφάλεια και να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση.

Το μέλλον της τεχνολογίας αναγνώρισης προσώπου είναι πολλά υποσχόμενο αλλά κρύβει και κινδύνους. Η τρέχουσα έρευνα αποσκοπεί στη βελτίωση της ακρίβειας και της ποιότητας καθώς και ζητημάτων που αφορούν την ασφάλεια και τα προσωπικά δεδομένα. Είναι όμως μια διαδικασία που έχει να διανύσει ακόμα πολύ δρόμο. Οι εφαρμογές της καλύπτουν διάφορους τομείς, φέρνοντας επανάσταση στην ασφάλεια, τον έλεγχο πρόσβασης και τη συναισθηματική ανάλυση αλλά ταυτόχρονα οι ηθικές ανησυχίες και τα ζητήματα προστασίας της ιδιωτικής ζωής παραμένουν σημαντικά.

ΚΕΦΑΛΑΙΟ 2

2. Απαιτήσεις και τεχνολογίες του συστήματος

2.1 HTML

Η HTML (Hypertext Markup Language) είναι μια τυπική γλώσσα σήμανσης που χρησιμοποιείται για τη δόμηση του περιεχομένου σε εφαρμογές ιστού. Παρέχει την δυνατότητα της οργάνωσης και παρουσίασης κειμένων, εικόνων και άλλων μέσων. Η HTML χρησιμοποιεί μια σειρά από ετικέτες για να καθορίσει τη δομή και τη μορφοποίηση του περιεχομένου μιας ιστοσελίδας ή μιας web εφαρμογής, όπως επικεφαλίδες, παραγράφους, λίστες και συνδέσμους. Οι ετικέτες περικλείονται σε αγκύλες και υποδεικνύουν την αρχή και το τέλος ενός στοιχείου. Τα χαρακτηριστικά παρέχουν πρόσθετες πληροφορίες σχετικά με ένα στοιχείο, όπως το χρώμα του κειμένου ή τη διεύθυνση URL ενός συνδέσμου.

Είναι απαραίτητη για την ανάπτυξη ιστοσελίδων ή web εφαρμογών και χρησιμοποιείται συχνά σε συνδυασμό με άλλες τεχνολογίες όπως η Cascading Style Sheets (CSS) και η JavaScript. Με την HTML, οι προγραμματιστές μπορούν να δημιουργήσουν web εφαρμογές καλά δομημένες και εύκολες στην πλοήγηση για τους χρήστες.

2.2 CSS

Η CSS (Cascading Style Sheets) είναι μια γλώσσα φύλλων ύφους που χρησιμοποιείται για την παρουσίαση μιας ιστοσελίδας ή web εφαρμογής. Με την CSS, οι προγραμματιστές μπορούν να ελέγχουν τη διάταξη, τη μορφοποίηση και το χρώμα των στοιχείων της εφαρμογής και να δημιουργούν οπτικά ελκυστικά στοιχεία .

Η CSS λειτουργεί με τη χρήση επιλογέων για τη επιλογή συγκεκριμένων στοιχείων HTML και την εφαρμογή συγκριμένων στυλ σε αυτά τα στοιχεία. Για παράδειγμα, ένας προγραμματιστής μπορεί να χρησιμοποιήσει την CSS για να αλλάξει όλες τις επικεφαλίδες σε μια ιστοσελίδα και να εφαρμόσει μια συγκεκριμένη γραμματοσειρά και χρώμα σε αυτές.

Επιτρέπει στους προγραμματιστές να διαχωρίζουν την παρουσίαση μιας ιστοσελίδας από το περιεχόμενό της διευκολύνοντας τη διαχείριση και τη συντήρηση σύνθετων εφαρμογών ιστού.

2.3 JavaScript

Η JavaScript είναι μια διερμηνευμένη γλώσσα προγραμματισμού που επιτρέπει στους προγραμματιστές να δημιουργούν διαδραστικές web εφαρμογές και ιστοσελίδες.

Με τη JavaScript, οι προγραμματιστές μπορούν να χειρίζονται και να ενημερώνουν το περιεχόμενο μιας ιστοσελίδας ή εφαρμογής σε πραγματικό χρόνο, να ανταποκρίνονται σε συμβάντα του χρήστη, όπως το πάτημα ενός κουμπιού, και να δημιουργούν σύνθετα κινούμενα στοιχεία και οπτικά εφέ. Η JavaScript είναι μια ευέλικτη γλώσσα που μπορεί να χρησιμοποιηθεί τόσο στην πλευρά του χρήστη (στο πρόγραμμα περιήγησης) όσο και στην πλευρά του διακομιστή με τεχνολογίες όπως το Node.js, γεγονός που την καθιστά βασική τεχνολογία για τη δημιουργία ευέλικτων, διαδραστικών εφαρμογών ιστού.

Η JavaScript είναι μια ευέλικτη και ισχυρή γλώσσα, με ένα ευρύ φάσμα βιβλιοθηκών και frameworks που είναι διαθέσιμα στους προγραμματιστές. Αποτελεί βασικό εργαλείο για τη δημιουργία

σύγχρονων ιστοσελίδων και εφαρμογών. Ορισμένες δημοφιλείς βιβλιοθήκες και frameworks της JavaScript είναι: jQuery, React, Angular και Vue.js.

Είναι μια γλώσσα προγραμματισμού που εξελίσσεται συνεχώς, με νέα χαρακτηριστικά και δυνατότητες να προστίθενται τακτικά. Η γλώσσα υποστηρίζεται από όλα τα μεγάλα προγράμματα περιήγησης ιστού, γεγονός που την καθιστά μια ευρέως χρησιμοποιούμενη και σημαντική τεχνολογία στον τομέα της ανάπτυξης ιστοσελίδων και web εφαρμογών.

2.4 Rest API

Το REST (Representational State Transfer) είναι ένα αρχιτεκτονικό στυλ λογισμικού για τη δημιουργία διαδικτυακών υπηρεσιών. Οι RESTful υπηρεσίες ιστού χρησιμοποιούν το πρωτόκολλο HTTP για την υποβολή αιτημάτων και τη λήψη απαντήσεων. Το REST είναι ένα σύνολο κατευθυντήριων γραμμών και αρχών που καθορίζουν τον τρόπο με τον οποίο πρέπει να σχεδιάζονται και να υλοποιούνται οι υπηρεσίες ιστού.

Τα RESTful APIs (Application Programming Interfaces - Διεπαφές προγραμματισμού εφαρμογών) κατασκευάζονται με τη χρήση της αρχιτεκτονικής REST. Παρέχουν έναν τρόπο επικοινωνίας των εφαρμογών λογισμικού μεταξύ τους μέσω του διαδικτύου. Τα RESTful APIs χρησιμοποιούν μεθόδους HTTP (GET, POST, PUT, DELETE) για τη δημιουργία, ανάγνωση, ενημέρωση και διαγραφή πόρων.

Οι κύριες αρχές του REST περιλαμβάνουν:

Αρχιτεκτονική πελάτη-εξυπηρετητή: Ο πελάτης και ο διακομιστής διαχωρίζονται μεταξύ τους, επιτρέποντας μεγαλύτερη επεκτασιμότητα και ευελιξία.

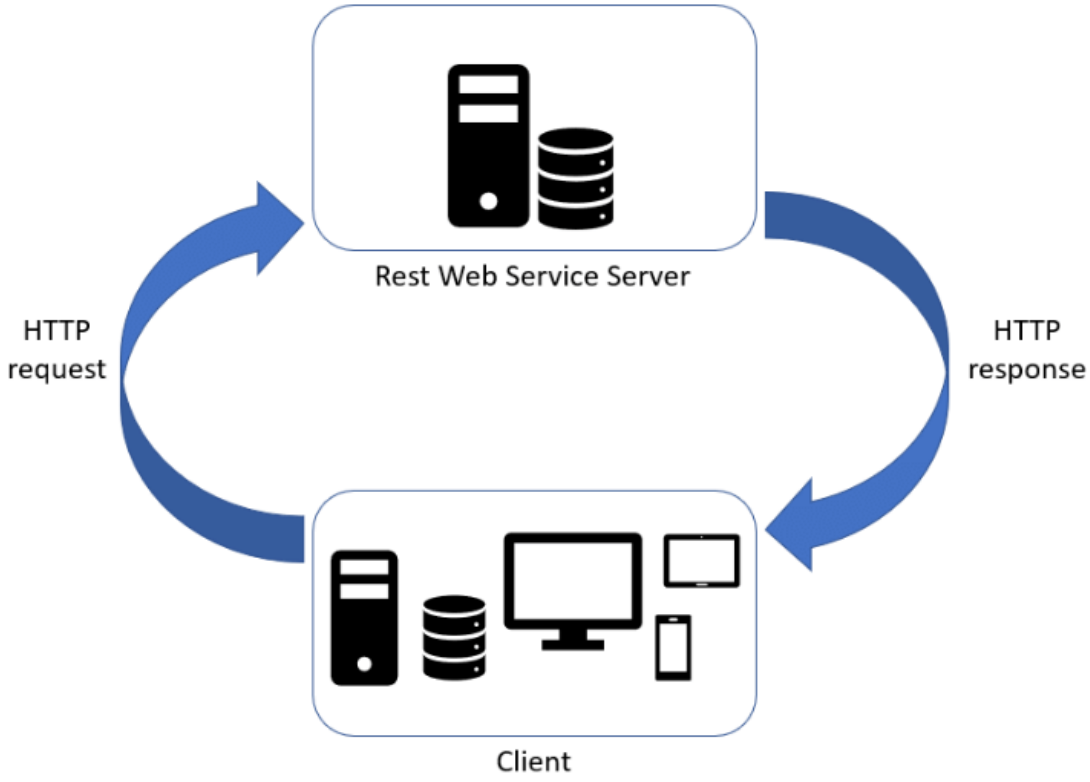
Ανεξαρτησία κατάστασης: Κάθε αίτημα από τον πελάτη προς τον διακομιστή περιέχει όλες τις απαραίτητες πληροφορίες ώστε ο διακομιστής να κατανοήσει και να επεξεργαστεί το αίτημα του πελάτη. Ο διακομιστής δεν χρειάζεται να παρακολουθεί την κατάσταση του πελάτη.

