ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Βιομετρικά Συστήματα

&

Τεχνητή Νοημοσύνη

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Μιχαηλίδη Φώτιου

Επιβλέπουσα: Βασιλική Διαμαντοπούλου

Μέλη εξεταστικής επιτροπής: Σπύρος Κοκολάκης, Κωνσταντίνος Μαλιάτσος

Σάμος, Σεπτέμβριος 2025

Κατάλογος εικόνων.

Κατάλογος πινάκων.

Αρκτικόλεξο

Table 1 Αρτικόλεξο.

AI	Artificial Intelligence
FAR	False Accept Rate
FRR	False Reject Rate
FNMR	False Non-Match Rate
ROC	Relative Operating Characteristic
EER	Equal Error Rate
FTE or FER	Failure to Enroll Rate
FTC	Failure to Capture Rate
DCT	Discrete Cosine Transformation

Περίληψη

Η μελέτη αυτή διερευνά τη συνύπαρξη των βιομετρικών συστημάτων αυθεντικοποιήσης και της τεχνητής νοημοσύνης (AI), εστιάζοντας στις προκλήσεις και τα οφέλη που αφορούν την ασφάλεια των πληροφοριών που τυγχάνουν επεξεργασίας από τα εν λόγω συστήματα. Η βιομετρική ταυτοποίηση, μέθοδος όπου χρησιμοποιούνται μοναδικά φυσιολογικά ή συμπεριφορικά χαρακτηριστικά, όπως δακτυλικά αποτυπώματα, μοτίβα ίριδας και αναγνώριση προσώπου, έχει καταστεί αναπόσπαστο μέρος των σύγχρονων συστημάτων ταυτοποίησης.

Αρχικά, γίνεται εισαγωγή στα βιομετρικά συστήματα, περιγράφοντας λεπτομερώς τα βασικά τους στοιχεία, τις φάσεις της πιστοποίησης (εγγραφή και επαλήθευση) και τα βασικά χαρακτηριστικά τους όπως την καθολικότητα, τη μοναδικότητα και τη μονιμότητα. Στη συνέχεια, αναλύονται συγκεκριμένες βιομετρικές μέθοδοι, όπως η αναγνώριση δακτυλικών αποτυπωμάτων, της ίριδας, του προσώπου και της παλάμης. Η επιλογή των βιομετρικών συστημάτων έγινε έχοντας ως κριτήριο τον βαθμό χρήσης τους σε πραγματικές περιπτώσεις εφαρμογές, όπως ταυτοποίηση σε κρίσιμες υποδομές και σε συσκευές τελικών χρηστών για παράδειγμα κινητά τηλέφωνα και υπολογιστές.

Σημαντικό μέρος της μελέτης αποτελεί η ανάλυση της ασφάλειας των βιομετρικών συστημάτων πιστοποίησης και στον τρόπο με τον οποίο οι τεχνικές και οι αλγόριθμοι που βασίζονται στην τεχνητή νοημοσύνη (Artificial Intelligence - AI) επηρεάζει τόσο τις απειλές όσο και τα αντίμετρα.

Η μελέτη ολοκληρώνεται με συστάσεις για την αντιμετώπιση των κινδύνων, συμπεριλαμβανομένης της πολυπαραγοντικής πιστοποίησης, της κρυπτογράφησης και της ανίχνευσης ζωντανότητας με τη βοήθεια της τεχνητής νοημοσύνης. Αντιμετωπίζοντας αυτές τις προκλήσεις, η ενσωμάτωση εργαλείων τεχνητής νοημοσύνης στα βιομετρικά συστήματα μπορεί να οδηγήσει στη δημιουργία ισχυρών πλαισίων ασφάλειας, ικανά να προσαρμοστούν στις αναδυόμενες απειλές.

Λέξεις-κλειδιά: Βιομετρικά συστήματα, τεχνητή νοημοσύνη, ασφάλεια πληροφοριών, πλαστογράφηση (spoofing), εντοπισμός ζωντανότητας.

Abstract.

This study explores the intersection of biometric systems and artificial intelligence (AI), focusing on security challenges and benefits. Biometric authentication, which utilizes unique physiological or behavioral traits such as fingerprints, iris patterns, and facial recognition, has become an integral part of modern authentication systems.

The paper begins with an introduction to biometric systems, detailing their fundamental components, authentication phases (enrollment and verification), and key characteristics like universality, uniqueness, and permanence. It then examines specific biometric modalities, including fingerprint, iris, facial, and palm recognition, analyzing their basic operations.

A significant portion of the study is dedicated to analyze the security of biometric authentication systems and how AI affects both threats and countermeasures.

The study concludes with recommendations for mitigating risks, including multi-factor authentication, encryption, and AI-driven liveness detection. By addressing these challenges, the integration of AI and biometrics can achieve robust security frameworks capable of adapting to emerging threats.

Keywords: Biometric systems, artificial intelligence, security, spoofing, deepfakes, liveness detection.

Κεφάλαιο Α: Εισαγωγή

Η ραγδαία ανάπτυξη της τεχνολογίας τα τελευταία χρόνια έχει επιφέρει σημαντικές αλλαγές στον τρόπο με τον οποίο οι άνθρωποι αλληλοεπιδρούν με τα πληροφοριακά συστήματα και χρησιμοποιούν τις διάφορες υπηρεσίες. Οι αλλαγές αυτές δημιούργησαν την ανάγκη για περισσότερες και ασφαλέστερες μεθόδους αυθεντικοποιήσης για τα πληροφοριακά συστήματα. Σε αυτό το πλαίσιο, η βιομετρική αυθεντικοποιήση έχει αναδειχθεί ως μια από τις πιο συνηθισμένες μεθόδους ενίσχυσης της ασφάλειας.

Η ασφάλεια των βιομετρικών συστημάτων δεν αποτελεί μόνο τεχνολογικό ζήτημα, αλλά άπτεται και θεμάτων κοινωνικών, νομικών και ηθικών. Η δυνατότητα ενός συστήματος να ταυτοποιεί ή να επαληθεύει την ταυτότητα ενός χρήστη βασιζόμενο σε μοναδικά φυσιολογικά ή συμπεριφορικά χαρακτηριστικά (όπως το δακτυλικό αποτύπωμα, η ίριδα, το πρόσωπο, η φωνή, ο τρόπος βάδισης) έχει μεταβάλει ριζικά την ασφάλεια των σύγχρονων πληροφοριακών συστημάτων και των οργανισμών.

Ωστόσο, με την ολοένα και αυξανόμενη χρήση των βιομετρικών συστημάτων αυθεντικοποιήσης αυξάνεται και η ικανότητα των κακόβουλων χρηστών να παρακάμπτουν τα μέτρα ασφαλείας και να προκαλούν αρνητικές συνέπειες τόσο σε τελικούς χρήστες όσο και σε διάφορους οργανισμούς, με επιθέσεις όπως, οι επιθέσεις παρουσίασης (presentation attacks) ή οι επιθέσεις επανάληψης (replay attacks). Σε αυτό το σημείο, η συνεισφορά της Τεχνητής Νοημοσύνης αποδεικνύεται κομβική, καθώς οι αλγόριθμοι μηχανικής μάθησης (machine learning) και οι αλγόριθμοι βαθιάς μάθησης (deep learning) μπορούν να βελτιώσουν την ανίχνευση τέτοιων επιθέσεων, αλλά και να αξιοποιηθούν από επιτιθέμενους για τη δημιουργία τεχνικών παραπλάνησης.

Η ασφάλεια των βιομετρικών συστημάτων μπορεί να χωριστεί σε τέσσερα βασικά επίπεδα: το επίπεδο του λογισμικού (Software), όπου εντάσσονται όλοι οι αλγόριθμοι ταυτοποίησης, το επίπεδο του Υλικού (Hardware), όπου περιλαμβάνονται ο αισθητήρας εισόδου και η μικροαρχιτεκτονική του βιομετρικού συστήματος, το επίπεδο του σήματος επικοινωνίας (Communications), που αφορά τη μεταφορά των βιομετρικών δεδομένων μέσω των φυσικών διαύλων επικοινωνίας και το επίπεδο των βάσεων δεδομένων (Databases) όπου περιλαμβάνεται η βάση δεδομένων στην οποία αποθηκεύονται τα βιομετρικά δεδομένα. Κάθε ένα από αυτά τα επίπεδα αντιμετωπίζει διαφορετικές προκλήσεις οι οποίες πρέπει να αντιμετωπιστούν για να υπάρξει η επιθυμητή ασφάλεια των αγαθών που προστατεύονται από βιομετρικά συστήματα.

Οι εφαρμογές τεχνητής νοημοσύνης, με την ικανότητά τους να εκπαιδεύονται και να προσαρμόζονται σε νέα δεδομένα, μπορούν να ενισχύσουν την άμυνα των βιομετρικών συστημάτων, προσφέροντας τεχνικές όπως οι ανιχνευτές πλαστογράφησης (spoofing) και οι εξελιγμένοι μηχανισμοί ταυτοποίησης. Παράλληλα, όμως, μπορούν να αποτελέσουν όπλο στα χέρια κακόβουλων χρηστών. Χαρακτηριστικό παράδειγμα αποτελούν τα deepfakes, όπου

τεχνολογίες βαθιάς μάθησης χρησιμοποιούνται για τη δημιουργία πλαστών βιομετρικών δεδομένων (π.χ. ψεύτικων προσώπων ή φωνών), που μπορούν να ξεγελάσουν ακόμη και τα πιο εξελιγμένα συστήματα αναγνώρισης. Αυτή η διττή φύση της Τεχνητής Νοημοσύνης – ως εργαλείο άμυνας αλλά και επίθεσης – καθιστά την ανάλυση της σχέσης της με τα βιομετρικά συστήματα ιδιαίτερα σημαντική.

Στόχος εργασίας

Στο πλαίσιο της παρούσας εργασίας, επιχειρείται να διερευνηθεί η σχέση μεταξύ των βιομετρικών συστημάτων και της τεχνητής νοημοσύνης, εστιάζοντας ιδιαίτερα στην ασφάλεια και στις προκλήσεις που δημιουργούνται. Στόχος είναι, να αναλυθούν οι τεχνικές, οι κίνδυνοι και οι καλές πρακτικές που πρέπει να ακολουθούνται, ώστε να διασφαλιστεί ότι η ενσωμάτωση των ΤΝ τεχνικών στα βιομετρικά συστήματα γίνεται με τρόπο που ενισχύει την ασφάλεια, αντί να την υπονομεύει.

Μεθοδολογία Εργασίας

Η παρούσα διπλωματική εργασία έχει βασιστεί στη μεθοδολογία του Desktop Research, ή αλλιώς, έρευνας με χρήση ηλεκτρονικού υπολογιστή. Η μέθοδος αυτή επιλέχθηκε λόγω των δυνατοτήτων που προσφέρει, να αντληθούν δεδομένα από υπάρχουσες και τεκμηριωμένες πηγές, προσφέροντας κατανόηση του αντικειμένου. Στο παρόν κεφάλαιο αναλύεται το θεωρητικό υπόβαθρο της μεθοδολογίας, οι πηγές που αξιοποιήθηκαν καθώς και οι λόγοι επιλογής της σε σχέση με εναλλακτικές μεθόδους.

Πλεονεκτήματα

Η μεθοδολογία Desktop Research παρουσιάζει σημαντικά πλεονεκτήματα που την καθιστούν ιδιαίτερα χρήσιμη και αποδοτική. Πρώτον, ξεχωρίζει για την **κοστολογική της αποδοτικότητα**, καθώς είναι σαφώς φθηνότερη και ταχύτερη από την πρωτογενή έρευνα. Δεν απαιτείται η συλλογή νέων δεδομένων ή η εκπόνηση χρονοβόρων αναφορών· αρκεί η ανάλυση των ήδη διαθέσιμων στοιχείων, γεγονός που επιτρέπει την άμεση εξαγωγή χρήσιμων συμπερασμάτων.

Επιπλέον, συμβάλλει στην **αποφυγή διπλής εργασίας**. Μέσα από την αξιοποίηση υπαρχόντων δεδομένων, ο ερευνητής αποκτά μια ολοκληρωμένη εικόνα του θέματος και των σχετικών ζητημάτων, αποτρέποντας την περιττή επανάληψη προσπαθειών και τη σπατάλη πόρων.

Ένα ακόμη πλεονέκτημα είναι η **βελτίωση της εγκυρότητας των δεδομένων**. Μέσω της σύγκρισης και αντιπαραβολής διαφορετικών πηγών και οπτικών, ενισχύεται η αξιοπιστία της έρευνας και επιτυγχάνεται τεκμηρίωση βασισμένη σε έγκυρες και αυθεντικές πληροφορίες.

Τέλος, η Desktop Reseacrh διευκολύνει τον **εντοπισμό νέων τάσεων και προτύπων** στα δεδομένα. Με αυτόν τον τρόπο, αποκαλύπτονται κενά γνώσης ή ανεξερεύνητες περιοχές έρευνας, επιτρέποντας τη διαμόρφωση πιο στοχευμένων και αποτελεσματικών λύσεων.

Μειονεκτήματα

Η μεθοδολογία Desktop Research, παρά τη χρησιμότητά της ως μέθοδος συλλογής δευτερογενών δεδομένων, παρουσιάζει ορισμένους ουσιώδεις περιορισμούς που επηρεάζουν την εγκυρότητα και την αξιοπιστία των αποτελεσμάτων της.

Αρχικά, ένα βασικό ζήτημα αφορά την **επικαιρότητα και ακρίβεια των δεδομένων**. Συχνά, οι διαθέσιμες πληροφορίες έχουν συλλεχθεί για διαφορετικούς σκοπούς, χρονικές περιόδους ή ερευνητικά πλαίσια, γεγονός που μπορεί να περιορίζει τη συνάφειά τους με το εκάστοτε ερευνητικό ερώτημα.

Επιπλέον, το **πεδίο εφαρμογής** της μεθόδου ενδέχεται να είναι περιορισμένο, καθώς συχνά αδυνατεί να προσφέρει εις βάθος κατανόηση ποιοτικών παραμέτρων, όπως οι στάσεις, οι προτιμήσεις, τα κίνητρα και οι συμπεριφορές των καταναλωτών.

Ένα ακόμη κρίσιμο ζήτημα αφορά την **πιθανότητα μεροληψίας** των δεδομένων. Οι διαθέσιμες πηγές ενδέχεται να περιέχουν ελλιπείς ή μεροληπτικές πληροφορίες, επηρεασμένες από την ιδεολογία του εκάστοτε φορέα. Κατά συνέπεια, ενδέχεται να προκύπτουν **ασυμβατότητες** μεταξύ διαφορετικών πηγών δεδομένων, λόγω διαφοροποιημένων ορισμών, ταξινομήσεων ή μεθοδολογιών συλλογής.