Δυνατότητα προσωρινής αποθήκευσης: Οι απαντήσεις από το διακομιστή μπορούν να αποθηκευτούν στην προσωρινή μνήμη του πελάτη, βελτιώνοντας την απόδοση και μειώνοντας την κυκλοφορία του δικτύου.

Ομοιόμορφη διεπαφή: Η διεπαφή μεταξύ του πελάτη και του διακομιστή είναι τυποποιημένη, διευκολύνοντας τους προγραμματιστές να κατανοήσουν και να χρησιμοποιήσουν το API.

Πολυεπίπεδο σύστημα: Το σύστημα αποτελείται από πολλαπλά επίπεδα, επιτρέποντας μεγαλύτερη ευελιξία και επεκτασιμότητα.

Τα RESTful APIs χρησιμοποιούνται ευρέως στην ανάπτυξη ιστού και χρησιμοποιούνται για τη δημιουργία ενός ευρέος φάσματος υπηρεσιών ιστού, από απλή ανάκτηση δεδομένων έως σύνθετες εφαρμογές ιστού. Είναι εξαιρετικά κλιμακούμενες και ευέλικτες, γεγονός που τις καθιστά δημοφιλή επιλογή για τη δημιουργία σύγχρονων υπηρεσιών ιστού.



Εικόνα 1: Αρχιτεκτονική Rest Api

2.5 Typescript

Η TypeScript είναι ένα υπερσύνολο της γλώσσας προγραμματισμού JavaScript, που αναπτύχθηκε από τη Microsoft. Προσθέτει πρόσθετα χαρακτηριστικά στη JavaScript, όπως προαιρετική στατική τυποποίηση, αντικειμενοστραφή προγραμματισμό βασισμένο σε κλάσεις και καλύτερη υποστήριξη για εφαρμογές μεγάλης κλίμακας.

Η TypeScript επιτρέπει στους προγραμματιστές να γράφουν κώδικα που είναι πιο εύκολο να διαβαστεί, να συντηρηθεί και να αποσφαλματωθεί.

Έχει σχεδιαστεί ώστε να είναι συμβατή με τον υπάρχοντα κώδικα και τις βιβλιοθήκες της JavaScript, καθιστώντας εύκολη την ενσωμάτωσή της σε υπάρχοντα έργα. Υποστηρίζεται επίσης από δημοφιλή εργαλεία επεξεργασίας κώδικα, όπως το Visual Studio Code, το οποίο παρέχει έξυπνη συμπλήρωση κώδικα, έλεγχο σφαλμάτων και υποστήριξη εντοπισμού σφαλμάτων.

Ένα από τα βασικά πλεονεκτήματα της TypeScript είναι η υποστήριξή διεπαφών και κλάσεων, οι οποίες επιτρέπουν στους προγραμματιστές να ορίζουν σύνθετες δομές δεδομένων και αντικείμενα

με πιο δομημένο και ευανάγνωστο τρόπο. Αυτό διευκολύνει τη συντήρηση και την ενημέρωση του κώδικα καθώς αυξάνεται η πολυπλοκότητά του.

Η TypeScript γίνεται ολοένα και πιο δημοφιλής μεταξύ των προγραμματιστών, ιδίως εκείνων που εργάζονται σε εφαρμογές μεγάλης κλίμακας. Η ευκολία χρήσης της, το ισχυρό σύστημα τυποποίησης και η ικανότητά της να ενσωματώνεται με τον υπάρχοντα κώδικα JavaScript την καθιστούν ένα ισχυρό εργαλείο για τη σύγχρονη ανάπτυξη εφαρμογών.

2.6 Εργαλεία ανάπτηξης κώδικα

Η ανάπτυξη λογισμικού, απαιτεί την ύπαρξη κατάλληλων εργαλείων έτσι ώστε να είναι εφικτή η ανάπτυξη εφαρμογών και συστημάτων. Μεταξύ του πλήθους των διαθέσιμων επιλογών, επιλέξαμε το IntelliJ και το Visual Studio Code για την υλοποίηση του έργου μας.

IntelliJ

Το IntelliJ, που αναπτύχθηκε από την JetBrains, είναι ένα ολοκληρωμένο περιβάλλον ανάπτυξης (IDE) ειδικά σχεδιασμένο για να καλύπτει τις ανάγκες ανάπτυξης λογισμικού. Το πλούσιο σε δυνατότητες περιβάλλον του παρέχει ένα εύχρηστο περιβάλλον εργασίας, έξυπνες προτάσεις κώδικα και ισχυρές δυνατότητες αποσφαλμάτωσης, καθιστώντας το μια από τις πρώτες επιλογές για τους προγραμματιστές παγκοσμίως.

Το IntelliJ προσφέρει μια καθαρή και καλά οργανωμένη διεπαφή χρήστη που επιτρέπει στους προγραμματιστές να περιηγηθούν αβίαστα στα έργα τους. Με τις λειτουργίες συμπλήρωσης κώδικα με επίγνωση περιβάλλοντος και έξυπνης πλοήγησης, μπορείτε να γράφετε κώδικα ταχύτερα και με μεγαλύτερη ακρίβεια.

Ακόμα, ένα από τα χαρακτηριστικά που ξεχωρίζουν στο IntelliJ είναι οι έξυπνες δυνατότητες ανάλυσης κώδικα και αναδιαμόρφωσης. Μπορεί να εντοπίσει πιθανά σφάλματα, να προτείνει βελτιώσεις και να αναδιατυπώσει αυτόματα τον κώδικά σας, βελτιώνοντας την ποιότητα και τη συντήρηση του.

Το IntelliJ συνοδεύεται από μια τεράστια σειρά ενσωματωμένων εργαλείων και πρόσθετων προγραμμάτων που επεκτείνουν τη λειτουργικότητά του. Εάν χρειάζεστε υποστήριξη για συστήματα ελέγχου εκδόσεων, εργαλεία κατασκευής ή frameworks για τεστς, το IntelliJ σας καλύπτει, παρέχοντας μια απρόσκοπτη εμπειρία ανάπτυξης.

Visual Studio Code

Το Visual Studio Code, που αναπτύχθηκε από τη Microsoft, έγινε γρήγορα ένα από τα πιο δημοφιλή εργαλεία των προγραμματιστών. Πρόκειται για έναν ελαφρύ και ευέλικτο επεξεργαστή κώδικα που προσφέρει ένα ευρύ φάσμα χαρακτηριστικών και μια ενεργή κοινότητα που συμβάλλει στο συνεχώς αναπτυσσόμενο οικοσύστημά του.

Το Visual Studio Code υποστηρίζει ένα ευρύ φάσμα γλωσσών προγραμματισμού, καθιστώντας το κατάλληλο για ποικίλα έργα. Είτε αναπτύσσετε εφαρμογές ιστού, είτε εφαρμογές για κινητά, είτε ακόμη και εργάζεστε σε τεχνολογίες όπως η μηχανική μάθηση ή η επιστήμη δεδομένων, το Visual Studio Code διαθέτει την απαραίτητη γλωσσική υποστήριξη και τις κατάλληλες επεκτάσεις.

Η δύναμη του Visual Studio Code έγκειται στην ικανότητά του να προσαρμόζεται στις ατομικές προτιμήσεις και στις απαιτήσεις του έργου. Προσφέρει πληθώρα επεκτάσεων όπως επεκτάσεις θεμάτων, υπογράμμιση συντακτικών λαθών και πολλά άλλα, επιτρέποντάς σας να προσαρμόσετε το περιβάλλον ανάπτυξής σας στις προτιμήσεις σας.

Το Visual Studio Code παρέχει εργαλεία εντοπισμού σφαλμάτων, επιτρέποντάς σας να διαγνώσετε και να διορθώσετε προβλήματα απευθείας μέσα από την εφαρμογή. Επιπλέον, προσφέρει δυνατότητες αυτοματοποίησης εργασιών, επιτρέποντάς σας να αυτοματοποιείτε επαναλαμβανόμενες εργασίες και να βελτιώνετε τη ροή εργασίας σας.

ΚΕΦΑΛΑΙΟ 3

3. Ανάλυση και σχεδιασμός συστήματος

Στην έναρξη κάθε έργου είναι αναγκαίο να προσδιοριστούν με ακρίβεια οι απαιτήσεις του έργου ή πιο απλά τι θα εξυπηρετεί το σύστημα το όποιο θέλουμε να αναπτύξουμε. Στην πρώτη φάση έναρξης του έργου πρέπει να καταγραφούν οι ανάγκες των χρηστών που θα εξυπηρετούνται μέσω του συστήματος.