Τέλος, η αξιοποίηση των δεδομένων μπορεί να παρεμποδίζεται από **νομικούς, ηθικούς ή τεχνικούς περιορισμούς**, οι οποίοι δυσχεραίνουν την πρόσβαση, τη διαχείριση και την ανάλυσή τους.

Πηγές και εργαλεία που χρησιμοποιήθηκαν

Κατά την εκπόνηση της εργασίας, αξιοποιήθηκαν οι εξής τύποι πηγών:

- **Ακαδημαϊκές βάσεις δεδομένων:** Google Scholar, IEEExplore , ScienceDirect.

Αξιολόγηση των πηγών

Η αξιολόγηση των πηγών που χρησιμοποιήθηκαν στη μελέτη βασίστηκε σε τρεις βασικούς άξονες: την επικαιρότητα, την αξιοπιστία και τη συνάφεια προς το αντικείμενο της έρευνας.

- **Επικαιρότητα:** Σε ό,τι αφορά την επικαιρότητα των πηγών, δεν υπήρχε σαφώς ορισμένο χρονικό διάστημα, λόγω του χαρακτήρα του θέματος και της διαθεσιμότητας των σχετικών δεδομένων. Ωστόσο, καταβλήθηκε προσπάθεια να προτιμηθούν πηγές που έχουν δημοσιευθεί από το 2010 και μετά, προκειμένου να διασφαλιστεί ότι τα στοιχεία και οι πληροφορίες που χρησιμοποιήθηκαν είναι σχετικά σύγχρονα και ανταποκρίνονται στις τρέχουσες εξελίξεις. Παρά την προσπάθεια αυτή, σε ορισμένες περιπτώσεις κρίθηκε απαραίτητη η χρήση παλαιότερων πηγών, όταν αυτές παρείχαν θεμελιώδη ή αναντικατάστατη γνώση για το θέμα.
- **Αξιοπιστία:** Η αξιοπιστία των πηγών αξιολογήθηκε με βάση την προέλευση τους, το κύρος του εκδότη ή του συγγραφέα, καθώς και την τεκμηρίωση που παρείχαν. Προτιμήθηκαν επιστημονικά άρθρα, επίσημες εκθέσεις, και έγκυρες βάσεις δεδομένων, ενώ αποφεύχθηκαν πηγές με ασαφές υπόβαθρο ή που παρουσίαζαν μεροληψία.
- **Συνάφεια:** Η συνάφεια των πηγών προς το αντικείμενο της μελέτης αποτέλεσε επίσης κριτήριο επιλογής. Επιλέχθηκαν μόνο εκείνες οι πηγές που σχετίζονται άμεσα με το θέμα, προκειμένου να εξασφαλιστεί η πληρότητα και η εστίαση της έρευνας.

Συνολικά, η αξιολόγηση των πηγών υπήρξε συστηματική και προσεκτική, με σκοπό τη διασφάλιση της ποιότητας και της εγκυρότητας των πληροφοριών που ενσωματώθηκαν στην παρούσα μελέτη.

Συμπεράσματα

Η επιλογή της μεθόδου Desktop Research αποδείχθηκε κατάλληλη για τις ανάγκες της παρούσας εργασίας, καθώς ανέδειξε κρίσιμες πτυχές του ερευνητικού θέματος. Παρά τα μειονεκτήματα της, η δευτερογενής έρευνα λειτούργησε ως ένα ισχυρό εργαλείο τεκμηρίωσης, πάνω στο οποίο βασίστηκε η ανάπτυξη των ερευνητικών συμπερασμάτων.

Δομή Εργασίας

Η διπλωματική εργασία είναι δομημένη σε τέσσερα κύρια κεφάλαια, καθένα από τα οποία συμβάλλει στην ολοκληρωμένη παρουσίαση και ανάλυση του θέματος της.

Κεφάλαιο Α: Εισαγωγή

Στο πρώτο κεφάλαιο γίνεται μια γενική εισαγωγή στο αντικείμενο της διπλωματικής εργασίας. Περιλαμβάνει τη σημασία και τον σκοπό της μελέτης, καθώς και τη μεθοδολογία που χρησιμοποιήθηκε για την υλοποίηση της.

Κεφάλαιο Β: Βιομετρικά Συστήματα Αυθεντικοποιήσης.

Στο δεύτερο κεφάλαιο γίνεται η ανάλυση των βιομετρικών συστημάτων. Αρχικά, αναλύονται τα βασικά υποσυστήματα των βιομετρικών συστημάτων καθώς και οι βασικές κοινές τους λειτουργίες. Στη συνέχεια, αναφέρονται τα κριτήρια με τα οποία γίνεται η αξιολόγηση των βιομετρικών συστημάτων ως προς την απόδοση και την ασφάλεια που παρέχουν. Τέλος, γίνεται αναλυτική περιγραφή των πιο ευρέως χρησιμοποιούμενων βιομετρικών συστημάτων.

Κεφάλαιο Γ: Μελέτη Ασφάλειας Βιομετρικών Συστημάτων Αυθεντικοποιήσης.

Στο τρίτο κεφάλαιο γίνεται η μελέτη ασφάλειας. Αναλύονται οι ευπάθειες των βιομετρικών συστημάτων, οι απειλές που υπάρχουν, οι πιθανές επιθέσεις καθώς και τα μέτρα προστασίας και ο αντίκτυπος των επιθέσεων.

Κεφάλαιο Δ: Επιρροή Τεχνητής Νοημοσύνης στην ασφάλεια των Βιομετρικών συστημάτων.

Στο τέταρτο κεφάλαιο εξετάζουμε πώς επηρεάζουν οι διάφορες εφαρμογές τεχνητής νοημοσύνη τη μελέτη ασφάλειας που πραγματοποιήσαμε στο τρίτο κεφάλαιο. Η μελέτη αυτή ανέδειξε την σημασία της χρήσης διαφόρων μεθόδων τεχνητής νοημοσύνης και μηχανικής μάθησης στα βιομετρικά συστήματα καθώς και στις διάφορες προκλήσεις που προκαλούνται από την χρήση κακόβουλων εργαλείων τεχνητής .Κεφάλαιο Β: Βιομετρικά Συστήματα Αυθεντικοποίησης

Β.1 Γενική Περιγραφή Βιομετρικών Συστημάτων Αυθεντικοποιήσης.

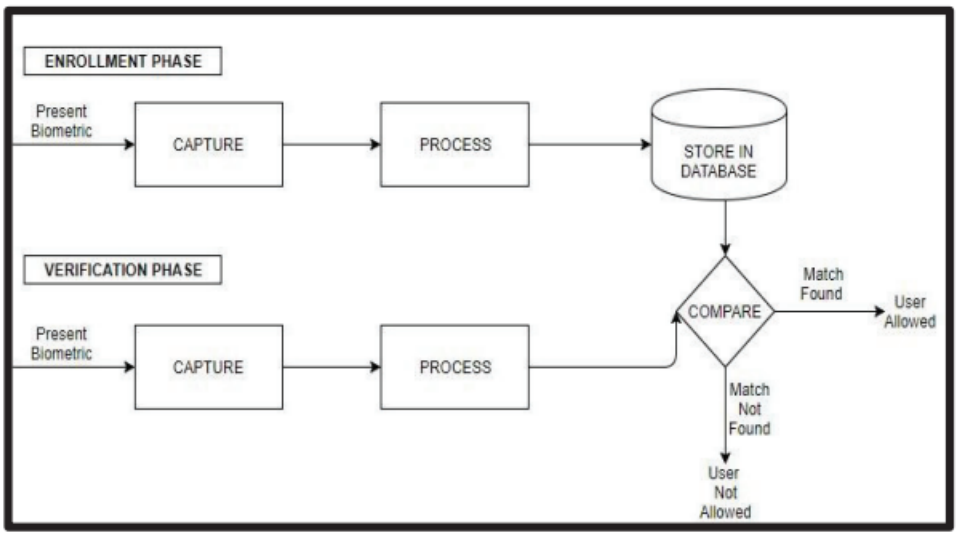
Τα βιομετρικά συστήματα αυθεντικοποίησης είναι τεχνολογίες που χρησιμοποιούν φυσικά ή συμπεριφορικά χαρακτηριστικά ενός ατόμου για να επιβεβαιώσουν την ταυτότητα του κάθε φυσικού προσώπου. Αυτά τα συστήματα συλλέγουν, αναλύουν και αποθηκεύουν βιομετρικά δεδομένα, όπως δακτυλικά αποτυπώματα, πρόσωπα, ίριδες ή φωνητικές ενδείξεις προκειμένου να τα συγκρίνουν με τα ήδη αποθηκευμένα πρότυπα και να επιβεβαιώσουν αν το άτομο που ζητά πρόσβαση είναι πράγματι αυτό που ισχυρίζεται. Η διαδικασία αυτή συμβάλλει στην ενίσχυση της ασφάλειας, μειώνει τον κίνδυνο υποκλοπής ή πλαστοπροσωπίας και προσφέρει ευκολία στη χρήση σε σύγκριση με παραδοσιακές μεθόδους, όπως κωδικούς ή κάρτες πρόσβασης.

Τα βιομετρικά συστήματα προσφέρουν υψηλή ακρίβεια στην αναγνώριση της ταυτότητας και είναι ιδιαίτερα δύσκολο να αντιγραφούν ή να πλαστογραφηθούν. Επιπλέον, εξασφαλίζουν άνεση και ταχύτητα στη διαδικασία αυθεντικοποίησης, ενώ απαλλάσσουν τον χρήστη από την ανάγκη απομνημόνευσης κωδικών ή την κατοχή φυσικών καρτών πρόσβασης.

Παρά τα οφέλη τους, τα συστήματα αυτά παρουσιάζουν και μειονεκτήματα. Το κόστος εγκατάστασης και συντήρησής τους είναι συχνά υψηλό, ενώ εγείρονται σοβαρές ανησυχίες για την προστασία και την ιδιωτικότητα των προσωπικών δεδομένων. Επιπλέον, η αξιοπιστία τους μπορεί να επηρεαστεί σε περιπτώσεις τραυματισμών, ασθενειών ή μεταβολών στα φυσικά χαρακτηριστικά του ατόμου. Τέλος, σε περίπτωση που τα βιομετρικά δεδομένα παραβιαστούν, η απώλεια ασφάλειας είναι μη αναστρέψιμη, καθώς τα βιομετρικά χαρακτηριστικά των ανθρώπων είναι κατά κύριο λόγο αμετάβλητα.

Β.1.1 Βασικές Λειτουργίες Βιομετρικών Συστημάτων.

Κάθε βιομετρικό σύστημα αυθεντικοποιήσης εκτελεί δύο κύριες διαδικασίες. Η πρώτη διαδικασία αφορά στη διαδικασία δημιουργίας και αποθήκευσης του βιομετρικού προτύπου (φάση εγγραφής) και η δεύτερη διαδικασία περιλαμβάνει την αυθεντικοποιήση των χρηστών. Οι παραπάνω διαδικασίες απεικονίζονται στην **Εικόνα 1**.



Εικόνα 1: Γενικό διάγραμμα συστήματος βιομετρική αυθεντικοποίησης

Β.1.2.1 Φάση Εγγραφής.

Η πρώτη διαδικασία που περιλαμβάνει τη διαδικασία δημιουργίας και αποθήκευσης του βιομετρικού προτύπου (φάση εγγραφής) λειτουργεί ως εξής: Κάθε βιομετρικό σύστημα διαχειρίζεται μια βάση δεδομένων είτε τοπική είτε αποθηκευμένη σε κάποια cloud υπηρεσία . Όταν ένας νέος χρήστης πρόκειται να χρησιμοποιήσει ένα βιομετρικό σύστημα, καταρχάς πρέπει να πραγματοποιηθεί επιτυχώς η διαδικασία εγγραφής. Η διαδικασία αυτή απαιτεί από τον χρήστη να εισάγει στην είσοδο του βιομετρικού το απαραίτητο βιομετρικό χαρακτηριστικό του, ώστε να δημιουργηθεί το βιομετρικό πρότυπο το οποίο θα αποθηκευτεί σε μια βάση δεδομένων, και θα χρησιμοποιηθεί μελλοντικά για αυθεντικοποίηση.

Β.1.2.2 Φάση Αυθεντικοποιήσης.

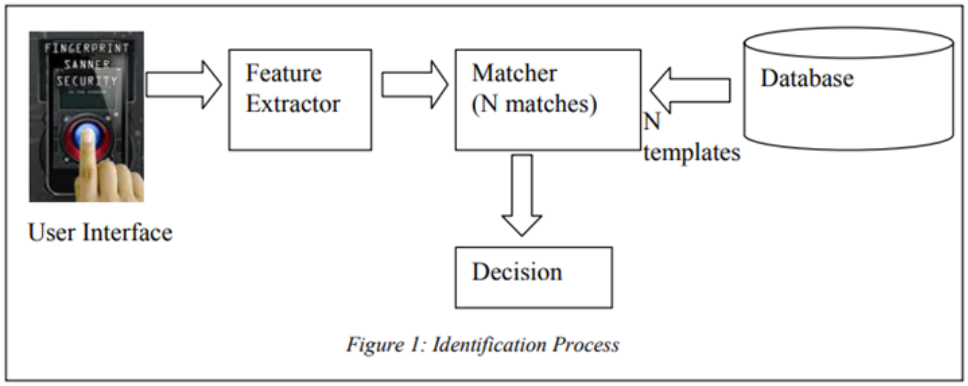
Η δεύτερη διαδικασία που ακολουθεί τη φάση εγγραφής είναι η φάση της αυθεντικοποίησης. Κατά τη φάση αυτή, τα βιομετρικά συστήματα πραγματοποιούν τη διαδικασία της αυθεντικοποιήσης με δύο τρόπους, με αναγνώριση ή με επιβεβαίωση. Η επιλογή της μεθόδου αυθεντικοποιήσης εξαρτάται από τον βαθμό ασφαλείας που θέλουμε να επιτύχουμε. Οι δύο αυτές μέθοδοι αναλύονται ως εξής:

- **Αυθεντικοποίηση με Αναγνώριση (Authentication with identification).**

Η αυθεντικοποίηση με αναγνώριση, επιτυγχάνεται με την αναγνώριση της ταυτότητας ενός ανώνυμου χρήστη από μια βάση δεδομένων με αποθηκευμένα βιομετρικά πρότυπα (Biometrical templates). Αρχικά, ο χρήστης εισάγει στην είσοδο του βιομετρικού συστήματος, το βιομετρικό χαρακτηριστικό που απαιτείται. Έπειτα, γίνεται σύγκριση με όλες τις εγγραφές στη βάση δεδομένων προκειμένου να ταυτοποιηθεί ο χρήστης. Αν η είσοδος ταιριάζει με

κάποια αποθηκευμένη έγγραφη στη βάση, τότε επιτρέπεται η είσοδος στο σύστημα. Η διαδικασία αυτή απεικονίζεται στην Εικόνα 2.

Ένα πρακτικό παράδειγμα είναι η εφαρμογή αναγνώρισης προσώπου σε Αεροδρόμια και δημόσιοι χώροι. Σαρώνονται πλήθη με κάμερες για να αναγνωριστούν ζητούμενοι κακοποιοί ή αγνοούμενα πρόσωπα.

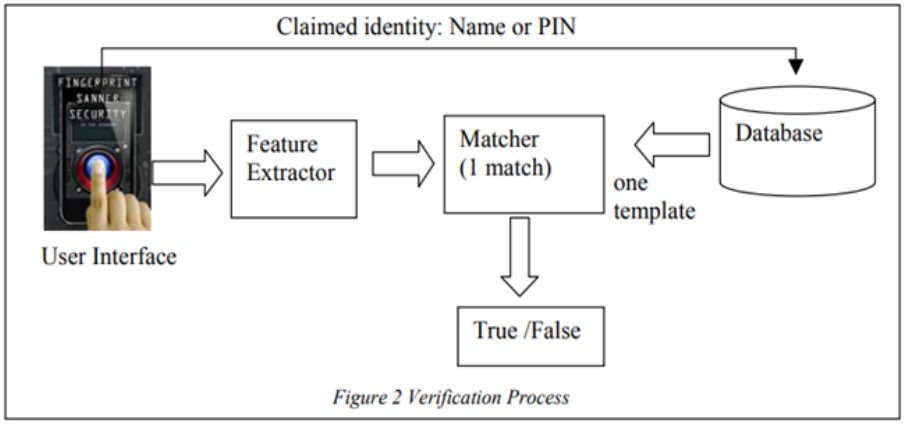


Εικόνα 2: Διάγραμμα συστήματος αυθεντικοποιήσης με αναγνώριση

- Αυθεντικοποίηση με Επιβεβαίωση (Authentication with Verification).

Αντίθετα, η αυθεντικοποίηση με επιβεβαίωση είναι η διαδικασία επιβεβαίωσης ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι. Σε αυτή την περίπτωση, ο χρήστης παρέχει τα βιομετρικά του δεδομένα, τα οποία συγκρίνονται με ένα συγκεκριμένο δείγμα που έχει αποθηκευτεί στο σύστημα. Αυτή η μέθοδος επιβεβαιώνει την ταυτότητα του χρήστη σε σχέση με ένα συγκεκριμένο αναγνωριστικό, όπως παραδείγματος χάριν έναν κωδικό πρόσβασης (password) ή ένα όνομα χρήστη (username). Αυτή η μέθοδος αυθεντικοποιήσης χρησιμοποιείται όταν θέλουμε να επιτύχουμε μεγαλύτερο βαθμό ασφάλειας. Η διαδικασία απεικονίζεται στην Εικόνα 3.

Κλασικό παράδειγμα χρήσης αυθεντικοποίησης με επιβεβαίωση είναι το ξεκλείδωμα των κινητών τηλεφώνων με τη χρήση κάποιου βιομετρικού χαρακτηριστικού του χρήστη. Σε αυτές τις εφαρμογές το τηλέφωνο ελέγχει αν το χαρακτηριστικό ταιριάζει με αυτό που έχει αποθηκευτεί και ξεκλειδώνει. Επίσης, στις τραπεζικές εφαρμογές e-banking όταν ο χρήστης προσπαθεί να συνδεθεί, εισάγει κάποιο βιομετρικό χαρακτηριστικό για την είσοδο του στην εφαρμογή.



Εικόνα 3 Διάγραμμα συστήματος αυθεντικοποιήσης με επιβεβαίωση.

Β.1.3 Αρχές των Βιομετρικών Χαρακτηριστικών.

Οποιοδήποτε βιολογικό ή συμπεριφορικό ανθρώπινο χαρακτηριστικό μπορεί να χαρακτηριστεί ως βιομετρικό εφόσον εκπληρώνει τις απαιτήσεις, της Καθολικότητας (Universality), της Μοναδικότητας (Uniqueness), της Μονιμότητας (Permanence), της Συλλεκτικότητας (Collectability). Ωστόσο για τα βιομετρικά συστήματα αυθεντικοποιήσης, υπάρχουν και κάποια επιπλέον στοιχεία που πρέπει να ικανοποιούνται, αυτά της Απόδοσης (Performance), της Αποδοχής χρηστών (Acceptance) και του βαθμού δυνατότητας Παραπλάνησης (Circumvention).

Τα παραπάνω χαρακτηριστικά χρησιμοποιούνται για την επιλογή των βιομετρικών συστημάτων. Παρακάτω φαίνεται η ανάλυση τους [1][2]:

1. Καθολικότητα (Universality): Η καθολικότητα αναφέρεται στο πόσο συχνή είναι εμφάνιση του χαρακτηριστικού στα φυσικά πρόσωπα. Όσο πιο υψηλή είναι η καθολικότητα τόσο πιο πολλούς χρήστες μπορεί να εξυπηρετήσει το σύστημα.
2. Μοναδικότητα (Uniqueness): Η μοναδικότητα αναφέρεται στο πόσο διαφορετικό είναι ένα βιομετρικό χαρακτηριστικό σε κάθε άτομο. Όσο μεγαλύτερη είναι η μοναδικότητα τόσο πιο ακριβής είναι η αυθεντικοποιήση.
3. Μονιμότητα (Permanence): Η μονιμότητα αναφέρεται στο πόσο αναλλοίωτο διατηρείται ένα χαρακτηριστικό με την πάροδο του χρόνου.
4. Συλλεκτικότητα (Collectability): Η συλλεκτικότητα αναφέρεται στο πόσο εύκολο είναι να συλλέξουμε και να ποσοτικοποιήσουμε τα βιομετρικά δεδομένα.
5. Απόδοση (Performance): Η απόδοση αναφέρεται στην επιτεύξιμη ακρίβεια και ταχύτητα ταυτοποίησης, στους πόρους που απαιτούνται για να τις επιτύχουμε και στους λειτουργικούς και περιβαλλοντικούς παράγοντες που τις επηρεάζουν.

6. Αποδοχή (Acceptance): Η αποδοχή αναφέρεται στο πόσο αποδεκτή είναι η χρήση του βιομετρικού συστήματος από τους χρήστες.
7. Δυνατότητα Παραπλάνησης (τρωτότητα) (Circumvention): Η δυνατότητα παραπλάνησης αναφέρεται στο πόσο δύσκολο είναι να προσπελασθεί το σύστημα από κακόβουλους χρήστες.

Β.1.4 Χαρακτηριστικά που επηρεάζουν την απόδοση των Βιομετρικών Συστημάτων Αυθεντικοποιήσης.

Πολύ σημαντικό, όμως, είναι να αξιολογήσουμε και την απόδοση των βιομετρικών συστημάτων. Τα χαρακτηριστικά των συστημάτων τα οποία χρησιμοποιούμε είναι αυτά της Ασφάλειας (Security), της Άνεσης Χρήσης (Convenience), της Διαλειτουργικότητας (Interoperability), της Επεκτασιμότητας (Scalability), του Κόστους (Cost), της Ιδιωτικότητας (Privacy) και της Ανθεκτικότητας (Robustness) [2].

Παρακάτω αναλύουμε τα χαρακτηριστικά που προαναφέραμε:

1. Ασφάλεια (Security): Η ασφάλεια αναφέρεται στην ικανότητα του συστήματος να ταυτοποιεί τους χρήστες αξιόπιστα και με ακρίβεια.
2. Άνεση Χρήσης (Convenience): Η άνεση χρήσης αναφέρεται στο πόσο απλή είναι η χρήση του συστήματος από τους χρήστες.
3. Διαλειτουργικότητα (Interoperability): Η διαλειτουργικότητα αναφέρεται στην ικανότητα του συστήματος να λειτουργεί σε συνεργασία με άλλα διαφορετικά συστήματα και συσκευές.
4. Επεκτασιμότητα (Scalability): Η επεκτασιμότητα αναφέρεται στην ικανότητα του συστήματος να διαχειριστεί μεγάλο αριθμό χρηστών χωρίς να επηρεαστούν οι επιδώσεις του.
5. Κόστος (Cost): Το κόστος αναφέρεται στο χρηματικό ποσό που πρέπει να δαπανηθεί για την ανάπτυξη, την εγκατάσταση, τη χρήση και τη συντήρηση του συστήματος.
6. Ιδιωτικότητα (Privacy): Η ιδιωτικότητα αναφέρεται στην ικανότητα του συστήματος να προστατεύσει τις προσωπικές πληροφορίες των χρηστών του.
7. Ανθεκτικότητα (Robustness): Η ανθεκτικότητα αναφέρεται στην ικανότητα του συστήματος να αντιστέκεται σε πιθανές επιθέσεις καθώς και σε σφάλματα.

Β.1.5 Χαρακτηριστικά που επηρεάζουν τον βαθμό ασφαλείας των Βιομετρικών Συστημάτων Αυθεντικοποίησης.

Η εκτίμηση του βαθμού ασφαλείας είναι επίσης απαραίτητη για την επιλογή του κατάλληλου βιομετρικού συστήματος αυθεντικοποίησης. Κατά την επιλογή, πρέπει να φροντίζουμε, ο βαθμός

ασφαλείας να είναι υψηλός προκειμένου να εξασφαλίσουμε αξιόπιστη αυθεντικοποιήση και κατ' επέκταση, καλύτερη προστασία των δεδομένων των χρηστών [4].

Τα χαρακτηριστικά που επηρεάζουν την ασφάλεια των Βιομετρικών Συστημάτων Αυθεντικοποιήσης είναι τα:

1. False Accept Rate (FAR): Υπολογίζει την πιθανότητα μια είσοδος να θεωρηθεί αντίστοιχη με κάποια αποθηκευμένη εγγραφή στη βάση δεδομένων, χωρίς όμως να είναι. Η λανθασμένη αυτή αντιστοιχία προκαλεί λανθασμένη αυθεντικοποιήση.
2. False Reject Rate (FRR) or False Non-Match Rate (FNMR): Υπολογίζει την πιθανότητα το σύστημα να δηλώσει εσφαλμένα την αποτυχία αντιστοίχισης μεταξύ της εισόδου και της αντίστοιχης εγγραφής στη βάση δεδομένων.
3. Relative Operating Characteristic (ROC): Είναι μια γραφική παράσταση η οποία εξαρτάται από τις τιμές FAR και FRR. Χρησιμοποιείται για να πετύχουμε τη μεγαλύτερη δυνατή ασφάλεια με τη μεγαλύτερη δυνατή ευχρηστία.
4. Equal Error Rate (EER): Είναι το σημείο στο οποίο η πιθανότητα FAR και η πιθανότητα FRR είναι ίσες. Πιο συγκεκριμένα, είναι το πλήθος των χρήσεων του συστήματος κατά το οποίο το σύστημα αποδέχεται λανθασμένα μη εξουσιοδοτημένους χρήστες (FAR) και απορρίπτει εξουσιοδοτημένους χρήστες (FRR) στο ίδιο επίπεδο. Ο δείκτης EER παρέχει μια μοναδική τιμή που βοηθά στην αξιολόγηση της συνολικής απόδοσης του συστήματος – χαμηλότερες τιμές EER συνήθως δείχνουν ένα πιο ακριβές βιομετρικό σύστημα.
5. Failure to Enroll Rate (FTE or FER): Παρουσιάζει το ποσοστό από βιομετρικά πρότυπα που αποτυγχάνουν να αποθηκευτούν στο σύστημα. Η αποτυχία αποθήκευσης συχνά συμβαίνει όταν η είσοδος θεωρείται μη αποδεκτή ή όταν η ποιότητά της είναι χαμηλή.
6. Failure to Capture Rate (FTC): Υπολογίζει την πιθανότητα το σύστημα να αποτύχει να αναγνωρίσει έναν χρήστη από βιομετρικό χαρακτηριστικό του, όταν αυτό εισάγεται σωστά στην είσοδό του.
7. Template Capacity: Παρουσιάζει τον μέγιστο αριθμό από βιομετρικά χαρακτηριστικά που μπορεί το σύστημα αποθηκεύσει στη βάση δεδομένων του.

Β.2 Ανάλυση Βιομετρικών Συστημάτων Αυθεντικοποιήσης.

Στο κεφάλαιο αυτό θα αναλύσουμε τα βιομετρικά συστήματα τα οποία θα μελετήσουμε ως προς την τρωτότητα τους. Η επιλογή των βιομετρικών συστημάτων έγινε με βάση την εφαρμογή τους για αυθεντικοποιήση χρηστών. Επειδή υπήρχαν πολλοί διαφορετικοί τύποι για κάθε κατηγορία βιομετρικού συστήματος στα επιστημονικά άρθρα, επιλέχθηκε εκείνος που θεωρούμε, με βάση τις πηγές, ότι χρησιμοποιείται περισσότερο και που καλύπτει μια .

Β.2.2 Συστήματα Αναγνώρισης Δαχτυλικών Αποτυπωμάτων.

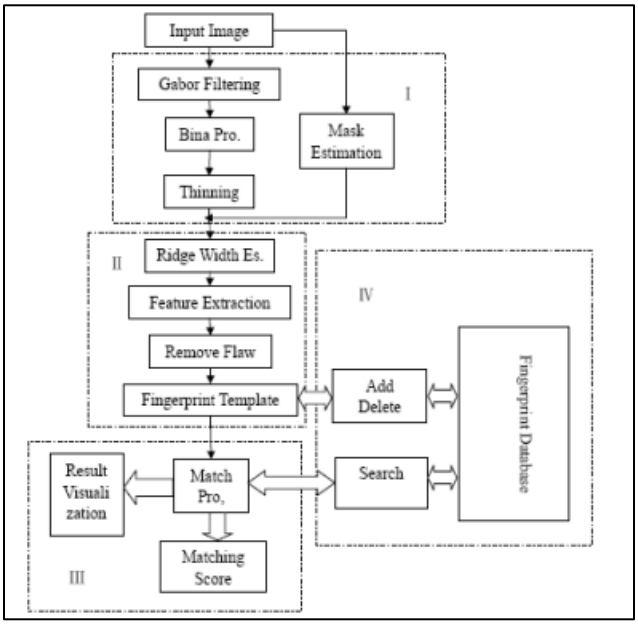
Β.2.2.1 Εισαγωγή.

Η ταυτοποίηση μέσω δαχτυλικών αποτυπωμάτων είναι η παλαιότερη και η πιο γνωστή μέθοδος βιομετρικής ταυτοποίησης. Το γεγονός ότι κάθε άτομο έχει διαφορετικό δαχτυλικό αποτύπωμα βοήθησε στην εκτεταμένη χρήση συστημάτων αναγνώρισης δαχτυλικών αποτυπωμάτων.