3.1 Σύλληψη απαιτήσεων

Μετά από σχετική έρευνα για τις ανάγκες του χρήστη, καταγράψαμε τις απαιτήσεις που θα πρέπει να έχει το σύστημα αλλά και τις ενέργειες τις όποιες θα μπορεί να πραγματοποιήσει ο χρήστης. Για να γίνει αυτό ακολουθήσαμε την διαδικασία που περιλαμβάνει τρία στάδια.

	Actor	**Use Case**
	User	Login με την χρήση username και password
	User	Ανεπιτυχές Login με την χρήση username και password
	User	Εγγραφή του user για την επαλήθευση της ταυτότητας του με χρήση 3D matching
	User	Ανεπιτυχής εγγραφή του user για την επαλήθευση της ταυτότητας του με χρήση 3D matching
	User	Επαλήθευση της ταυτότητας του user με χρήση 3D matching και είσοδος στην εφαρμογή
	User	Ανεπιτυχής επαλήθευση της ταυτότητας του user με χρήση 3D matching και είσοδος στην εφαρμογή

Πίνακας 1: Πίνακας σύλληψης απαιτήσεων

3.2 Ανάλυση χρηστών

Στο σύστημα το οποίο σχεδιάσαμε υπάρχει μόνο ένα είδος χρήστη ο οποίος θα μπορεί να χρησιμοποιήσει τις διάφορες λειτουργίες του συστήματος.

1. Ο χρήστης θα μπορεί να συνδεθεί στην εφαρμογή με την χρήση του προσωπικού του username και password.
2. Ο χρήστης θα μπορεί να εγγραφεί στο σύστημα με την χρήση του προσώπου του έτσι ώστε να μπορεί να το χρησιμοποιήσει για την επαλήθευση της ταυτότητας του.
3. Ο χρήστης θα μπορεί να επαληθεύσει την ταυτότητα του και να συνδεθεί στην εφαρμογή με την χρήση του faceTec authentication

3.3 Σχεδιασμός

Use Case 1	
Title	Login με την χρήση username και password.
Description	Ο user προσπαθεί να συνδεθεί στην εφαρμογή με την χρήση του προσωπικού του username και του αντίστοιχου password.
Use case id	Story 1
Actors	User
Precondition	Ο user πρέπει να έχει προσωπικό username και password προκειμένου να συνδεθεί στην εφαρμογή.

Postcondition	Αν η επαλήθευση των στοιχείων του πραγματοποιηθεί επιτυχώς, επιτυγχάνετε η είσοδος στην εφαρμογή.
Path	
1	Ο user επιθυμεί να κάνει login στην εφαρμογή.
2	Ο user εισάγει το username του.
3	Ο user εισάγει το password του.
4	Ο user επιλέγει το κουμπί Login.
5	Στην περίπτωση που έχουν δοθεί τα σωστά στοιχεία ο user συνδέεται στην εφαρμογή.
6	Τέλος πρώτης περίπτωσης χρήσης.

Πίνακας 2: Use Case 1

Use Case 2	
Title	Ανεπιτυχές Login με την χρήση username και password.
Description	Ο user προσπαθεί να συνδεθεί στην εφαρμογή με την χρήση του προσωπικού του username και του αντίστοιχου password.
Use case id	Story 2
Actors	User
Precondition	Ο user πρέπει να έχει προσωπικό username και password προκειμένου να συνδεθεί στην εφαρμογή.
Postcondition	Αν η επαλήθευση των στοιχείων του αποτύχει, δεν επιτυγχάνετε η είσοδος στην εφαρμογή.
Path	
1	Ο user επιθυμεί να κάνει login στην εφαρμογή.
2	Ο user εισάγει το username του.
3	Ο user εισάγει το password του.

4	Ο user επιλέγει το κουμπί Login.
5	Τα στοιχεία που έχει πληκτρολογήσει ο user είναι λανθασμένα.
6	Εμφανίζεται μήνυμα στην οθόνη που ενημερώνει το user ότι τα στοιχεία που έχει εισάγει είναι λανθασμένα.
7	Ο χρήστης δεν μπορεί να εισέλθει στην εφαρμογή.
8	Τέλος δεύτερης περίπτωσης χρήσης.

Πίνακας 3: Use Case 2

Use Case 3	
Title	Εγγραφή του user για την επαλήθευση της ταυτότητας του με χρήση 3D matching.
Description	Ο user προκειμένου να μπορεί μελλοντικά να επαληθεύσει την ταυτότητα του με τη χρήση προσώπου του ώστε να καταφέρει να συνδεθεί στην εφαρμογή πρέπει πρώτα να κάνει εγγραφή με τη χρήση του προσώπου του.
Use case id	Story 3
Actors	User

Precondition	Ο user πρέπει να χρησιμοποιήσει την κάμερα του προσωπικού του υπολογιστή για να καταφέρει να ολοκληρώσει τη διαδικασία. Επίσης θα πρέπει να διαθέτει λογαριασμό ηλεκτρονικού ταχυδρομείου που θα του παρέχει ο admin του συστήματος για την επιτυχή εγγραφή του.
Postcondition	Αν η επαλήθευση των στοιχείων του είναι αληθής πραγματοποιείτε εγγραφή του χρήστη.
Path	
1	Ο user επιθυμεί να κάνει login στην εφαρμογή.
2	Ο user επιλέγει το κουμπί Login with FaceTec.
3	Ο χρήστης πληκτρολογεί το email του στο πεδίο που εμφανίζεται.
4	Ο user επιλέγει το κουμπί Enroll User.
5	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου 3D face scan στον FaceTec Server.
6	Γίνεται η εγγραφή του χρήστη.
7	Τα δεδομένα του user αποθηκεύονται στη βάση δεδομένων της FaceTec.
8	Τέλος τρίτης περίπτωσης χρήσης.

Πίνακας 4: Use Case 3

Use Case 4	
Title	Ανεπιτυχής εγγραφή του user για την επαλήθευση της ταυτότητας του με χρήση 3D matching.
Description	Ο user προκειμένου να μπορεί μελλοντικά να επαληθεύσει την ταυτότητα του με την χρήση του προσώπου του ώστε να καταφέρει να συνδεθεί στην εφαρμογή πρέπει πρώτα να κάνει εγγραφή.
Use case id	Story 4
Actors	User
Precondition	Ο user πρέπει να χρησιμοποιήσει την κάμερα του προσωπικού του υπολογιστή για να καταφέρει να ολοκληρώσει την διαδικασία. Επίσης θα πρέπει να διαθέτει λογαριασμό ηλεκτρονικού ταχυδρομείου που θα του παρέχει ο admin του συστήματος για την επιτυχή εγγραφή του.
Postcondition	Αν η επαλήθευση των στοιχείων αποτύχει, δεν πραγματοποιείτε εγγραφή του χρήστη.
Path	
1	Ο user επιθυμεί να κάνει login στην εφαρμογή.
2	Ο user επιλέγει το κουμπί Login with FaceTec.

3	Ο χρήστης πληκτρολογεί το email του στο πεδίο που εμφανίζεται.
4	Ο user επιλέγει το κουμπί Enroll User.
5	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου 3D face scan στον FaceTec Server.
6	Δεν γίνεται η εγγραφή του χρήστη
7	Τα δεδομένα του user δεν αποθηκεύονται στη βάση δεδομένων της FaceTec
8	Τέλος τέταρτης περίπτωσης χρήσης.

Πίνακας 5: Use Case 4

Use Case 5	
Title	Επιτυχής επαλήθευση της ταυτότητας του χρήστη με χρήση 3D matching και είσοδος στην εφαρμογή.
Description	Ο χρήστης επαληθεύει την ταυτότητα του με την χρήση του προσώπου του.
Use case id	Story 5

Actors	User
Precondition	Ο user πρέπει να χρησιμοποιήσει την κάμερα του προσωπικού του υπολογιστή για να καταφέρει να ολοκληρώσει την διαδικασία. Επίσης θα πρέπει να διαθέτει λογαριασμό ηλεκτρονικού ταχυδρομείου που θα του παρέχει ο admin του συστήματος για την επιτυχή εγγραφή του.
Postcondition	Αν η επαλήθευση της ταυτότητας με την χρήση του προσώπου του πραγματοποιηθεί επιτυχώς, επιτυγχάνετε η είσοδος στην εφαρμογή.
Path	
1	Ο user επιθυμεί να κάνει login στην εφαρμογή.
2	Ο user επιλέγει το κουμπί Login with FaceTec.
3	Ο χρήστης πληκτρολογεί το username του στο πεδίο που εμφανίζεται.
4	Ο user επιλέγει το κουμπί Authenticate User.
5	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου 3D face scan στον FaceTec Server.
6	Επιβεβαιώνεται η ταυτότητα του user.
7	Πραγματοποιείται η είσοδος του user στην εφαρμογή.

8	Τέλος πέμπτης περίπτωσης χρήσης.

Πίνακας 6: Use Case 5

Use Case 6	
Title	Ανεπιτυχής επαλήθευση της ταυτότητας του user με χρήση 3D matching .
Description	Ο user προσπαθεί να επαληθεύσει την ταυτότητα του με τη χρήση του προσώπου του για να καταφέρει να συνδεθεί στην εφαρμογή αλλά η διαδικασία αποτυγχάνει.
Use case id	Story 6
Actors	User
Precondition	Ο user πρέπει να έχει κάνει εγγραφή με την χρήση του προσώπου του και ο admin να του παρέχει το username του. Το πρόσωπο που θα επαληθευτεί θα πρέπει να είναι διαφορετικό από του user.
Postcondition	Αν η επαλήθευση της ταυτότητας με την χρήση του προσώπου αποτύχει, δεν επιτυγχάνεται η είσοδος στην εφαρμογή.
Path	
1	Ο user επιθυμεί να κάνει login στην εφαρμογή.

2	Ο user επιλέγει το κουμπί Login with FaceTec.
3	Ο χρήστης πληκτρολογεί το username του στο πεδίο που εμφανίζεται.
4	Ο user επιλέγει το κουμπί Authenticate User.
5	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου 3D face scan στον FaceTec Server.
6	Δεν επιβεβαιώνεται η ταυτότητα του user.
7	Εμφανίζεται μήνυμα στην οθόνη που ενημερώνει το user ότι η διαδικασία έχει αποτύχει.
8	Τέλος έκτης περίπτωσης χρήσης.

Πίνακας 7: Use Case 6

ΚΕΦΑΛΑΙΟ 4

4.Υλοποίηση – Customazition FaceTec SDK

Στο κεφάλαιο αυτό θα παρουσιάσουμε σημεία του κώδικά που αφορούν την λειτουργικότητα του συστήματος μας. Θα παρουσιάσουμε τον κώδικα που αφορά τόσο την επαλήθευση της ταυτότητας με την χρήση username και password όσο και με την λύση που παρέχει η FaceTec. Επίσης θα παρουσιάσουμε τις αλλαγές και το customization που κάναμε στο SDK που παρέχει η FaceTec.

Όπως έχουμε διευκρινίσει το σύστημα μας δεν χρησιμοποιεί τοπική βάση δεδομένων αλλά χρησιμοποιεί την βάση που παρέχει η FaceTec. Έτσι δεν έχουμε άμεση πρόσβαση σε όλα τα δεδομένα όπως και δεν μπορούμε να επιδράσουμε σε αυτά.

Σύμφωνα σε την ανάλυση απαιτήσεων αρχικά ο χρήστης έχει τη δυνατότητα να επαληθεύσει την ταυτότητα του με την χρήση του προσωπικού username και password. Αν επιτύχει η διαδικασία επαλήθευσης ο χρήστης έχει πρόσβαση στην dashboard. Ακόμα, για να είναι πιο φιλική προς τον χρήστη η διαδικασία της επαλήθευσης της ταυτότητας του προσθέσαμε κάποια βοηθητικά μηνύματα για την περίπτωση που ο χρήστης δεν εισάγει username ή password και για την περίπτωση που ο χρήστης πληκτρολογήσει λανθασμένα στοιχεία.

4.1 Παρουσίαση κώδικα

```
<script>
  var form = document.querySelector("form");
  form.addEventListener("submit", function (event) {
    event.preventDefault();
    var username = document.querySelector("#username").value;
    var password = document.querySelector("#password").value;
    if (username === "" || password === "") {
      swal("Please enter a username and password.");
      return;
    }
    if (username === 'admin' && password === 'admin1') {
      // validation success
      window.location.href = 'welcome1.html';
    } else {
      swal('Invalid username or password');
    }
  });
```

Εικόνα 2: Έλεγχος username και password χρήστη

```html
<body>
  <div class="navbar" id="browser-nav-bar" style="display:block;">
    <div class="logoContainer">
      <img src="./sample-app-resources/images/UNIPI_(logo).png" class="logo">
      <div>My FaceTec App</div>
    </div>
    <form>
      <label for="username">Username:</label>
      <input type="text" id="username" name="username">
      <br>
      <label for="password">Password:</label>
      <input type="password" id="password" name="password">
      <br>
      <input type="submit" value="Login">
    </form>

    <a href="./sample-apps/sample-app-js/">Login with FaceTec</a>

  </div>
```

Εικόνα 3: Κώδικας html της login σελίδας

```css
.logo {
  height: 120px;
  width: 120PX;
}

input[type="text"],
input[type="password"],
input[type="email"] {
  padding: 12px 20px;
  margin: 8px 0;
  box-sizing: border-box;
  border: 2px solid #ccc;
  border-radius: 24px;


}

input[type="submit"] a.hover {
  color: white;
}

input[type="submit"] {
  width: 80%;
  background-color: rgb(147 187 219);
  font-family: 'Source Sans Pro', Helvetica, sans-serif;
  color: #3b4242;
  padding: 14px 20px;
  margin: 8px 0;
  border: none;
  border-radius: 4px;
  cursor: pointer;
  font-weight: bold;


}
```

Εικόνα 4: Κώδικας CSS της Login σελίδας

```
function onEnrollUserPressed() {
    initializeResultObjects();
    SampleAppUtilities.fadeOutMainUIAndPrepareForSession();
    getSessionToken(function (sessionToken) {
        latestEnrollmentIdentifier = localStorage.userEmail + "1";
        latestProcessor = new EnrollmentProcessor(sessionToken, SampleApp);
    });
}
```

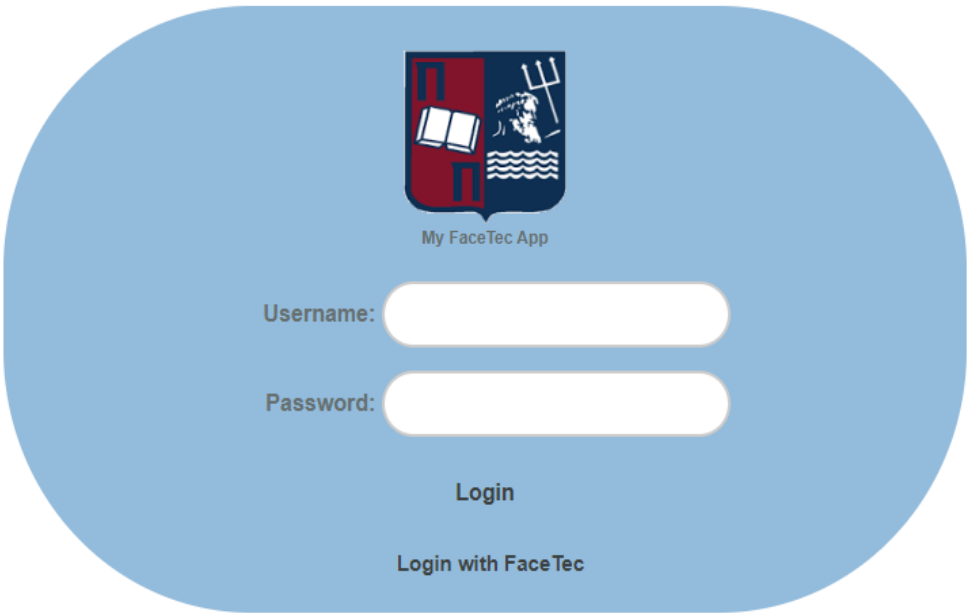
Εικόνα 5: Κώδικας εγγραφής χρήστη

```
function onAuthenticateUserPressed() {
    initializeResultObjects();
        SampleAppUtilities.fadeOutMainUIAndPrepareForSession();
        getSessionToken(function (sessionToken) {
            latestProcessor = new AuthenticateProcessor(sessionToken, SampleApp);
        });
    }
}
```