Στα σύγχρονα συστήματα αναγνώρισης δαχτυλικών αποτυπωμάτων χρησιμοποιούνται οπτικά, θερμικά, πυριτικά ή υπερηχητικά μέσα. Ο οπτικός αναγνώστης δακτυλικών αποτυπωμάτων είναι ο πιο κοινός αυτή τη στιγμή και έχει την ικανότητα να αξιολογεί και να προσαρμόζει το αποτύπωμα με τα καταγεγραμμένα δείγματα. Περιλαμβάνει την πηγή φωτός, τον αισθητήρα φωτός και μια ειδική επιφάνεια ανάκλασης που μεταβάλλει την ανάκλαση ανάλογα με την πίεση. Κάποιοι από τους αναγνώστες είναι επίσης εξοπλισμένοι με μικροτσίπ για καλύτερη απόδοση κατά την δημιουργία της αρχικής εικόνας [4].

Β.2.2.2 Βασικές λειτουργίες Συστημάτων Αναγνώρισης Δαχτυλικών Αποτυπωμάτων.

Κάθε σύστημα αυθεντικοποιήσης δαχτυλικών αποτυπωμάτων εκτελεί τέσσερεις βασικές λειτουργίες, την προεπεξεργασία εικόνας δακτυλικών αποτυπωμάτων (Fingerprint image preprocessing), την εξαγωγή χαρακτηριστικών κάθε δαχτυλικού αποτυπώματος (Feature extraction), την ταυτοποίηση των χρηστών (Fingerprint matching) και τη Διαχείριση βάσης δεδομένων δακτυλικών αποτυπωμάτων (Fingerprint database management), όπως βλέπουμε στην **Εικόνα 4**.



Εικόνα 4 Βιομετρικό Σύστημα Αναγνώρισης Δαχτυλικών Αποτυπωμάτων.

Αρχικά, το σύστημα, μέσω μιας συσκευής εισόδου (αναγνώστης), δημιουργεί μια εικόνα από το δαχτυλικό αποτύπωμα του χρήστη. Η εικόνα αυτή θα χρησιμοποιηθεί από τις υπόλοιπες λειτουργίες του συστήματος.

Μετά την ανάγνωση, ξεκινάει η διαδικασία της Προεπεξεργασίας. Σε αυτή τη φάση οι εικόνες τροποποιούνται ώστε να μπορέσουν να χρησιμοποιηθούν από τις επόμενες λειτουργίες του συστήματος. Αρχικά, εκτελείται η αναπαράσταση της αρχικής εικόνας σε εικόνα με 8 bits ανά pixel. Αυτό το βήμα είναι σημαντικό επειδή η αρχική εικόνα που δημιουργείται έχει υψηλή ανάλυση και, κατά συνέπεια, περισσότερη πληροφορία από αυτή που απαιτείται για τις λειτουργίες του συστήματος. Η ολοκλήρωση αυτής της διαδικασίας δίνει τη δυνατότητα να αποθηκεύονται στο σύστημα εικόνες με μικρότερο μέγεθος. Στη συνέχεια, ξεκινάει η διαδικασία της βελτίωσης της εικόνας (image enhancement) η αφαίρεση του θορύβου προκειμένου να εξασφαλιστεί η καθαρότητα και η σαφήνεια των λεπτομερειών. Αυτό βοηθά στην ακριβή αναγνώριση των αποτυπωμάτων, αποφεύγοντας σφάλματα που μπορεί να προκύψουν από θόρυβο ή κακής ποιότητας εικόνες. Με αυτόν τον τρόπο, βελτιώνεται η αξιοπιστία και η απόδοση του συστήματος ταυτοποίησης. .

Η βελτίωση περιλαμβάνει το φιλτράρισμα της εικόνας, τον προσανατολισμό της εικόνας εισόδου, την εκτίμηση της μάσκας (mask) του δαχτυλικού αποτυπώματος, την εικόνα δηλαδή που χρησιμοποιείται για να προσδιορίσει τις περιοχές της εικόνας αποτυπώματος όπου υπάρχουν χρήσιμες πληροφορίες, όπως οι γραμμές και οι κοιλότητες, τον υπολογισμό της συχνότητας στις ράχες του αποτυπώματος, την αραίωση για να μετατρέψει τις παχιές γραμμές του αποτυπώματος σε λεπτές, διευκολύνοντας έτσι την αναγνώριση και ανάλυση χαρακτηριστικών όπως οι διακλαδώσεις και οι τερματισμοί των γραμμών και την κανονικοποίηση της εικόνας.

Η βελτίωση των εικόνων πραγματοποιείται με τη χρήση των φίλτρων Gabor και του μετασχηματισμού διακριτού συνημιτονιακού μετασχηματισμού (Discrete Cosine Transform – DCT). Η μέθοδος DCT και το Gabor WT συνδυάστηκαν για να εξάγουν τα χαρακτηριστικά από τις εικόνες και για τη μείωση της διαστασιμότητας ,της μεταξύ τους δηλαδή απόστασης. Στη συνέχεια, η ταξινόμηση γίνεται με τον αλγόριθμο του πλησιέστερου γείτονα (Nearest Neighbor Algorithm). Πραγματοποιείται, επίσης, προσανατολισμός της εικόνας εισόδου, ώστε να φέρει την εικόνα σε μια καθορισμένη από το σύστημα θέση. Οι εικόνες των δακτυλικών αποτυπωμάτων που δημιουργούνται κατά την είσοδο πρέπει να έχουν μια συγκεκριμένη κατεύθυνση, ώστε να μπορεί το σύστημα να τις αντιστοιχήσει με τις εικόνες που είναι αποθηκευμένες στη βάση δεδομένων και να ταυτοποιήσει τους χρήστες. Το βήμα του προσανατολισμού της εικόνας είναι απαραίτητο πριν από τη διαδικασία εξαγωγής χαρακτηριστικών και αντιστοίχισης. Πραγματοποιείται, επίσης, η διαδικασία της αύξησης του πλάτους των ραχών των δαχτυλικών αποτυπωμάτων στις εικόνες. Αυτή θεωρείται ζωτικής σημασίας διαδικασία, καθώς βοηθάει στη δημιουργία του τελικού βελτιωμένου προτύπου που αποτυπώματος. Τέλος, η βελτιστοποίηση ολοκληρώνεται με την

κανονικοποίηση της βελτιωμένης εικόνας προκειμένου να ταιριάζει με τις προδιαγραφές μεγέθους του συστήματος. Με αυτό τον τρόπο αυξάνεται η πιθανότητα για μια ορθή εκτίμηση κατά τη διαδικασία της αντιστοίχισης.

Μετά από την προεπεξεργασία, ξεκινάει η διαδικασία εξαγωγής των χαρακτηριστικών των δαχτυλικών αποτυπωμάτων. Είναι ίσως η πιο σημαντική διαδικασία των συστημάτων, και επηρεάζεται άμεσα από τη διαδικασία της προεπεξεργασίας. Η ορθή ολοκλήρωσή της εξάγει τις λεπτομέρειες των δαχτυλικών αποτυπωμάτων.

Οι λεπτομέρειες ορίζονται ως τα βασικά σημεία σε οποιαδήποτε εικόνα δακτυλικού αποτυπώματος και αποτελούνται από τα άκρα των ακμών και τις διακλαδώσεις τους. Τα χαρακτηριστικά αυτά είναι μοναδικά σε κάθε άτομο, συνεπώς θεωρούνται κατάλληλα για την αναγνώριση της ταυτότητας του χρήστη. Τα εξαγόμενα χαρακτηριστικά ενός δακτυλικού αποτυπώματος ενδέχεται να περιέχουν αρκετές ψευδείς λεπτομέρειες, λόγω της αναπόφευκτης ανακρίβειας ,όπως βρόχους (loop), γέφυρες (bridge) κ.λπ.

Υπάρχει επίσης, και η διαδικασία της ταυτοποίησης των χρηστών. Με αυτή τη διαδικασία, τα συστήματα αυθεντικοποιούν τους χρήστες χρησιμοποιώντας την εικόνα εισόδου και τα αποθηκευμένα πρότυπα στη βάση δεδομένων. Αυτή η διαδικασία είναι υπεύθυνη για την αναγνώριση της ταυτότητας των χρηστών.

Τέλος, όπως κάθε σύστημα βιομετρικής αυθεντικοποιήσης, έτσι και τα συστήματα δαχτυλικών αποτυπωμάτων περιλαμβάνουν και κάποιες λειτουργίες διαχείρισης μιας βάσης δεδομένων, είτε εσωτερικής είτε απομακρυσμένης. Οι κύριες λειτουργίες είναι η αποθήκευση, η διαγραφή και η αναζήτηση εικόνων των δαχτυλικών αποτυπωμάτων των χρηστών. Κάθε σύστημα αποθηκεύει, ένα πρότυπο για κάθε χρήστη, ώστε να μπορεί να χρησιμοποιηθεί μελλοντικά για την ταυτοποίηση, μπορεί να αναζητά τα πρότυπα των χρηστών κατά την ταυτοποίηση και τέλος μπορεί να διαγράψει, αν χρειαστεί, κάποια εγγραφή.

Κλείνοντας, οι παραπάνω διαδικασίες είναι κοινές για κάθε σύστημα αναγνώρισης δαχτυλικών αποτυπωμάτων. Παρ’ όλα αυτά, υπάρχουν διαφοροποιήσεις [3][5] σε κάθε σύστημα ανάλογα με το επίπεδο ακριβείας και ασφάλειας που απαιτείται.

Β.2.3 Συστήματα Αναγνώρισης ίριδας.

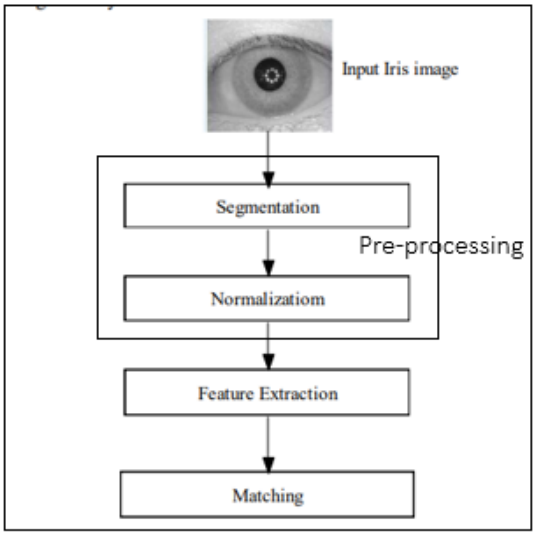
Β.2.3.1 Εισαγωγή.

Η αναγνώριση της ίριδας είναι μια αξιόπιστη τεχνική βιομετρικής αυθεντικοποίησης που ταυτοποιεί τους χρήστες με βάση τα μοναδικά μοτίβα που βρίσκονται στην περιοχή γύρω από την κόρη του ματιού. Η ίριδα περιέχει, περίπλοκες λεπτομέρειες όπως κρύπτες, ακτινωτές αυλακώσεις, νήματα, χρωστικές κροκίδες, κηλίδες, γραμμές και καμπύλιους συνδέσμους, που

συνθέτουν ένα μοναδικό μοτίβο για κάθε άτομο. Η τυχαία διασπορά των παραπάνω χαρακτηριστικών την καθιστά ένα από τα πιο αξιόπιστα βιομετρικά χαρακτηριστικά, με αποτέλεσμα η αναγνώριση της ίριδας αποτελεί ένα ευρέως εφαρμόσιμο εργαλείο στον τομέα της αυθεντικοποίησης χρηστών.

Β.2.3.2 Βασικές λειτουργίες Συστημάτων Αναγνώρισης ίριδας.

Οι βασικές λειτουργίες που εκτελεί ένα σύστημα αναγνώρισης της ίριδας για τη φάση της προεπεξεργασίας είναι η Τμηματοποίηση (Segmentation), η Κανονικοποίηση (Normalization), η Εξαγωγή χαρακτηριστικών (Feature Extraction), η Αναγνώριση της ταυτότητας του χρήστη (Matching) όπως φαίνεται στην **Εικόνα 5.** Επίσης όπως και σε όλα τα βιομετρικά συστήματα εκτελείται διαχείριση βάσης δεδομένων, η οποία αφορά την αποθήκευση και οργάνωση των προτύπων της ίριδας ώστε να είναι δυνατή η γρήγορη και αξιόπιστη ανάκτηση κατά τη διαδικασία ταυτοποίησης.



Εικόνα 5 Βιομετρικό Σύστημα Αναγνώρισης Ίριδας .

Αρχικά, η συσκευή εισόδου αναγνώρισης καταγράφει ένα στιγμιότυπο του οφθαλμού του χρήστη, το οποίο θα χρησιμοποιηθεί για όλες τις λειτουργίες του συστήματος. Στη συνέχεια, ακολουθεί η διαδικασία της προεπεξεργασίας της εικόνας αυτής.

Κατά τη διαδικασία της προεπεξεργασίας της εικόνας αρχικά πραγματοποιείται τμηματοποίηση. Η τμηματοποίηση είναι η διαδικασία κατά την οποία απλοποιείται και αλλάζει η αναπαράσταση της εικόνας σε μορφή που είναι πιο εύκολο να αναλυθεί και να χρησιμοποιηθεί από το σύστημα. Η ίριδα, μπορεί να προσεγγιστεί από δύο κύκλους, έναν για τα όρια ίριδας-χιτώνα και έναν για τα όρια ίριδας-κόρης. Έπειτα, χρησιμοποιείται ο μετασχηματισμός Hough [23] ,για την εύρεση της ακτίνας και των συντεταγμένων του κέντρου της κόρης και την εύρεση της περιοχής της ίριδας. Τέλος, ορίζονται τα εσωτερικά και εξωτερικά όρια της ίριδας.

Όμως, σε κάθε χρήση του συστήματος, η περιοχή που περικλείεται από τα εσωτερικά και εξωτερικά όρια της ίριδας μπορεί να ποικίλει λόγω της διαστολής και συστολής της κόρης. Συνεπώς, η επίδραση αυτών των μεταβολών πρέπει να ελαχιστοποιηθεί πριν από τη διαδικασία της ταυτοποίησης του χρήστη. Για αυτόν τον λόγο μετά από την τμηματοποίηση εκτελείται η διαδικασία της κανονικοποίησης. Σε αυτό το βήμα της προεπεξεργασίας, η τμηματοποιημένη περιοχή της ίριδας αντιστοιχίζεται σε μια περιοχή σταθερών διαστάσεων. Με την ολοκλήρωση του σταδίου της κανονικοποίησης, μπορεί το σύστημα να προχωρήσει στην εξαγωγή των χαρακτηριστικών της ίριδας.

Με την εξαγωγή χαρακτηριστικών (feature extraction), τα στοιχεία της ίριδας αποτυπώνονται σε ένα διάνυσμα χαρακτηριστικών, το οποίο αποτελείται από την τακτοποιημένη ακολουθία που δημιουργείται από τις διάφορες αναπαραστάσεις των εικόνων της ίριδας. Η πιο συνηθισμένη τακτική εξαγωγής είναι τα φίλτρα Gabor. Αυτή η μέθοδος περιλαμβάνει τη διαίρεση της επιφάνειας σε τμήματα, την εξαγωγή των χαρακτηριστικών με την εφαρμογή δισδιάστατων φίλτρων Gabor και την κανονικοποίηση της εικόνας για τον προσανατολισμό της. Ιδιαίτερα εκτεταμένη είναι και η χρήση του DCT για την εξαγωγή των χαρακτηριστικών της ίριδας σε συστήματα με χαμηλή υπολογιστική πολυπλοκότητα και υψηλή ακρίβεια. Τα δεδομένα εισόδου αναπαρίστανται ως άθροισμα συνημίτονων διαφορετικών μεγεθών και συχνοτήτων, ώστε το σήμα να αποσυντίθεται στα βασικά του συστατικά.

Επίσης, κάθε σύστημα, εκτελεί και τη διαδικασία της αναγνώρισης της ταυτότητας των χρηστών. Η διαδικασία της ταυτοποίησης των χρηστών είναι το στάδιο εκείνο, στο οποίο το πρότυπο της ίριδας συγκρίνεται με την εικόνα της ίριδας που είναι αποθηκευμένη στη βάση δεδομένων. Οι διάφορες τεχνικές που χρησιμοποιούνται περιλαμβάνουν την απόσταση Hamming, τη σταθμισμένη Ευκλείδεια απόσταση και την κανονικοποιημένη συσχέτιση.

Τέλος, κάθε σύστημα αναγνώρισης ίριδας διαχειρίζεται μια βάση δεδομένων. Οι κύριες λειτουργίες είναι η αποθήκευση, η διαγραφή και η αναζήτηση προτύπων της ίριδας των χρηστών. Κάθε σύστημα αποθηκεύει ένα πρότυπο για κάθε χρήστη, μετά την εξαγωγή χαρακτηριστικών, ώστε το πρότυπο αυτό να μπορεί να χρησιμοποιηθεί μελλοντικά για την ταυτοποίηση. Επίσης, υπάρχει η λειτουργία αναζήτησης των προτύπων κατά την εξακρίβωση της ταυτότητας του χρήστη. Και τέλος, κάθε σύστημα μπορεί να διαγράψει τα αποθηκευμένα πρότυπα όποτε αυτό χρειάζεται.

Οι παραπάνω διαδικασίες είναι κοινές για κάθε σύστημα αναγνώρισης της ίριδας του οφθαλμού. Υπάρχουν όμως διαφοροποιήσεις σε κάθε σύστημα ανάλογα με το επίπεδο ακριβείας και ασφάλειας που απαιτείται.

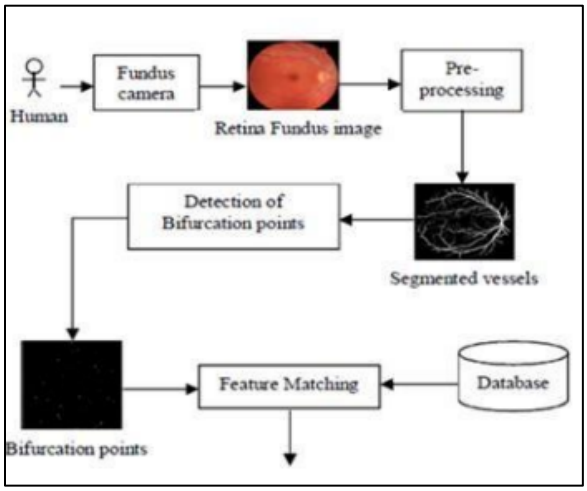
Β.2.4 Συστήματα Αναγνώρισης κερατοειδούς.

Β.2.4.1 Εισαγωγή.

Ο ανθρώπινος κερατοειδής είναι ένας ευαίσθητος ιστός που παρουσιάζει μοναδική δομή και σχέδιο αιμοφόρων αγγείων για κάθε άτομο, εκτός εάν επηρεαστεί από κάποια παθολογική κατάσταση. Η μοναδικότητα του κερατοειδούς επιτρέπει την ανάπτυξη και χρήση βιομετρικών συστημάτων, τα οποία χρησιμοποιούν τον κερατοειδή ως βιομετρικό χαρακτηριστικό αυθεντικοποίησης [1].

Β.2.4.2 Βασικές λειτουργίες Συστημάτων Αναγνώρισης κερατοειδούς.

Όπως βλέπουμε στην **εικόνα 6**, τα συστήματα αναγνώρισης του κερατοειδούς χιτώνα εκτελούν τη λειτουργία της προεπεξεργασίας εικόνας (Pre-processing), του εντοπισμού των διακλαδώσεων (Detection of bifurcation points), της αντιστοίχισης (Matching) και της διαχείρισης μιας βάσης δεδομένων.



Εικόνα 6 Βιομετρικό Σύστημα Αναγνώρισης Κερατοειδούς.

Αρχικά, το σύστημα χρησιμοποιώντας μια συσκευή εισόδου δημιουργεί μια αρχική εικόνα του οφθαλμού του χρήστη. Αυτή η εικόνα θα χρησιμοποιηθεί από τις υπόλοιπες λειτουργίες του συστήματος.

Έπειτα, σε αυτό το στάδιο προεπεξεργασίας, πραγματοποιείται τμηματοποίηση και βελτίωση των αιμοφόρων αγγείων που βοηθούν στην εξαγωγή του μοτίβου αιμοφόρων αγγείων του αμφιβληστροειδούς από την εικόνα του κερατοειδή. Στη συνέχεια, εντοπίζονται τα αιμοφόρα αγγεία του κερατοειδούς με τη διαδικασία της εξαγωγής χαρακτηριστικών. Τα αιμοφόρα αγγεία περιλαμβάνουν διακλαδώσεις (bifurcations), οι οποίες χρησιμοποιούνται για την ταυτοποίηση των χρηστών. Επειδή τα σημεία διακλαδώσεων διαφέρουν από άτομο σε άτομο, τα καθιστά ιδανικά για μια αξιόπιστη αναγνώριση ταυτότητας. Ο εντοπισμός τους γίνεται κατά την εξαγωγή χαρακτηριστικών με τη μέθοδο **skeletonization**.

Επιπλέον, υπάρχει και η μέθοδος ταυτοποίησης των χρηστών. Στο στάδιο αυτό, το πρότυπο το οποίο είναι αποθηκευμένο στη βάση δεδομένων για την ταυτοποίηση της δηλωμένης ταυτότητας κάθε χρήστη, συγκρίνεται με το πρότυπο που εξήχθη κατά το στάδιο της εξαγωγής χαρακτηριστικών. Λόγω των κινήσεων του ματιού, κατά το στάδιο απόκτησης της εικόνας, είναι απαραίτητο οι εικόνες να ευθυγραμμιστούν για να μπορέσει να γίνει η ταυτοποίηση. Οι κινήσεις του ματιού στη διαδικασία απόκτησης εικόνας προκαλούν μετατοπίσεις και στους δύο άξονες, με αποτέλεσμα ο αριθμός των σημείων διακλάδωσης στα δύο πρότυπα να μπορεί να διαφέρει. Επομένως, είναι απαραίτητο να μετασχηματιστεί το πρότυπο του χρήστη έτσι ώστε να προσεγγίσει το πρότυπο αναφοράς και να επιτευχθεί η αναγνώριση της ταυτότητας.

Τέλος, κάθε σύστημα αναγνώρισης του κερατοειδούς διαχειρίζεται μια βάση δεδομένων. Οι κύριες λειτουργίες είναι η αποθήκευση, η διαγραφή και η αναζήτηση των προτύπων του κερατοειδούς χιτώνα των χρηστών. Κάθε σύστημα αποθηκεύει ένα πρότυπο αναφοράς για κάθε χρήστη, μετά την εξαγωγή χαρακτηριστικών, ώστε να μπορεί να χρησιμοποιηθεί μελλοντικά για την ταυτοποίηση. Επιπλέον, κάθε σύστημα μπορεί και αναζήτα μέσα στη βάση δεδομένων για τα πρότυπα ώστε να επιτυγχάνεται η ταυτοποίηση της ταυτότητας του χρήστη. Και τέλος, κάθε σύστημα μπορεί να διαγράψει τα αποθηκευμένα πρότυπα.

Β.2.5 Συστήματα Αναγνώρισης προσώπου.

Β.2.5.1 Εισαγωγή.

Η τεχνολογία αναγνώρισης προσώπου στα πρώτα στάδια της χρήσης της περιοριζόταν στον εντοπισμό χαρακτηριστικών που σχετίζονταν με τα μάτια, τα αυτιά, τη μύτη, το στόμα, τη γραμμή του σαγονιού και τη δομή των ζυγωματικών. Ωστόσο, με την πρόοδο της τεχνολογίας, η αναγνώριση προσώπου έχει εξελιχθεί, ώστε να βασίζεται σε εξελιγμένα μαθηματικά μοντέλα και διαδικασίες σύγκρισης που χρησιμοποιούν τόσο τυχαία όσο και φωτομετρικά χαρακτηριστικά.

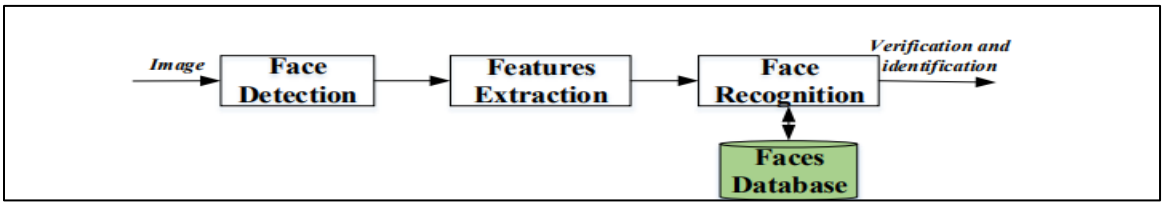
Η τεχνολογία λειτουργεί αναλύοντας τη δομή, το σχήμα και τις αναλογίες του προσώπου ενός ατόμου, συμπεριλαμβανομένων των αποστάσεων μεταξύ των ματιών, της μύτης, του στόματος και της γραμμής του σαγονιού. Εξετάζει επίσης, τα ανώτερα περιγράμματα των οφθαλμικών κοιλοτήτων, τις πλευρές του στόματος, τη θέση της μύτης και των ματιών, καθώς και την περιοχή γύρω από τα ζυγωματικά [1].

Το σύστημα αναγνώρισης προσώπου ως μέσο ταυτοποίησης έχει ήδη αρχίσει να προσφέρεται στους καταναλωτές πέρα από τη χρήση σε κινητά τηλέφωνα, όπως σε σημεία ελέγχου στα αεροδρόμια, σε στάδια, κατά τη διεξαγωγή αθλητικών εκδηλώσεων και συναυλιών, κ.α.

Επιπλέον, το σύστημα αυτό λειτουργεί χωρίς την ανάγκη ανθρώπινης παρέμβασης, καθιστώντας δυνατή την ταυτοποίηση ατόμων αποκλειστικά μέσω εικόνων που λαμβάνονται από κάμερες. Αυτή η δυνατότητα ενισχύει την αποτελεσματικότητα και την αυτοματοποίηση της διαδικασίας ταυτοποίησης.

Β.2.5.2 Βασικές Λειτουργίες ενός συστήματος αναγνώρισης προσώπου.

Τα συστήματα αναγνώρισης προσώπου εκτελούν τη λειτουργία του εντοπισμού προσώπου (Face Detection), της εξαγωγής των χαρακτηριστικών του προσώπου (Feature Extraction), τη διαδικασία ταυτοποίησης του χρήστη (face recognition) και της διαχείρισης μιας βάσης δεδομένων, όπως φαίνεται στην **εικόνα 7** [8].



Εικόνα 7 Βιομετρικό Σύστημα Αναγνώρισης Προσώπου.

Αρχικά, τα συστήματα αναγνώρισης προσώπων εντοπίζουν τα πρόσωπα των χρηστών και τα αποτυπώνουν σε μια συγκεκριμένη εικόνα. Παράγοντες όπως οι αλλαγές στον φωτισμό και η έκφραση του προσώπου μπορεί να εμποδίσουν την κατάλληλη ανίχνευση, όμως η δημιουργία σωστού προτύπου είναι ζωτικής σημασίας. Για αυτό αρχικά γίνεται η ανίχνευση του προσώπου, ώστε να επιβεβαιωθεί η παρουσία προσώπου στην εικόνα. Αυτό επιτυγχάνεται εντοπίζοντας την περιοχή της εικόνας που περιέχει το πρόσωπο. Μόλις εντοπιστεί το πρόσωπο, σχεδιάζεται ένα όριο ή πλαίσιο γύρω από αυτό, διαχωρίζοντας το πρόσωπο από το φόντο της εικόνας. Έπειτα, πραγματοποιείται αποκοπή εικόνας, ώστε μόνο η περιοχή του προσώπου να χρησιμοποιείται για τις λειτουργίες του συστήματος.

Σημαντικό είναι και το στάδιο εξαγωγής των χαρακτηριστικά των προσώπων. Η διαδικασία αυτή δημιουργεί ένα διάνυσμα χαρακτηριστικών που περιγράφει τα βασικά χαρακτηριστικά του προσώπου, όπως το στόμα, η μύτη και τα μάτια, μαζί με τη γεωμετρική τους διάταξη. Ο πιο συνηθισμένος μετασχηματισμός για αυτή τη διαδικασία είναι τα φίλτρα Gabor.

Η ταυτοποίηση των χρηστών γίνεται με βάση τα εξαγόμενα χαρακτηριστικά, τα οποία συγκρίνονται με τα χαρακτηριστικά των προσώπων που είναι αποθηκευμένα σε μια βάση δεδομένων. Μια απλοποιημένη εκδοχή της σύγκρισης προτύπων προσώπου (template matching) περιλαμβάνει τη σύγκριση μιας δοκιμαστικής εικόνας, η οποία αναπαρίσταται ως πίνακας τιμών έντασης, με ένα μόνο πρότυπο που αντιπροσωπεύει ολόκληρο το πρόσωπο. Η σύγκριση πραγματοποιείται με τη χρήση ενός κατάλληλου μέτρου, όπως η ευκλείδεια απόσταση.