Εικόνα 6: Κώδικας επαλήθευσης ταυτότητας χρήστη

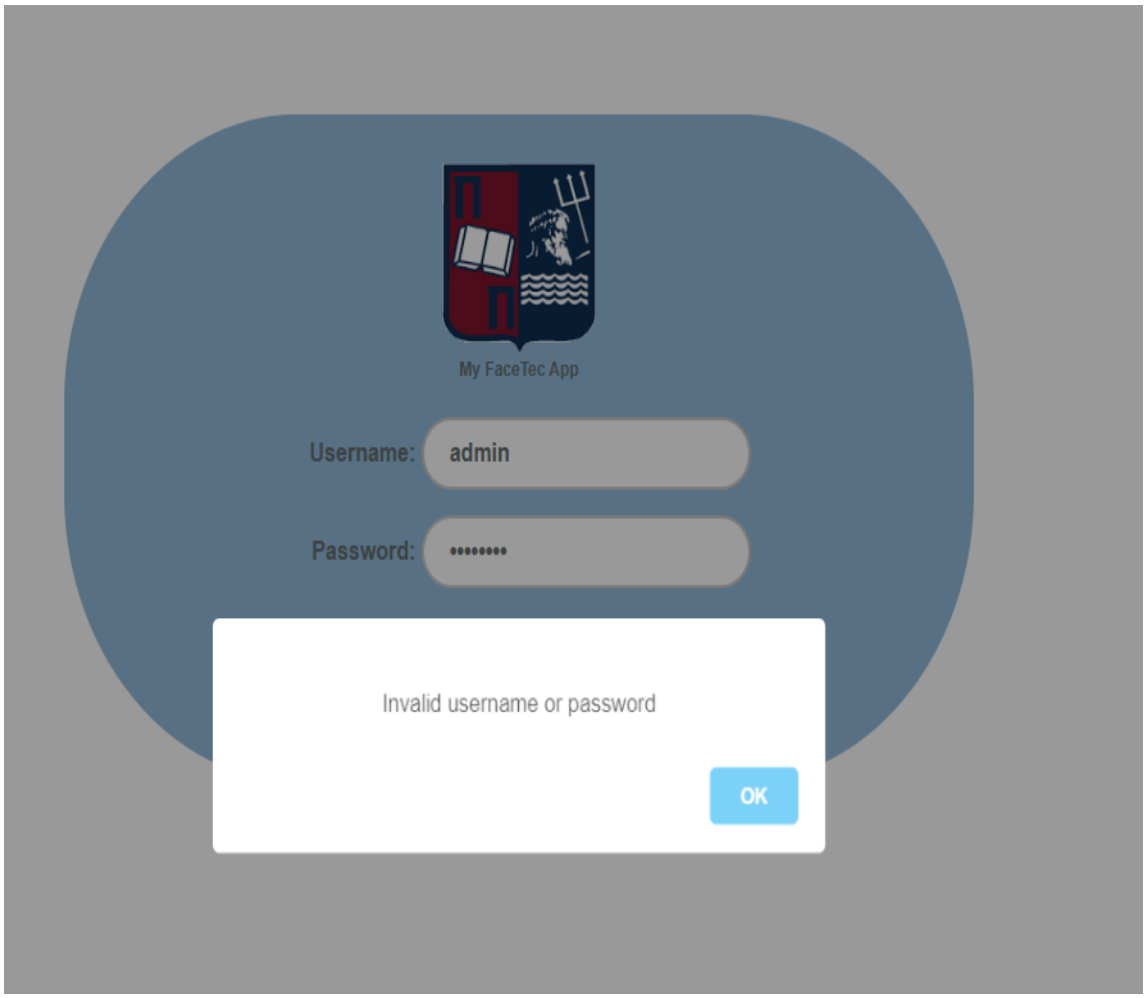
4.2 Ροή εφαρμογής

Αρχικά ο χρήστης μπορεί να επιλέξει για την επαλήθευση της ταυτότητα του την χρήση των προσωπικών κωδικών ή με την ταυτοποίηση μέσω του προσώπου του.



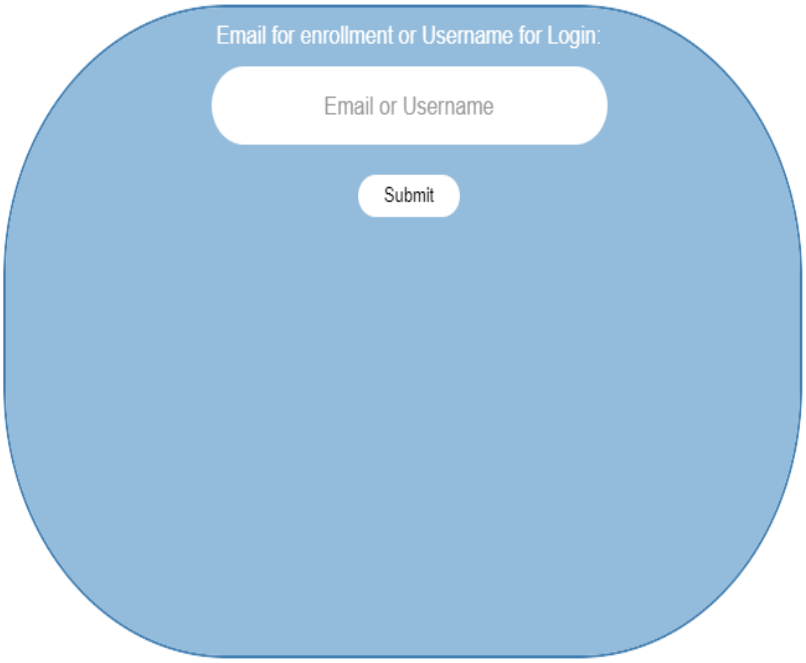
Εικόνα 7: Login σελίδα

Στην περίπτωση που ο χρήστης εισάγει λανθασμένα στοιχεία εμφανίζεται ένα μήνυμα που τον ενημερώνει ότι τα στοιχεία του είναι λανθασμένα.



Εικόνα 8: Μήνυμα σε περίπτωση λανθασμένου password ή username

Αν ο χρήστης επιλέξει για την ταυτοποίηση της ταυτότητας του την χρήση της τεχνολογίας αναγνώρισης προσώπου εμφανίζεται μια νέα σελίδα που τον καλεί να εισάγει το email του αν δεν έχει εγγραφεί και θέλει να εγγραφεί ή το username σε περίπτωση έχει εγγραφεί και θέλει μόνο να επαληθεύσει την ταυτότητα του.

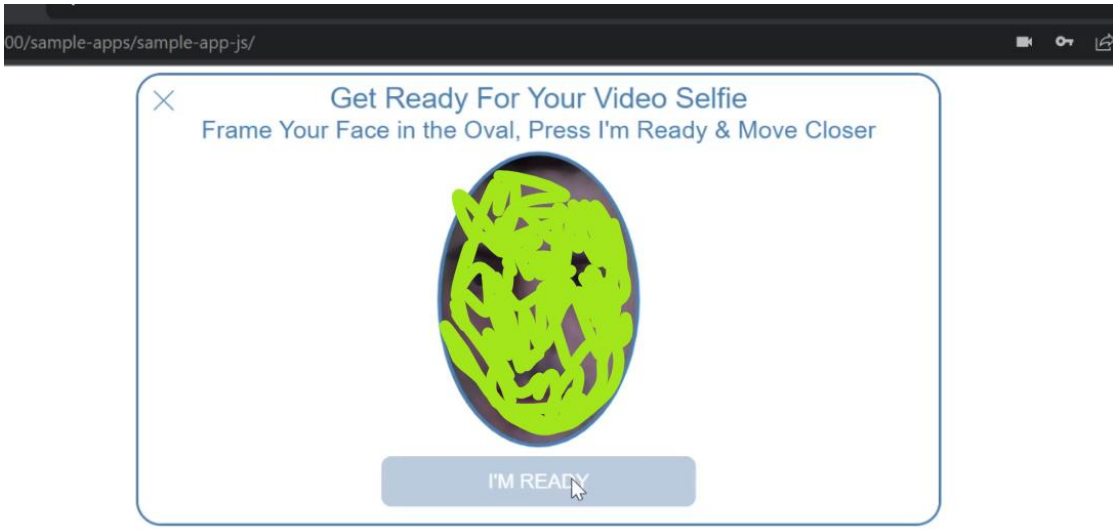


Εικόνα 9: Σελίδα εγγραφής ή επαλήθευσης ταυτότητας

Εισάγοντας το email ο χρήστης ανακατευθύνεται στην σελίδα εγγραφής.

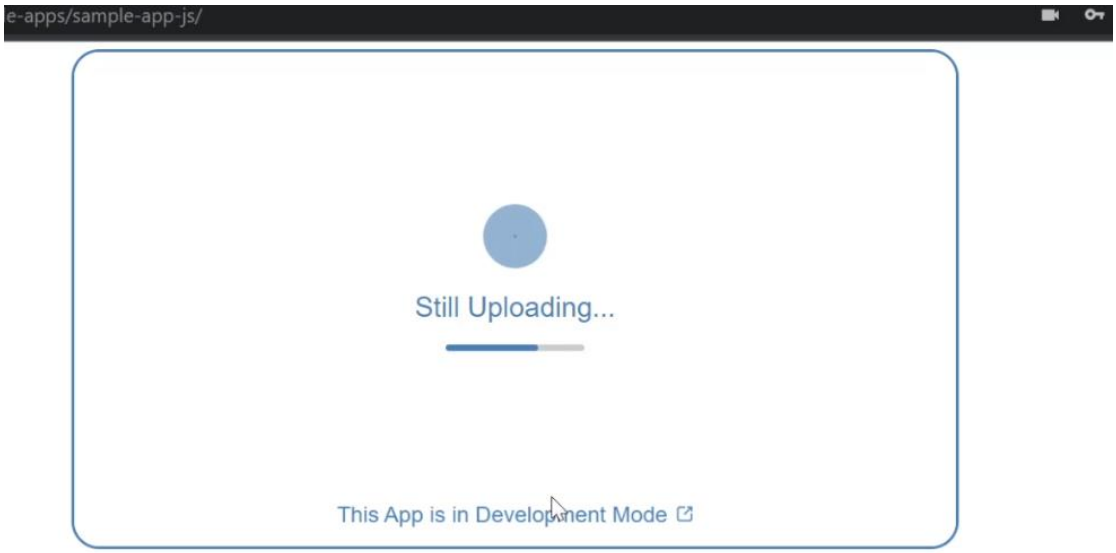
Εικόνα 10: Σελίδα εγγραφής του χρήστη

Πατώντας το κουμπί Enroll User, ο χρήστης ανακατευθύνεται στην επόμενη οθόνη.



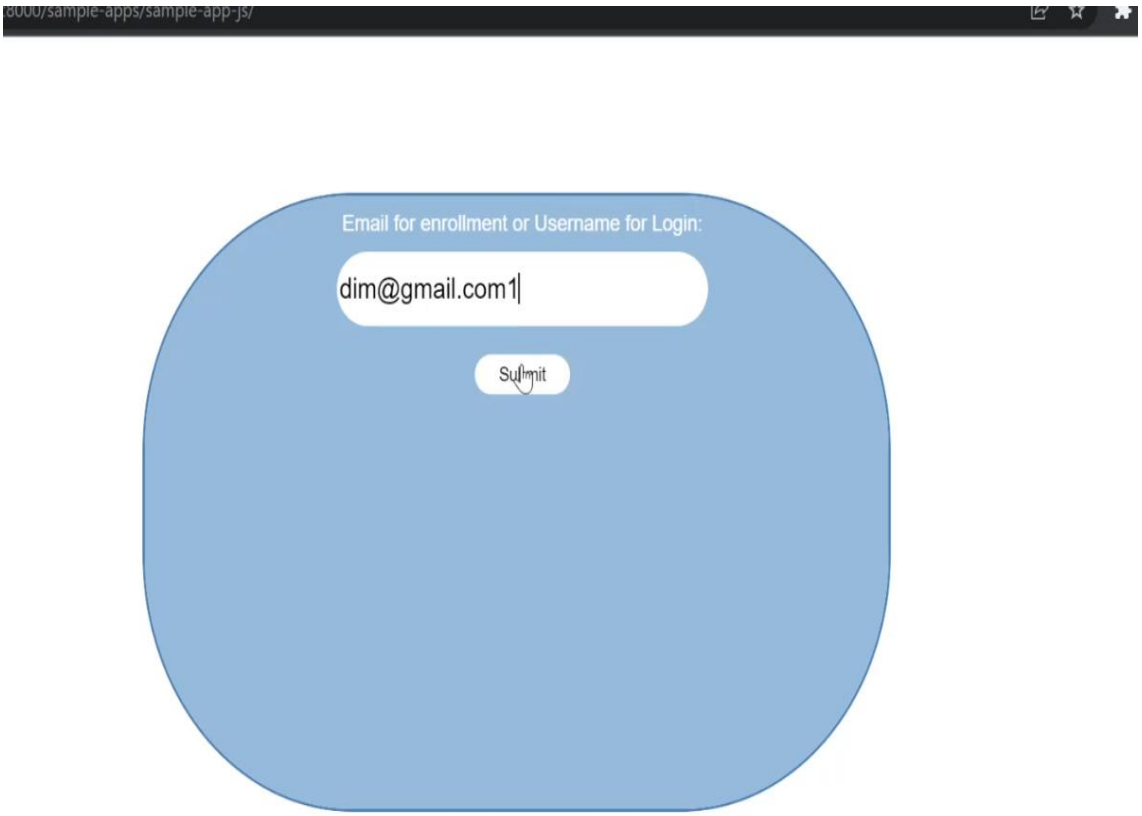
Εικόνα 11: Σελίδα εγγραφής του χρήστη με την χρήση του προσώπου του

Στο επόμενο βήμα η φωτογραφία αποθηκεύεται στην βάση δεδομένων της FaceTec



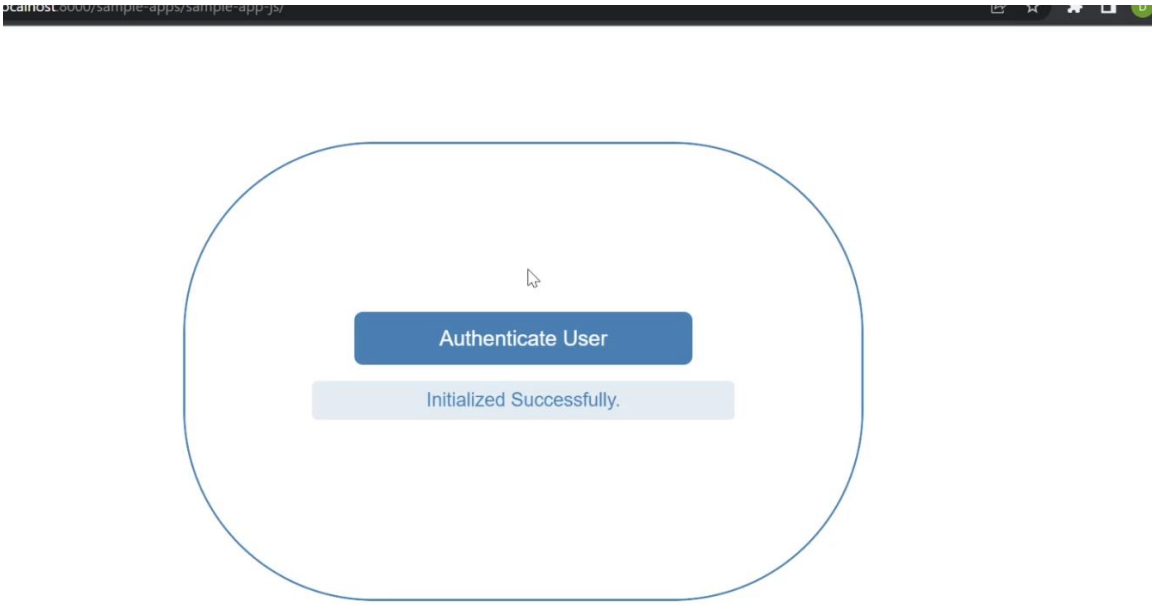
Εικόνα 12: Αποθήκευση φωτογραφίας χρήστη

Μετά την εγγραφή του ο χρήστης μπορεί να πληκτρολογήσει το username του το οποίο ακολουθεί μια συγκεκριμένη ακολουθία έτσι ώστε να χρησιμοποιήσει την αναγνώριση προσώπου για να εισέλθει στην εφαρμογή.



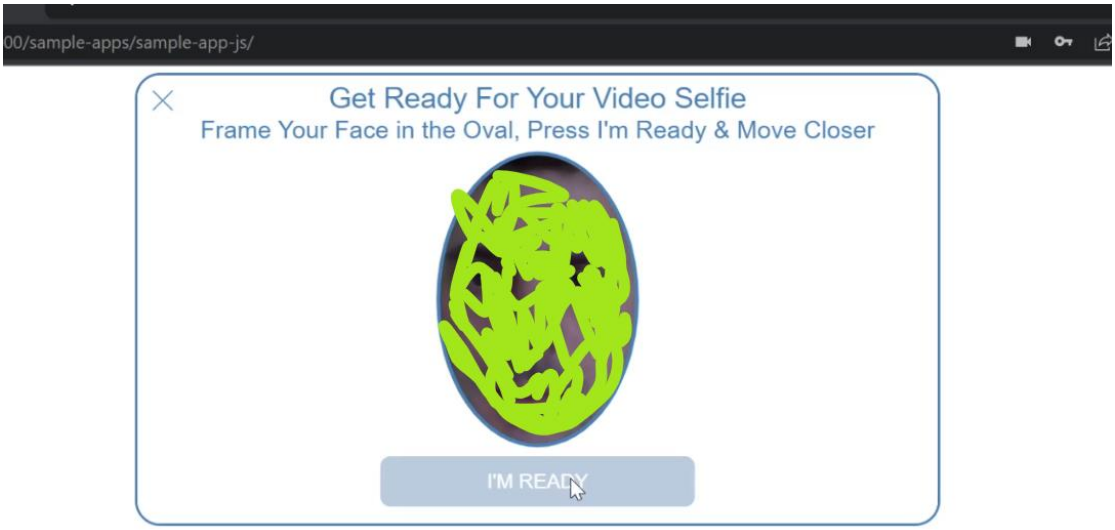
Εικόνα 13: Σελίδα εισαγωγής του username του χρήστη

Στις επιλογές πλέον δεν εμφανίζεται η επιλογή εγγραφής αλλά η επιλογή Authentication User διότι ο user έχει πληκτρολογήσει το username του.



Εικόνα 14: Σελίδα Authentication user

Στο επόμενο βήμα ενεργοποιείται η κάμερα του υπολογιστή έτσι ώστε ο χρήστης να επαληθεύσει την ταυτότητα του μέσω του liveness της FaceTec.



Εικόνα 15: Επαλήθευση ταυτότητας με χρήση του liveness της FaceTec

Επαλήθευση της ταυτότητας ενός χρήστη με τη χρήση τεχνολογιών αναγνώρισης προσώπου

Μετά την επαλήθευση της ταυτότητας του ο χρήστης ανακατευθύνεται στην dashboard του συστήματος μας.

Εικόνα 16: Dashboard συστήματος

ΚΕΦΑΛΑΙΟ 5

5. Παρουσίαση της σουίτας της FaceTect

Η FaceTec είναι μια εταιρία παροχής λύσεων βιομετρικού ελέγχου ταυτότητας που δίνουν τη δυνατότητα σε επιχειρήσεις ή οργανισμούς να επαληθεύουν την ταυτότητα των χρηστών τους χρησιμοποιώντας την τεχνολογία αναγνώρισης προσώπου. Η σουίτα της FaceTec παρέχει στους πελάτες της έναν ασφαλή και εύκολο στην χρήση τρόπο να πιστοποιούν τους χρήστες τους και να αποτρέπουν φαινόμενα απατών.

5.1 Περιπτώσεις χρήσης

Η σουίτα FaceTec βρίσκει εφαρμογή σε ένα ευρύ φάσμα επιχειρήσεων και οργανισμών από διάφορους κλάδους. Ακολουθούν ορισμένες από τις περιπτώσεις χρήσης της σουίτας της FaceTec:

Τραπεζικά και χρηματοπιστωτικά ιδρύματα: για την επαλήθευση της ταυτότητας των πελατών της, αλλά και για την ασφάλεια των τραπεζικών συναλλαγών.

Πάροχοι υγειονομικής περίθαλψης: για να διασφαλιστεί ότι στα ιατρικά αρχεία των ασθενών και σε άλλες ευαίσθητες πληροφορίες έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα.

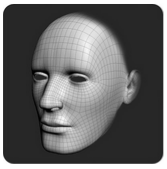
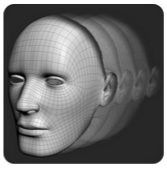
Πλατφόρμες ηλεκτρονικού εμπορίου: για την ασφάλεια των ηλεκτρονικών συναλλαγών και την αποφυγή φαινομένων απάτης.