Υπάρχουν και πιο εξελιγμένες εκδοχές της σύγκρισης προτύπων στην αναγνώριση προσώπου. Για παράδειγμα, μπορούν να χρησιμοποιηθούν περισσότερα από ένα πρότυπα προσώπου που αντιστοιχούν σε διαφορετικές γωνίες προβολής για την αναπαράσταση του προσώπου ενός

ατόμου. Αυτή η προσέγγιση αυξάνει την ακρίβεια, καθώς λαμβάνει υπόψη ποικίλες συνθήκες θέασης και στάσης του προσώπου [9].

Τέλος, κάθε σύστημα αποθηκεύει ένα πρότυπο για κάθε χρήστη μετά την εξαγωγή των χαρακτηριστικών ώστε το πρότυπο αυτό να μπορεί να χρησιμοποιηθεί μελλοντικά για την ταυτοποίηση. Επίσης, υπάρχει η λειτουργία αναζήτησης των προτύπων κατά την εξακρίβωση της ταυτότητας του χρήστη. Και τέλος, κάθε σύστημα μπορεί να διαγράψει τα αποθηκευμένα πρότυπα όποτε αυτό χρειάζεται.

Β.2.6 Συστήματα Αναγνώρισης παλάμης.

Β.2.6.1 Εισαγωγή.

Το ανθρώπινο χέρι αποτελεί πολύτιμη πηγή μοναδικών πληροφοριών με διακριτικά χαρακτηριστικά όπως το σχήμα, το μήκος, το πλάτος, το πάχος και το μοτίβο των γραμμών της παλάμης, τα οποία μπορούν να χρησιμοποιηθούν για σκοπούς ταυτοποίησης μέσω της αναγνώρισης γεωμετρίας χεριού.

Αυτά τα χαρακτηριστικά είναι μοναδικά για κάθε άτομο και δεν μπορούν να αναγνωριστούν εύκολα με γυμνό μάτι. Ωστόσο, ηλεκτρονικές συσκευές όπως κάμερες μπορούν να τα καταγράψουν και να τα αναγνωρίσουν.

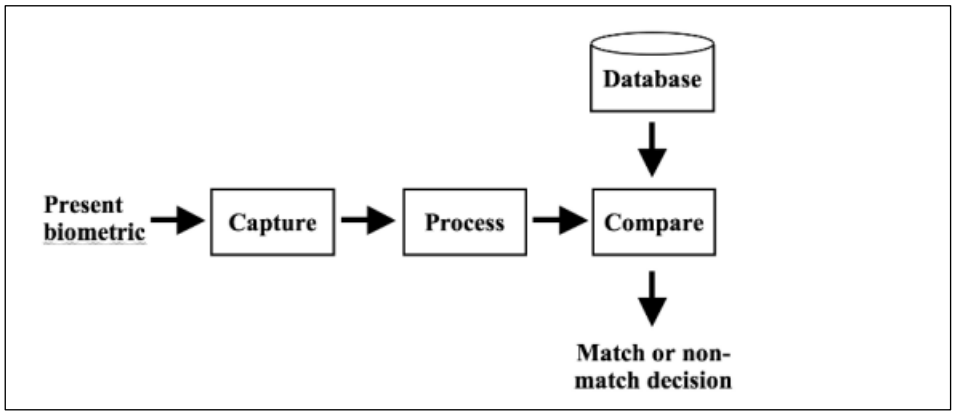
Η διαδικασία αναγνώρισης γεωμετρίας χεριού περιλαμβάνει τη σάρωση του μεγέθους και του σχήματος του χεριού, καθώς και την καταγραφή του μήκους, του πλάτους, του πάχους και της επιφάνειας της παλάμης μέσω κάμερας. Αυτές οι πληροφορίες μπορούν να αξιοποιηθούν για την ταυτοποίηση ατόμου, εξασφαλίζοντας παράλληλα την ασφαλή ανταλλαγή ευαίσθητων δεδομένων.

Η λήψη του βιομετρικού δείγματος πραγματοποιείται συχνά με τη χρήση μιας τυπικής οπτικής κάμερας ή ενός σαρωτή επίπεδης επιφάνειας. Κάποιες συσκευές βασίζονται αποκλειστικά στο φυσικό φως, ενώ οι περισσότερες διαθέτουν δικό τους φωτισμό, συνήθως στο υπέρυθρο φάσμα [11][12].

Β.2.6.2 Βασικές λειτουργίες συστημάτων αναγνώρισης παλάμης.

Τα βιομετρικά συστήματα αυθεντικοποιήσης που χρησιμοποιούν την παλάμη του χεριού του χρήστη ως βιομετρικό χαρακτηριστικό για ταυτοποίηση, εκτελούν και αυτά τις βασικές λειτουργίες των βιομετρικών συστημάτων. Δηλαδή, τη λειτουργία της προεπεξεργασίας εικόνας

(preprocessing), της εξαγωγής των χαρακτηριστικών (feature extraction), της ταυτοποίησης των χρηστών (Matching) και της διαχείρισης μιας βάσης δεδομένων, όπως φαίνεται στην **εικόνα 8**



Εικόνα 8 Βιομετρικό Σύστημα Αναγνώρισης Παλάμης.

Αρχικά, τα συστήματα αναγνώρισης της γεωμετρίας της παλάμης περιλαμβάνουν μια συσκευή εισόδου η οποία δημιουργεί την αρχική εικόνα της παλάμης του χρήστη σε μορφή grayscale. Κατά το στάδιο της προεπεξεργασίας η εικόνα αυτή θα μετασχηματιστεί ώστε να μπορεί να χρησιμοποιηθεί από το σύστημα.

Το στάδιο της προεπεξεργασίας είναι πολύ σημαντικό για κάθε βιομετρικό σύστημα αναγνώρισης γεωμετρίας παλάμης. Δεδομένου ότι η αναγνώριση βασίζεται στην ανάλυση των περιγραμμάτων του χεριού, τα συστήματα αυτά μετατρέπουν την καταγεγραμμένη εικόνα σε κλίμακα του γκρι (grayscale) σε μια εικόνα δίχρωμη (black-and-white silhouette). Χάρη σε αυτή τη διαδικασία, τα συστήματα γεωμετρίας χεριού είναι ανθεκτικά σε αλλαγές επιφανειακών χαρακτηριστικών, όπως τατουάζ, τρίχες, κοψίματα, γρατζουνιές, εγκαύματα, βρωμιά τα οποία ενδέχεται να επηρεάζουν άλλες βιομετρικές μεθόδους [11].

Επίσης, οι αποκλίσεις του χεριού μέσα στην εικόνα που οφείλονται κυρίως σε μικρές μεταβολές στη θέση της κάμερας, διορθώνονται μέσω αλλαγής μεγέθους και περιστροφής της εικόνας. Αυτό επιτυγχάνεται εντοπίζοντας δύο από τις κορυφές στις πλατφόρμες (τη μία που πιέζει το μικρό δάχτυλο και την κορυφή που βρίσκεται μεταξύ του δείκτη και του μεσαίου δαχτύλου)[12]. Με την ολοκλήρωση της προεπεξεργασίας μπορεί το σύστημα να ξεκινήσει την εξαγωγή των χαρακτηριστικών.

Κατά την εξαγωγή των χαρακτηριστικών το σύστημα δημιουργεί ένα διάνυσμα που προκύπτει από τις μετρήσεις των μηκών των δακτύλων, τις γωνίες, το πλάτος και το πάχος της παλάμης. Υπάρχουν επίσης συστήματα που λειτουργούν απευθείας στο περίγραμμα του χεριού, χρησιμοποιώντας τα σημεία στο περίγραμμα ως σημεία αναφοράς.

Το διάνυσμα που προκύπτει από την εξαγωγή χαρακτηριστικών πρέπει να εισέλθει σε μια διαδικασία σύγκρισης για να επαληθευτεί αν το άτομο του οποίου λήφθηκε η εικόνα του χεριού είναι ο χρήστης που ισχυρίζεται ότι είναι. Αυτή η σύγκριση πραγματοποιείται έναντι ενός μοντέλου χρήστη το οποίο υπολογίζεται ανάλογα με τον αλγόριθμο σύγκρισης που χρησιμοποιείται. Η πιο συνηθισμένες μέθοδοι ταυτοποίησης είναι η ευκλείδεια απόσταση, η απόσταση Hamming και το Μοντέλο Μείγματος Κανονικών Κατανομών (Gaussian Mixture Model).

Τέλος, τα συστήματα αυτά μπορούν να αποθηκεύουν και να διαγράφουν τα βιομετρικά πρότυπα (είτε εικόνες είτε διανύσματα) σε μια βάση δεδομένων. Οι εγγραφές στη βάση δεδομένων είναι απαραίτητο να είναι έγκυρες και ενημερωμένες προκειμένου να επιτυγχάνεται η ταυτοποίηση των χρηστών με μεγαλύτερη ακρίβεια.

Κεφάλαιο Γ: Μελέτη Ασφάλειας Βιομετρικών Συστημάτων Αυθεντικοποιήσης.

Γ.1 Εισαγωγή.

Τα βιομετρικά συστήματα είναι μία από τις πιο διαδεδομένες μεθόδους ταυτοποίησης, λόγω της υψηλής αποτελεσματικότητάς τους. Ωστόσο, παρά την αξιοπιστία που παρέχουν, παρουσιάζουν ευπάθειες που μπορούν να εκμεταλλευτούν κακόβουλοι χρήστες, οδηγώντας σε σοβαρές επιθέσεις.

Οι κύριες ευπάθειες των βιομετρικών συστημάτων, προέρχονται από τεχνικά αλλά και από τα υλικά χαρακτηριστικά των συστημάτων αυτών. Η ακρίβεια των αισθητήρων, οι αλγόριθμοι ταυτοποίησης και η διαδικασία αποθήκευσης και μετάδοσης των δεδομένων επηρεάζουν άμεσα την ασφάλεια και την αξιοπιστία τους. Τυχόν αδυναμίες σε αυτούς τους τομείς μπορεί να οδηγήσουν σε σφάλματα ταυτοποίησης ή σε κίνδυνο παραβίασης των πληροφοριών.

Γνωστό είναι επίσης ότι οι επιθέσεις στα βιομετρικά συστήματα είναι πολλές και εξαιρετικά επικίνδυνες. Οι κακόβουλοι χρήστες χρησιμοποιούν τεχνικές για να παρακάμψουν τους μηχανισμούς ασφαλείας, να υποκλέψουν ευαίσθητες πληροφορίες και να παράξουν πλαστά βιομετρικά δεδομένα με στόχο να αποκτήσουν πρόσβαση σε υπηρεσίες και αγαθά, χωρίς εξουσιοδότηση. Οι επιθέσεις αυτές, αν επιτύχουν, θέτουν σε κίνδυνο την ακεραιότητα των δεδομένων και των αγαθών με αποτέλεσμα να δημιουργούνται πολλά προβλήματα τόσο στους χρήστες όσο και στους οργανισμούς που χρησιμοποιούν τα συστήματα αυτά.

Χαρακτηριστικό παράδειγμα αποτελεί ο Trojan GoldPickaxe, ένα εξελιγμένο κακόβουλο λογισμικό που στοχεύει συσκευές Android και iOS με σκοπό την υποκλοπή βιομετρικών δεδομένων προσώπου και στοιχείων ταυτότητας. Τα δεδομένα αυτά χρησιμοποιούνται για τη δημιουργία deepfake βίντεο που επιτρέπουν την παραβίαση τραπεζικών λογαριασμών και άλλων υπηρεσιών που βασίζονται σε βιομετρικούς ελέγχους. Ένα ακόμη περιστατικό μεγάλης κλίμακας ήταν η παραβίαση του συστήματος Biostar 2 της Suprema, το οποίο χρησιμοποιούνταν από την αστυνομία του Λονδίνου, τράπεζες και εταιρείες άμυνας. Σε αυτή την περίπτωση, διέρρευσαν περισσότερα από ένα εκατομμύριο δακτυλικά αποτυπώματα, δεδομένα αναγνώρισης προσώπου, ονόματα χρηστών και κωδικοί πρόσβασης σε απλό κείμενο, όλα αποθηκευμένα χωρίς κρυπτογράφηση σε μια δημόσια προσβάσιμη βάση δεδομένων. Η ευπάθεια αυτή επέτρεψε σε ερευνητές να αποκτήσουν πλήρη πρόσβαση στις εγγραφές, να δουν στοιχεία εισόδου και εξόδου χρηστών σε χώρους υψηλής ασφάλειας και ακόμη και να δημιουργήσουν νέους λογαριασμούς με δικά τους βιομετρικά χαρακτηριστικά.[24][25].

Συνοψίζοντας, τα βιομετρικά συστήματα προσφέρουν σημαντικά πλεονεκτήματα στην ταυτοποίηση και την ασφάλεια, αλλά η ύπαρξη ευπαθειών καθιστά αναγκαία τη συνεχή βελτίωσή τους για να επιτευχθεί η καλύτερη δυνατή προστασία των χρηστών και των αγαθών. Η μελέτη των ασφάλειας είναι ζωτικής σημασίας για την αποτροπή απειλών και την εξασφάλιση της εμπιστευτικότητας ,της ακεραιότητας και της διαθεσιμότητας των βιομετρικών δεδομένων αυθεντικοποιήσης.

Γ.2 Συνήθεις ευπάθειες των βιομετρικών συστημάτων αυθεντικοποιήσης.

Αν και τα βιομετρικά συστήματα προσφέρουν αυξημένη ασφάλεια σε σχέση με άλλες μεθόδους ταυτοποίησης, έχουν και πολλές ευπάθειες, τις οποίες μπορούν να εκμεταλλευτούν οι κακόβουλοι χρήστες. Αυτές οι αδυναμίες μπορούν να προκύψουν από διάφορους παράγοντες, όπως η ποιότητα των τεχνολογιών ανίχνευσης, οι περιορισμοί στους αλγορίθμους επεξεργασίας δεδομένων ή ακόμα και οι τρόποι αποθήκευσης και μετάδοσης των βιομετρικών πληροφοριών. Παρακάτω, αναλύονται οι κυριότερες ευπάθειες των βιομετρικών συστημάτων, οι οποίες σχετίζονται τόσο με την ποιότητα και την ακρίβεια των αισθητήρων, όσο και με τον τρόπο αποθήκευσης και διαχείρισης των δεδομένων. Επιπλέον, σημαντικά ζητήματα προκύπτουν από τα σφάλματα ταυτοποίησης που μπορεί να οδηγήσουν σε ψευδείς αποδοχές ή απορρίψεις χρηστών, καθώς και από τις αδυναμίες των αλγορίθμων αναγνώρισης που ενδέχεται να επιτρέψουν σε κακόβουλους χρήστες να παρακάμψουν το σύστημα. Στην ίδια κατεύθυνση, η ανεπαρκής ασφάλεια κατά τη μετάδοση των βιομετρικών πληροφοριών αυξάνει τον κίνδυνο υποκλοπής και μη εξουσιοδοτημένης χρήσης, ενώ εξαιρετικά ανησυχητική θεωρείται και η πιθανότητα ανακατασκευής βιομετρικών δεδομένων από αποθηκευμένα πρότυπα, γεγονός που καθιστά αναγκαία την εφαρμογή προηγμένων τεχνικών προστασίας.

1. Ποιότητα και Ακρίβεια Αισθητήρων.

   Η ποιότητα των αισθητήρων αποτελεί καθοριστικό παράγοντα για την αξιοπιστία ενός βιομετρικού συστήματος. Όταν οι αισθητήρες είναι χαμηλής ανάλυσης ή έχουν φθαρεί από περιβαλλοντικούς παράγοντες, όπως σκόνη και υγρασία, τότε τα δεδομένα που συλλέγονται μπορεί να είναι ελλιπή ή αλλοιωμένα. Αυτό έχει ως αποτέλεσμα τη δημιουργία λαθών κατά τη διαδικασία αναγνώρισης, καθώς ο αισθητήρας αδυνατεί να καταγράψει με ακρίβεια τα χαρακτηριστικά του χρήστη.

   Η απειλή αυτή προκύπτει κυρίως από αστοχία υλικού ή εξωτερικούς περιβαλλοντικούς παράγοντες. Ο τρόπος με τον οποίο πραγματοποιείται αφορά την αδυναμία του συστήματος να συγκρίνει επαρκώς την είσοδο με το αποθηκευμένο πρότυπο, οδηγώντας σε σφάλματα ταυτοποίησης.

Ο αντίκτυπος είναι διττός. Σε επίπεδο συστήματος, παρατηρείται αύξηση του Failure to Capture Rate και του Failure to Enroll Rate, κάτι που μειώνει τη διαθεσιμότητα και την ακεραιότητα του συστήματος. Σε επίπεδο χρήστη, μπορεί να προκληθεί αποτυχία πρόσβασης σε κρίσιμες υπηρεσίες, με χαρακτηριστικό παράδειγμα την αδυναμία ξεκλειδώματος κινητού τηλεφώνου όταν ο χρήστης έχει μικρές πληγές στο δάχτυλο. Η απαίτηση ασφάλειας που διακυβεύεται είναι κυρίως η διαθεσιμότητα, καθώς και η αξιοπιστία της διαδικασίας αυθεντικοποίησης.

Για την αντιμετώπιση του προβλήματος απαιτείται τακτική συντήρηση και καθαρισμός των αισθητήρων, αξιοποίηση συσκευών υψηλής ανάλυσης και ενσωμάτωση μηχανισμών ελέγχου ποιότητας των εισαγόμενων δεδομένων.

2. Αποθήκευση και Διαχείριση Βιομετρικών Δεδομένων.

Η αποθήκευση των βιομετρικών προτύπων είναι από τα πιο ευαίσθητα σημεία σε ένα βιομετρικό σύστημα. Εάν αυτά τα δεδομένα αποθηκεύονται σε μη ασφαλή μορφή, υπάρχει αυξημένος κίνδυνος υποκλοπής και πλαστογράφησης. Το σημείο εκκίνησης της απειλής μπορεί να είναι τόσο κακόβουλη ενέργεια, όπως μία κυβερνοεπίθεση, όσο και ανθρώπινο λάθος στη διαχείριση ή τη συντήρηση των βάσεων δεδομένων.

Η απειλή πραγματοποιείται με τη μορφή υποκλοπής ή αντιγραφής μη κρυπτογραφημένων δεδομένων, τα οποία στη συνέχεια μπορούν να χρησιμοποιηθούν από τρίτους. Ο αντίκτυπος για το σύστημα είναι σημαντικός, καθώς μια τέτοια παραβίαση μειώνει την ακεραιότητα και την εμπιστευτικότητα, ενώ επηρεάζει τον δείκτη Template Capacity, δηλαδή τη διαχείριση του όγκου των αποθηκευμένων δεδομένων. Για τον άνθρωπο, η συνέπεια μπορεί να είναι η κλοπή ταυτότητας ή η μη εξουσιοδοτημένη χρήση βιομετρικών του δεδομένων.

Ένα χαρακτηριστικό παράδειγμα είναι η διαρροή αποτυπωμάτων από σύστημα ελέγχου πρόσβασης μετά από κυβερνοεπίθεση. Σε αυτήν την περίπτωση, η απαίτηση ασφάλειας που διακυβεύεται είναι η εμπιστευτικότητα, αλλά και η ακεραιότητα της πληροφορίας.

Ως αντίμετρα προτείνονται η κρυπτογράφηση δεδομένων, η χρήση ακυρώσιμων βιομετρικών ώστε να μπορούν να αντικατασταθούν σε περίπτωση διαρροής, καθώς και η αυστηρή διαχείριση πρόσβασης στις βάσεις δεδομένων.

3. Ψευδείς Αποδοχές και Απορρίψεις κατά την Ταυτοποίηση (False Positives & False Negatives).

Τα βιομετρικά συστήματα είναι πιθανό να εμφανίσουν σφάλματα με τη μορφή ψευδών αποδοχών (false positives) ή ψευδών απορρίψεων (false negatives). Η απειλή αυτή έχει ως σημείο εκκίνησης κυρίως αστοχίες αλγορίθμων ή περιβαλλοντικούς παράγοντες, όπως

χαμηλός φωτισμός, θόρυβος ή αλλαγές στα βιομετρικά χαρακτηριστικά ενός ατόμου λόγω τραυματισμού ή γήρανσης.

Ο τρόπος με τον οποίο πραγματοποιείται η απειλή σχετίζεται με την αδυναμία του αλγορίθμου να συγκρίνει ορθά τα εισαγόμενα δεδομένα με τα αποθηκευμένα πρότυπα. Ο αντίκτυπος σε επίπεδο συστήματος αποτυπώνεται στους δείκτες False Accept Rate, False Reject Rate, Relative Operating Characteristic και Equal Error Rate. Η αύξηση των τιμών αυτών συνεπάγεται μείωση της ακρίβειας και της αξιοπιστίας, γεγονός που διακυβεύει τη διαθεσιμότητα και την ακεραιότητα. Σε επίπεδο χρήστη, μπορεί να οδηγήσει είτε σε μη εξουσιοδοτημένη πρόσβαση, είτε σε αποκλεισμό νόμιμου χρήστη.

Ένα χαρακτηριστικό παράδειγμα είναι η περίπτωση όπου ένα σύστημα αναγνώρισης προσώπου απορρίπτει επανειλημμένα έναν υπάλληλο επειδή φοράει γυαλιά. Η απαίτηση ασφάλειας που πλήττεται είναι η διαθεσιμότητα και η αξιοπιστία της διαδικασίας ελέγχου ταυτότητας.

Ως αντίμετρα συνιστάται η συνεχής βελτίωση και εκπαίδευση των αλγορίθμων με ποικιλία δεδομένων, η τακτική ενημέρωση λογισμικού και η χρήση πολυπαραγοντικής αυθεντικοποίησης.

4. Ευπάθειες στους Αλγορίθμους Αναγνώρισης.

Οι αλγόριθμοι που χρησιμοποιούνται για τη σύγκριση και ταυτοποίηση μπορεί να αποτελέσουν σημείο ευπάθειας. Εάν δεν είναι επαρκώς προστατευμένοι, μπορούν να παρακαμφθούν με τη χρήση ψευδών ή αλλοιωμένων δεδομένων. Η απειλή αυτή ξεκινά είτε από αστοχία λογισμικού είτε από κακόβουλη ενέργεια, όπως η δημιουργία πλαστών προτύπων που μιμούνται τα πραγματικά.

Η πραγματοποίηση γίνεται με τη δημιουργία βιομετρικών στοιχείων που ξεγελούν τον αλγόριθμο. Ο αντίκτυπος είναι άμεσος στην ασφάλεια του συστήματος, καθώς αυξάνεται ο δείκτης False Accept Rate, μειώνεται η αξιοπιστία και διακυβεύονται η εμπιστευτικότητα και η ακεραιότητα. Σε επίπεδο χρήστη, η συνέπεια μπορεί να είναι η απώλεια ιδιωτικότητας και η παραβίαση προσωπικών δεδομένων.

Παράδειγμα αποτελεί η χρήση τρισδιάστατης μάσκας που εξαπατά ένα σύστημα αναγνώρισης προσώπου, επιτρέποντας την είσοδο σε μη εξουσιοδοτημένο άτομο. Η απαίτηση ασφάλειας που διακυβεύεται είναι η εμπιστευτικότητα, καθώς και η ακεραιότητα της διαδικασίας αυθεντικοποίησης.

Για την αντιμετώπιση του κινδύνου αυτού απαιτούνται προηγμένοι αλγόριθμοι ανίχνευσης επιθέσεων spoofing και συνδυαστικές μέθοδοι ταυτοποίησης, ώστε να καθιστούν πιο δύσκολη την εξαπάτηση του συστήματος.

5. Αδυναμίες στη Μετάδοση Δεδομένων.

Η διαδικασία μετάδοσης βιομετρικών δεδομένων προς τον κεντρικό server μπορεί να αποτελέσει σημείο ευπάθειας. Όταν τα δεδομένα δεν μεταδίδονται μέσω ασφαλών πρωτοκόλλων, υπάρχει αυξημένος κίνδυνος υποκλοπής. Το σημείο εκκίνησης της απειλής μπορεί να είναι είτε μια κακόβουλη ενέργεια, όπως επίθεση τύπου man-in-the-middle, είτε αστοχία στην υλοποίηση των πρωτοκόλλων επικοινωνίας.

Η απειλή πραγματοποιείται μέσω υποκλοπής ή αλλοίωσης των δεδομένων κατά την επικοινωνία. Ο αντίκτυπος αφορά την ακεραιότητα και την εμπιστευτικότητα, καθώς τα δεδομένα μπορεί να παραποιηθούν ή να χρησιμοποιηθούν από τρίτους. Σε επίπεδο δεικτών, μπορεί να επηρεαστεί ο Failure to Enroll Rate, λόγω αλλοίωσης δεδομένων κατά τη μεταφορά. Για τον άνθρωπο, ο αντίκτυπος μπορεί να είναι κλοπή ταυτότητας και πιθανές οικονομικές απώλειες.

Παράδειγμα αποτελεί η υποκλοπή δεδομένων κατά την αποστολή από τερματικό εισόδου σε κεντρικό server. Η απαίτηση ασφάλειας που πλήττεται είναι κυρίως η εμπιστευτικότητα.

Για την αποφυγή τέτοιων περιστατικών απαιτείται η χρήση πρωτοκόλλων κρυπτογράφησης όπως TLS/SSL, η δημιουργία ασφαλών καναλιών επικοινωνίας και ο έλεγχος ταυτότητας των κόμβων.

6. Ανακατασκευή Βιομετρικών Δεδομένων από Αποθηκευμένα Πρότυπα.

Η πρόσβαση εισβολέων σε αποθηκευμένα πρότυπα δημιουργεί τον κίνδυνο ανακατασκευής βιομετρικών δεδομένων. Η απειλή αυτή προέρχεται από κακόβουλες ενέργειες, όπως η παραβίαση μιας βάσης δεδομένων.

Η πραγματοποίηση γίνεται με την αντιστροφή των αποθηκευμένων προτύπων, ώστε να δημιουργηθούν ψευδή βιομετρικά χαρακτηριστικά που μπορούν να χρησιμοποιηθούν για να εξαπατήσουν το σύστημα. Ο αντίκτυπος σε επίπεδο συστήματος είναι σοβαρός, καθώς αυξάνεται το False Accept Rate και επηρεάζεται η τιμή του Equal Error Rate, γεγονός που μειώνει την αξιοπιστία. Σε επίπεδο χρήστη, οι συνέπειες είναι ακόμη πιο σημαντικές, καθώς η απώλεια ιδιωτικότητας είναι μη αναστρέψιμη: ένα αποτύπωμα ή η ίριδα δεν μπορούν να αλλάξουν όπως ένας κωδικός. Η απαίτηση ασφάλειας που διακυβεύεται είναι η εμπιστευτικότητα και η ακεραιότητα.

Παράδειγμα αποτελεί η εισβολή σε σύστημα και η ανακατασκευή δακτυλικού αποτυπώματος που στη συνέχεια χρησιμοποιείται για πρόσβαση σε άλλη συσκευή.

Η αντιμετώπιση απαιτεί την εφαρμογή ακυρώσιμων βιομετρικών, την αποθήκευση των δεδομένων σε μη αντιστρέψιμη μορφή και την πολυεπίπεδη κρυπτογράφηση.

Γ.3 Επιθέσεις Βιομετρικών συστημάτων Αυθεντικοποιήσης.

Τις παραπάνω συνήθεις ευπάθειες τις εκμεταλλεύονται κακόβουλοι χρήστες που επιθυμούν να παρακάμψουν την αυθεντικοποιήσή τους μέσω των βιομετρικών συστημάτων και να αποκτήσουν πρόσβαση σε δεδομένα που δεν τους ανήκουν. Παρακάτω θα αναλύσουμε τις πιο συνηθισμένες επιθέσεις σε βιομετρικά συστήματα αυθεντικοποιήσης.

1. Επιθέσεις Spoofing.

Το spoofing είναι μια επίθεση κατά την οποία ένας κακόβουλος χρήστης προσποιείται ότι είναι κάποιος άλλος. Στην περίπτωση των βιομετρικών συστημάτων, η επίθεση spoofing παρακάμπτει τους μηχανισμούς ασφάλειας παρέχοντας ένα πλαστό βιομετρικό αντίγραφο ενός εξουσιοδοτημένου χρήστη. Για την εκτέλεση της απειλής, απαιτείται η απόκτηση ενός βιομετρικού δείγματος από έναν νόμιμο χρήστη, το οποίο μπορεί να χρησιμοποιηθεί για την κατασκευή τεχνητών αναδημιουργημένων χαρακτηριστικών, όπως ενός ψεύτικου δακτύλου, μιας εικόνας υψηλής ανάλυσης της ίριδας ή μιας μάσκας προσώπου. Εκτός από τα φυσικά χαρακτηριστικά, η μίμηση χρησιμοποιείται συχνά και για την εξαπάτηση τεχνολογιών συμπεριφορικών βιομετρικών στοιχείων, όπως η ομιλία ή η υπογραφή.