Πάροχοι εφαρμογών κινητής τηλεφωνίας: για να επιτρέπουν τον ασφαλή και εύκολο έλεγχο της ταυτότητας για τους χρήστες τους. Για παράδειγμα το ξεκλείδωμα του κινητού μπορεί να γίνει με χρήση τεχνολογιών αναγνώρισης προσώπου.

Πλατφόρμες μέσων κοινωνικής δικτύωσης: για την επαλήθευση της ταυτότητας του χρήστη και τη διασφάλιση του απορρήτου και της ασφάλειας των δεδομένων των δεδομένων του.

Εταιρείες τυχερών παιχνιδιών και ψυχαγωγίας: για τη βελτίωση της εμπειρίας των χρηστών και την αποτροπή φαινομένων εξαπάτησης των χρηστών.

Μέσα μαζικής μεταφοράς: για την επαλήθευση της ταυτότητας των επιβατών τους.

TYPE	2D SOFTWARE	3D HARDWARE	FaceTec® 3D SOFTWARE
AXES	X,Y	X,Y,Z	X,Y + TIME
Vendors	Aware, BioID, Daon, FacePhi, Idemia, iProov, ID R&D, etc	Apple FaceID, Google Pixel 4, Intel RealSense®	FaceTec + **> 90 Channel Partners Worldwide**
Purpose	Face Matching	Unlock Mobile Phones	3D Face Matching
Installed Base	10+ Billion Smart Devices (Android-85% + iOS-14% & Webcams)	Only new iPhones have FaceID & Pixel 4 = < 12% of market	10+ Billion Smart Devices (Android-85% + iOS-14% & Webcams)
Portable Biometric	Varies	None, re-enroll on each device	Cross-Device & Cross-Platform
Technology	Legacy 2D Matching Software	Hardware: Infrared Camera Array & Neural Network Chip	Software: Real-time Computer Vision + 100% proprietary AI
Interface	Varies	Glance to unlock phone	3D Video Selfie: ~2 Seconds
Skin Tone Bias	Most 2D Algos have **bias at published FARs**	None-Reported	None observable in the **Lab or Real-World usage**
Device SDK Info	Varies	No SDK possible, special hardware required	Device SDKs for Android/iOS, web + Server SDK
Liveness Method	Blink, Smile, Turn Head or Flashing Lights, etc	Infrared dots + neural network chip determine if user is 3D	Measures 3D Depth, skin texture, eye reflections, etc
Liveness Strength	Fairly Weak	Fairly Strong	Very Strong
3D Depth Detection	Weak	Very Strong	Very Strong
Intellectual Property	Legacy tech, too old for meaningful patents	20+ infrared related patents acquired in 2013	5 US Patents on 3D process issued, +12 pending globally
FAR/FRR	Varies, but 1/<75,000 at real world usable FRRs	1/1M - No FRR stated	1/125,000,000 FAR @ <1% FRR
Identical Twin Differentiation	Very Weak	"If you have a Twin, use a PIN."	High 1:1 FAR provides Best Possible Twin Differentiation
Liveness Testing Certifications	No, only non-standardized conformances, no camera feed security tested	No Official 3rd Party Testing	Certified Level 1 & 2 Spoof Detection by NIST/NVLAP LAB - **Liveness.com**
Age Estimation	2D = poor Age Estimates	Not Available	"Better than Human" Face-only Anonymous **Age Estimation**
Match to Photo ID	Low-detail & problems with aged photos = low match rates	Not Available	Up to 1/2,000,000 Match Confidence with 3D:2D
Password Replacement?	Not secure enough, Liveness too Weak & FAR too low	No, only used for convenience	Yes, universal device support, highly secure & convenient
Spoof Bounty Programs?	No, **2D is easily spoofed**	No, no motivation	$600,000, **SpoofBounty.com**

Εικόνα 17: Σύγκριση της σουίτα της FaceTec

Επαλήθευση της ταυτότητας ενός χρήστη με τη χρήση τεχνολογιών αναγνώρισης προσώπου

5.2 3D Liveness

Το FaceTec 3D Liveness είναι μια τεχνολογία που βοηθά στην ενίσχυση της ασφάλειας με την χρήση μεθόδων βιομετρικής πιστοποίησης ταυτότητας, διασφαλίζοντας έτσι ότι κατά την διαδικασία πιστοποίησης είναι παρόν ένα πραγματικό, ζωντανό πρόσωπο και όχι μια φωτογραφία ή ένα βίντεο. Αυτό επιτυγχάνεται με την χρήση προηγμένης τρισδιάστατης χαρτογράφησης του προσώπου του χρήστη καθώς επίσης και με ισχυρούς και πολύπλοκους αλγορίθμους μηχανικής μάθησης για την ανίχνευση κινήσεων που συμβαίνουν φυσικά σε ένα ανθρώπινο πρόσωπο.

Όταν ένας χρήστης επιχειρεί να πιστοποιήσει την ταυτότητά του με ένα σύστημα που διαθέτει 3D Liveness, του ζητείται να εκτελέσει μια σειρά από τυχαίες κίνησεις, όπως να εστιάσει σε ένα συγκεκριμένο σημείο ή να γυρίσει το κεφάλι του προς μια συγκεκριμένη κατεύθυνση. Η σουίτα της FaceTec λειτουργεί καταγράφοντας ένα τρισδιάστατο πορτραίτο του προσώπου του χρήστη και το αναλύει για να διασφαλίσει ότι οι κινήσεις είναι πραγματικές και συνάδουν με εκείνες ενός πραγματικού φυσικού προσώπου. Εάν το σύστημα εντοπίσει στοιχεία που δεν επαληθεύουν την διαδικασία επαλήθευσης, θα αρνηθεί την πρόσβαση.

Πέρα όμως από την ενίσχυση της ασφάλειας, μέσω του 3D Liveness μπορεί επίσης να βελτιωθεί η εμπειρία ενός χρήστη, καθιστώντας τον έλεγχο ταυτότητας του ταχύτερο και πιο εύκολο. Οι χρήστες μπορούν απλώς να τραβήξουν ένα γρήγορο βίντεο του προσώπου τους για να επαληθεύσουν την ταυτότητά τους, χωρίς να χρειάζονται πολύπλοκους κωδικούς πρόσβασης ή κωδικούς ελέγχου ταυτότητας.

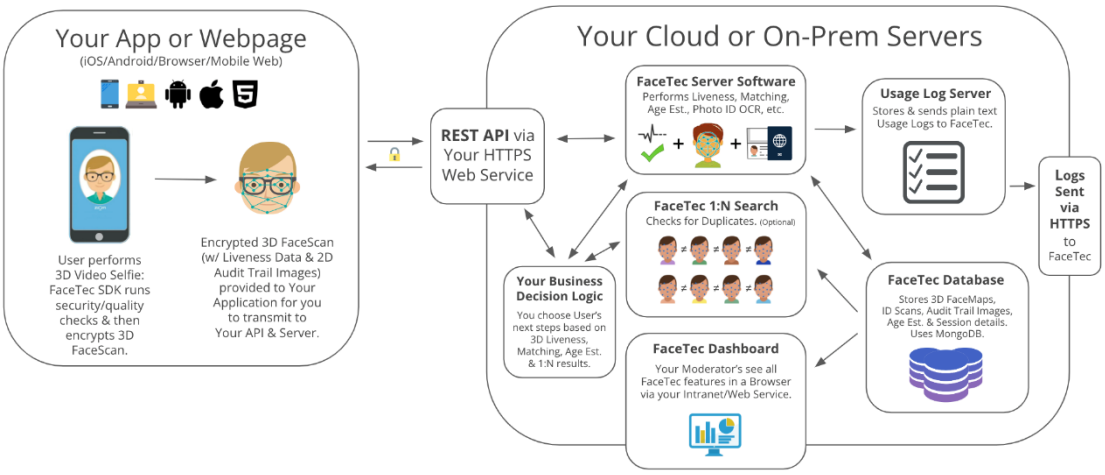
Η τεχνολογία FaceTec 3D Liveness βασίζεται σε μια εξελιγμένη αρχιτεκτονική που περιλαμβάνει διάφορα βασικά στοιχεία. Αυτά περιλαμβάνουν:

Χαρτογράφηση προσώπου 3D: Η FaceTec χρησιμοποιεί προηγμένους αλγορίθμους για τη δημιουργία ενός τρισδιάστατου χάρτη του προσώπου του χρήστη, καταγράφοντας εκατοντάδες σημεία δεδομένων που είναι μοναδικά για το συγκεκριμένο άτομο.

Μηχανική μάθηση: Το σύστημα χρησιμοποιεί αλγορίθμους μηχανικής μάθησης για την ανάλυση του προσώπου του χρήστη και τον εντοπισμό τυχόν ενδείξεων απάτης ή πλαστοπροσωπίας.

Anti-Spoofing: Η FaceTec περιλαμβάνει μέτρα anti-spoofing που εμποδίζουν τους επιτιθέμενους να χρησιμοποιήσουν φωτογραφίες ή βίντεο για να παρακάμψουν το σύστημα.

Ασφαλής αποθήκευση: Τα δεδομένα των χρηστών αποθηκεύονται με ασφάλεια, χρησιμοποιώντας προηγμένη κρυπτογράφηση και μέτρα προστασίας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.



Εικόνα 18: Αρχιτεκτονική της εφαρμογής της FaceTec

ΚΕΦΑΛΑΙΟ 6

6. Συμπεράσματα

Συμπερασματικά, η ενσωμάτωση και η χρήση της σουίτας της FaceTec αποδεικνύει την χρησιμότητα της τόσο στη διασφάλιση της ασφάλειας όσο και της βελτιωμένης εμπειρίας του χρήστη. Χρησιμοποιώντας προηγμένες τεχνικές αναγνώρισης προσώπου, η FaceTec παρέχει μια εξαιρετικά αξιόπιστη λύση για την επαλήθευση της ταυτότητας των προσώπων των χρηστών σε πραγματικό χρόνο.

Κατά τη διάρκεια της διατριβής, διερευνήσαμε διεξοδικά τις δυνατότητες του FaceTec liveness και διαπιστώσαμε την αποτελεσματικότητά του στην πρόληψη δόλιων δραστηριοτήτων, όπως η προσπάθεια της εισόδου στην εφαρμογή μη εξουσιοδοτημένου χρήστη. Η ενσωμάτωση της αναγνώρισης προσώπου όχι μόνο ενισχύει την ασφάλεια του συστήματός αλλά και εμπνέει εμπιστοσύνη στους χρήστες, γνωρίζοντας ότι τα στοιχεία τους και τα προσωπικά τους δεδομένα προστατεύονται.

Η τεχνολογία liveness της FaceTec αξιοποιεί εξελιγμένους αλγορίθμους που αναλύουν διάφορα χαρακτηριστικά του προσώπου καθώς και συγκεκριμένες κινήσεις του για να διασφαλίσουν ότι το πρόσωπο που παρουσιάζεται για επαλήθευση είναι όντως ένα πραγματικό πρόσωπο και όχι μια απατηλή αναπαράσταση. Χρησιμοποιώντας έναν συνδυασμό τεχνικών που συλλέγουν δεδομένα από διαφορετικές κινήσεις του κεφαλιού αλλά και από τα χαρακτηριστικά του η FaceTec μπορεί να αξιόπιστα να διακρίνει μεταξύ ενός πραγματικού προσώπου και μιας προσπάθειας πλαστογράφησης, ακόμη και με την παρουσία προηγμένων τεχνικών πλαστογράφησης, όπως οι τρισδιάστατες μάσκες.

Επιπλέον, το SDK και το API της FaceTec έχουν αποδειχθεί ευέλικτα και φιλικά προς τον χρήστη, επιτρέποντας την εύκολη ενσωμάτωση σε υπάρχοντα συστήματά και ελαχιστοποιώντας τον χρόνο ανάπτυξης. Η υποστήριξη που παρέχει η FaceTec συνέβαλαν καθοριστικά στην διαδικασία υλοποίησης, εξασφαλίζοντας απρόσκοπτη εμπειρία χρήσης και γρήγορη υιοθέτηση από τη βάση χρηστών μας.

Ένα από τα αξιοσημείωτα πλεονεκτήματα της τεχνολογίας liveness είναι η προσαρμοστικότητά της σε διαφορετικά σενάρια και περιβάλλοντα. Μπορεί να λειτουργήσει αποτελεσματικά σε διάφορες συνθήκες φωτισμού, γωνίες και αποστάσεις, καθιστώντας την κατάλληλη για ένα ευρύ φάσμα εφαρμογών. Είτε πρόκειται για έλεγχο ταυτότητας μέσω κινητών τηλεφώνων, είτε για συστήματα ελέγχου πρόσβασης, είτε για απομακρυσμένη επαλήθευση ταυτότητας, η τεχνολογία liveness της FaceTec μπορεί να προσφέρει συνεπή και αξιόπιστα αποτελέσματα.

Με την ενσωμάτωση της τεχνολογίας ζωντάνιας, αντιμετωπίσαμε με επιτυχία τα τρωτά σημεία που σχετίζονται με τις παραδοσιακές μεθόδους ελέγχου ταυτότητας, όπως οι κωδικοί οι οποίοι μπορούν εύκολα να παραβιαστούν. Η χρήση της αναγνώρισης προσώπου και της ανίχνευσης ζωντάνιας εξαλείφει την ανάγκη για πολύπλοκους κωδικούς πρόσβασης μειώνοντας τον κίνδυνο παραβίασης λογαριασμών.

6.1 Πιθανές επεκτάσεις

Χρησιμοποιώντας το FaceTec SDK αξιοποιήσαμε τις ισχυρές δυνατότητες αναγνώρισης προσώπου που προσφέρει. Βασιζόμενοι σε αυτό, διερευνούμε μελλοντικές επεκτάσεις που θα μπορούσαν να γίνουν στο σύστημα. Μια πιθανή επέκταση του συστήματος θα περιελάβανε την ενσωμάτωση μιας βάσης δεδομένων που θα ήταν τοπικά εγκατεστημένη. Με την ενσωμάτωση της βάσης δεδομένων, μπορούμε να αναβαθμίσουμε περαιτέρω τη λειτουργικότητα του έργου, την εξατομίκευση των χρηστών και τις δυνατότητες διαχείρισης δεδομένων.

Ακόμα με την βάση δεδομένων θα μπορούσαμε να παρέχουμε βελτιωμένες δυνατότητες, επιτρέποντάς μας να δημιουργήσουμε μια πιο ολοκληρωμένη και εξατομικευμένη εμπειρία για τους χρήστες. Μερικές από αυτές τις νέες δυνατότητες :

Ταυτοποίηση χρηστών και προφίλ: Η βάση δεδομένων μας δίνει τη δυνατότητα να εφαρμόσουμε ασφαλή έλεγχο ταυτότητας χρηστών και διαχείριση προφίλ. Αποθηκεύει βιομετρικά δεδομένα προσώπου μαζί με πρόσθετες πληροφορίες χρήστη, όπως στοιχεία επικοινωνίας, προτιμήσεις και μοτίβα συμπεριφοράς. Αυτό το ολοκληρωμένο προφίλ χρήστη μας δίνει την δυνατότητα για παραπέρα επεκτάσεις.

Εξατομίκευση βάσει του προφίλ του χρήστη: Με την βάση δεδομένων, μπορούμε να αξιοποιήσουμε τα αποθηκευμένα προφίλ χρηστών για να παρέχουμε εξατομικευμένες δυνατότητες με βάση το προφίλ. Τα προφίλ των αναγνωρισμένων χρηστών μας δίνουν την δυνατότητα να προσφέρουμε νέες δυνατότητες με βάση τις προτιμήσεις, τα δημογραφικά στοιχεία και την ιστορική τους συμπεριφορά.

Προηγμένη διαχείριση δεδομένων: Η βάση δεδομένων παρέχει ισχυρές δυνατότητες διαχείρισης δεδομένων. Εξασφαλίζει την ασφαλή αποθήκευση, τη συμμόρφωση με το απόρρητο και τους ελέγχους πρόσβασης στα δεδομένα.

Επιπρόσθετα στην ενσωμάτωση μιας τοπικής βάσης δεδομένων, θα μπορούσαμε να προβούμε και σε επεκτάσεις που αφορούν την διεπαφή χρήστη (UI). Οι βελτιώσεις του UI θα επέτρεπαν:

Βελτιστοποίηση της διαδικασίας εγγραφής των χρηστών: Απλοποιώντας τα βήματα και εξασφαλίζοντας σαφείς οδηγίες θα μπορούσαμε να απλοποιήσουμε την διαδικασία εγγραφής.

Προσαρμόσιμα θέματα UI: Προσφέροντας στους χρήστες τη δυνατότητα να εξατομικεύσουν το UI επιλέγοντας από μια σειρά θεμάτων ή προσαρμόζοντας τα χρωματικά σχήματα και τις επιλογές διάταξης. Αυτή η προσαρμογή βελτιώνει τη συνολική εμπειρία του χρήστη.

Τέλος, για να επεκτείνουμε περαιτέρω τις δυνατότητες του έργου, θα μπορούσαμε να ενσωματώσουμε και τεχνολογίες και εργαλεία όπως:

Ενσωμάτωση φωνητικής αναγνώρισης: Θα μπορούσαμε να συνδυάσουμε τα βιομετρικά στοιχεία του προσώπου με αυτά της φωνής για να ενισχύσουμε την ασφάλεια.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Michael Fairhurst(2019).Biometrics: A Very Short Introduction (Very Short Introductions), Oxford University Press.
2. Sébastien Marcel, Mark S. Nixon, Julian Fierrez, Nicholas Evans(2019).Handbook of Biometric Anti-Spoofing: Presentation Attack Detection, Springer.
3. FaceTec Competitors, URL: https://sourceforge.net/software/product/FaceTec/alternatives , 2022.
4. Laurence Lars Svekis, Maaike van Putten, Rob Percival(2021). JavaScript from Beginner to Professional: Learn JavaScript quickly by building fun, interactive and dynamic web apps, games, Packt Publishing.
5. Gunnar Overgaard, Karin Palmkvist(2004).Use cases patterns and blueprints, Addison-Wesley Professional.
6. Lengyel, G. (2017). Face Detection and Recognition: Theory and Practice in JavaScript. Independently published.
7. How to Create Use Case Description for Your Business Analysis Report, URL: https://www.dummies.com/business/business-strategy/how-to-create-use-case-description-for-your-business-analysis-report/ , 2022.
8. Simpson, K. (2015-2017). You Don't Know JS (Series). O'Reilly Medi.
9. Zakas, N. C. (2016). Understanding ECMAScript 6: The Definitive Guide for JavaScript Developers. No Starch Press.
10. Fogus, M. (2013). Functional JavaScript: Introducing Functional Programming with Underscore.js. O'Reilly Media.
11. Hohpe, G., & Woolf, B. (2004). Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions. Addison-Wesley Professional.