Η πραγματοποίηση μιας τέτοιας επίθεσης έχει σημαντικό αντίκτυπο στην ασφάλεια, καθώς υπονομεύει την εμπιστευτικότητα και την ακεραιότητα του συστήματος, ενώ μειώνει και τη διαθεσιμότητά του σε έμμεσο επίπεδο, εφόσον παρακάμπτονται οι μηχανισμοί ελέγχου ταυτότητας. Ο κίνδυνος αποτυπώνεται στους δείκτες False Accept Rate (FAR), αφού αυξάνει η πιθανότητα αποδοχής μη εξουσιοδοτημένων χρηστών, και Equal Error Rate (EER), καθώς επιδεινώνεται η συνολική απόδοση του συστήματος. Χαρακτηριστικό παράδειγμα είναι η δημιουργία ενός εκμαγείου δακτυλικού αποτυπώματος από ένα αποτύπωμα που έχει συλλεχθεί σε μια γυάλινη επιφάνεια, το οποίο μπορεί να χρησιμοποιηθεί για να ξεκλειδώσει μια κινητή συσκευή.

Ως αντίμετρα μπορούν να εφαρμοστούν τεχνικές ανίχνευσης ζωντανότητας (liveness detection), κρυπτογράφηση βιομετρικών δεδομένων, καθώς και πολυπαραγοντικός έλεγχος ταυτότητας ώστε να μειωθεί η πιθανότητα επιτυχούς spoofing. Το σημείο εκκίνησης αυτής της απειλής εντοπίζεται κυρίως στην κακόβουλη ενέργεια τρίτων, με συνδρομή ανθρώπινου λάθους ή ελλιπών διαδικασιών προστασίας βιομετρικών δειγμάτων.

2. Επιθέσεις Επανάληψης (replay attacks)

Η επίθεση επανάληψης συνιστά απειλή κατά την οποία ένας κακόβουλος χρήστης επαναχρησιμοποιεί δεδομένα βιομετρικής ταυτοποίησης που έχουν προηγουμένως καταγραφεί από έναν νόμιμο χρήστη. Αυτό μπορεί να γίνει μέσω συσκευών ή λογισμικού καταγραφής κατά τη

διάρκεια μιας επιτυχούς αυθεντικοποίησης ή με τη συλλογή ενός υπολειμματικού αποτυπώματος που έχει μείνει στον αισθητήρα. Στο πρώτο σενάριο, ο επιτιθέμενος εισάγει ένα καταγεγραμμένο σήμα δεύτερη φορά στο σύστημα, παρακάμπτοντας τον αισθητήρα, ενώ στο δεύτερο σενάριο υποβάλλει εκ νέου μια εικόνα όπως ακριβώς την εισήγαγε και ο νόμιμος χρήστης.

Ο αντίκτυπος μιας επίθεσης επανάληψης είναι σοβαρός, καθώς απειλείται η εμπιστευτικότητα και η ακεραιότητα του συστήματος, ενώ η αξιοπιστία των μηχανισμών ταυτοποίησης υπονομεύεται. Η ευπάθεια αποτυπώνεται στον δείκτη False Accept Rate (FAR), αφού το σύστημα μπορεί να αποδεχτεί ως νόμιμο ένα καταγεγραμμένο και επαναχρησιμοποιημένο δείγμα, ενώ επηρεάζεται και το Failure to Capture Rate (FTC), λόγω αδυναμίας διάκρισης γνήσιας εισόδου από εισαγόμενη. Παράδειγμα αποτελεί η χρήση καταγεγραμμένου ηχητικού αποσπάσματος φωνής σε ένα σύστημα αναγνώρισης φωνής για την παραπλάνηση του μηχανισμού αυθεντικοποίησης.

Ως αντίμετρα μπορούν να εφαρμοστούν τεχνικές χρονοσήμανσης, έλεγχοι ταυτότητας πολλαπλών παραμέτρων και η χρήση ασφαλών καναλιών μετάδοσης για την αποφυγή επαναχρησιμοποίησης δεδομένων. Η απειλή ξεκινά κυρίως από κακόβουλη ενέργεια επιτιθέμενου, σε συνδυασμό με τρωτότητες στη σχεδίαση ή στην ασφάλεια της υλοποίησης.

3. Προσομοίωση Δεδομένων.

Η προσομοίωση δεδομένων αξιοποιεί το γεγονός ότι τα βιομετρικά χαρακτηριστικά δεν είναι μυστικά και μπορούν να είναι διαθέσιμα στο διαδίκτυο. Ένας κακόβουλος χρήστης μπορεί να μιμηθεί τη φυσική υπογραφή ή την ομιλία ενός νόμιμου χρήστη, ή ακόμα να επιχειρήσει την αναπαραγωγή μοτίβων δακτυλικού αποτυπώματος ή εικόνας προσώπου. Το ανησυχητικό είναι ότι συχνά δεν απαιτείται υψηλή ακρίβεια στην προσομοίωση, καθώς ακόμη και πλαστά βιομετρικά χαρακτηριστικά χαμηλής ποιότητας μπορεί να παραπλανήσουν το σύστημα.

Η απειλή αυτή έχει σημαντικό αντίκτυπο, διότι υπονομεύει την ακεραιότητα και την εμπιστευτικότητα των βιομετρικών συστημάτων, επηρεάζοντας δείκτες όπως ο FAR και ο EER, αφού αυξάνεται η πιθανότητα να αποδεχθεί το σύστημα ψεύτικες εισόδους. Παράδειγμα αποτελεί η αναπαραγωγή μιας ηχογραφημένης φράσης για να παρακαμφθεί ένα σύστημα φωνητικής αναγνώρισης.

Ως αντίμετρα μπορούν να χρησιμοποιηθούν τεχνικές ανάλυσης συμπεριφοράς, έλεγχοι ζωντανότητας, καθώς και αλγόριθμοι εντοπισμού παραποιημένων δεδομένων. Η απειλή ξεκινά από κακόβουλη ενέργεια, αλλά μπορεί να διευκολυνθεί και από ανθρώπινο λάθος, όπως η απερίσκεπτη διάθεση βιομετρικών δεδομένων σε δημόσια δίκτυα.

4. Επίθεση κατά τη Μετάδοση.

Οι επιθέσεις κατά τη μετάδοση (man-in-the-middle) πραγματοποιούνται όταν ένας κακόβουλος χρήστης παρεμβάλλεται στη ροή των δεδομένων κατά τη μεταφορά τους από τον αισθητήρα προς

το σύστημα. Ο επιτιθέμενος μπορεί να παραποιήσει τα δεδομένα, να εισαγάγει ψεύτικα πρότυπα ή να αντικαταστήσει ένα έγκυρο δείγμα με πλαστό.

Ο αντίκτυπος μιας τέτοιας επίθεσης είναι η απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας του συστήματος, ενώ επηρεάζονται δείκτες όπως ο FAR, καθώς αυξάνεται η πιθανότητα αποδοχής ψευδών δεδομένων, και το Relative Operating Characteristic (ROC), καθώς η αξιοπιστία του συστήματος μειώνεται σημαντικά. Παράδειγμα αποτελεί η παρεμβολή σε ένα μη ασφαλές δίκτυο κατά τη μετάδοση δεδομένων αναγνώρισης προσώπου.

Ως αντίμετρα μπορούν να εφαρμοστούν κρυπτογράφηση των βιομετρικών δεδομένων, ασφαλή κανάλια μετάδοσης και μηχανισμοί ακεραιότητας. Η απειλή ξεκινά από κακόβουλη ενέργεια και εκμεταλλεύεται αδυναμίες στην αρχιτεκτονική του συστήματος.

5. Επίθεση σε Πρότυπα (Templates attacks)

Τα βιομετρικά πρότυπα μπορεί να αποθηκεύονται σε αυτόνομες συσκευές, τοπικούς υπολογιστές ή κεντρικές βάσεις δεδομένων, με αποτέλεσμα να αποτελούν στόχο επιθέσεων. Οι επιθέσεις αυτές περιλαμβάνουν την προσθήκη νέου προτύπου, την τροποποίηση ή διαγραφή ενός αποθηκευμένου προτύπου και κυρίως την κλοπή του. Ειδικά η κλοπή θεωρείται η πιο επικίνδυνη μορφή, καθώς μπορεί να οδηγήσει στη δημιουργία συνθετικών εικόνων που ξεγελούν τα συστήματα αναγνώρισης.

Ο αντίκτυπος αυτών των επιθέσεων είναι ιδιαίτερα σοβαρός, καθώς πλήττεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα του συστήματος, ενώ οι δείκτες Failure to Enroll Rate (FTE), Template Capacity και FAR επηρεάζονται άμεσα. Αν ο εισβολέας αποκτήσει πρόσβαση στη βάση δεδομένων προτύπων, μπορεί να διεξάγει επιθέσεις spoofing, denial of service ή man-in-the-middle. Παράδειγμα αποτελεί η κλοπή προτύπων δακτυλικών αποτυπωμάτων από μια κεντρική βάση δεδομένων και η χρήση τους για την κατασκευή ψεύτικων δειγμάτων.

Ως αντίμετρα απαιτείται κρυπτογράφηση των προτύπων, περιορισμός πρόσβασης μόνο σε εξουσιοδοτημένους διαχειριστές, καθώς και τακτικός έλεγχος και ανανέωση πολιτικών ασφαλείας. Η απειλή ξεκινά από κακόβουλη ενέργεια, αλλά μπορεί να ενισχυθεί από εσφαλμένες ρυθμίσεις ή ανθρώπινο λάθος.

6. Επίθεση στη βάση δεδομένων.

Οι βάσεις δεδομένων που αποθηκεύουν βιομετρικά δεδομένα αποτελούν βασικό στόχο επιθέσεων. Ένας τρόπος επίθεσης είναι το SQL Injection, όπου κακόβουλος SQL κώδικας εισάγεται μέσω του frontend και εκτελείται στο backend, παρέχοντας απεριόριστη πρόσβαση στους επιτιθέμενους. Παράλληλα, λανθασμένες ρυθμίσεις ή προεπιλεγμένοι λογαριασμοί μπορεί να αφήσουν τις βάσεις εκτεθειμένες, ενώ επιθέσεις άρνησης υπηρεσιών (DoS) μπορούν να

καταστήσουν τον διακομιστή μη διαθέσιμο. Σημαντικό πρόβλημα αποτελεί και η ύπαρξη μη διαχειριζόμενων ή ξεχασμένων δεδομένων, τα οποία παραμένουν ευάλωτα, όπως επίσης και τα μη προστατευμένα αρχεία αντιγράφων ασφαλείας. Επίσης, τα υπερβολικά δικαιώματα πρόσβασης επιτρέπουν κατάχρηση, ενώ η παρουσία κακόβουλου λογισμικού μπορεί να εκμεταλλευτεί τα δικαιώματα των χρηστών για να αποκτήσει πρόσβαση στη βάση.

Ο αντίκτυπος αυτών των απειλών είναι εκτεταμένος, αφού υπονομεύεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα του συστήματος, επηρεάζοντας άμεσα δείκτες όπως η Template Capacity και το Failure to Enroll Rate (FTE), λόγω της πιθανής αλλοίωσης, απώλειας ή μη εξουσιοδοτημένης αποκάλυψης δεδομένων. Παράδειγμα αποτελεί μια επίθεση SQL Injection που δίνει πρόσβαση σε όλα τα βιομετρικά δεδομένα μιας τράπεζας, με αποτέλεσμα τη διαρροή κρίσιμων προσωπικών πληροφοριών.

Ως αντίμετρα μπορούν να εφαρμοστούν ασφαλείς πρακτικές διαμόρφωσης, τακτικός έλεγχος δικαιωμάτων, ισχυρή κρυπτογράφηση, καθώς και σωστή διαχείριση αντιγράφων ασφαλείας. Το σημείο εκκίνησης αυτών των απειλών εντοπίζεται τόσο σε κακόβουλες ενέργειες όσο και σε ανθρώπινο λάθος ή σε αστοχίες υλοποίησης.

Γ.4 Μέτρα προστασίας των βιομετρικών συστημάτων.

Για την ενίσχυση της ασφάλειας των βιομετρικών συστημάτων αυθεντικοποιήσης, συνιστάται η εφαρμογή τεχνικών εντοπισμού ζωντανότητας (liveness detection) ή η χρήση πολυπαραγοντικής ταυτοποίησης που συνδυάζει βιομετρικά χαρακτηριστικά με άλλους παράγοντες, όπως κωδικούς πρόσβασης ή διακριτικά (tokens). Η χρήση κρυπτογράφησης και ελέγχων πρόσβασης για την προστασία των αποθηκευμένων προτύπων είναι επίσης απαραίτητη, όπως και η εφαρμογή τεχνικών προστασίας προτύπων, όπως ο μηχανισμός ασαφούς θήκης (fuzzy vaults) ή τα ακυρώσιμα βιομετρικά (cancelable biometrics). Η ανίχνευση ζωντανότητας (liveness detection) είναι κρίσιμη για να διασφαλιστεί ότι το βιομετρικό στοιχείο που παρουσιάζεται προέρχεται από ζωντανό χρήστη και όχι από αποθηκευμένο πρότυπο, ενώ πρέπει να γίνεται τακτική ενημέρωση και ασφαλής αποθήκευση των βιομετρικών προτύπων, καθώς και παρακολούθηση για ασυνήθιστα μοτίβα ταυτοποίησης.

Η εφαρμογή φυσικών μέτρων ασφαλείας για την προστασία του βιομετρικού αισθητήρα και του συστήματος, όπως η χρήση υλικού ανθεκτικού σε παραβιάσεις (tamper-resistant hardware) και η κρυπτογράφηση των βιομετρικών δεδομένων κατά τη μετάδοση και την αποθήκευση, αποτελεί επίσης σημαντικό βήμα. Συνιστάται η χρήση συστημάτων ανίχνευσης εισβολών (intrusion detection systems) για την παρακολούθηση ασυνήθιστης φυσικής δραστηριότητας, καθώς και η χρήση ασφαλών διαύλων επικοινωνίας μεταξύ του βιομετρικού αισθητήρα και του συστήματος..

Η χρήση πρωτοκόλλων πρόκλησης-απόκρισης (challenge-response) μπορεί να συμβάλλει στο να διασφαλιστεί ότι το βιομετρικό δείγμα είναι πρόσφατο, ενώ η εφαρμογή πολυπαραγοντικής ταυτοποίησης αποτελεί επιπλέον μέτρο ενίσχυσης της ασφάλειας. Είναι σημαντική η επιβολή αυστηρών ελέγχων πρόσβασης και διαδικασιών καταγραφής (auditing) ή η χρήση ανίχνευσης ανωμαλιών (anomaly detection) για τον εντοπισμό ασυνήθιστων προτύπων χρήσης του συστήματος.

Επιπρόσθετα, είναι κρίσιμο να εκπαιδεύονται οι χρήστες σχετικά με τους κινδύνους των επιθέσεων κοινωνικής μηχανικής (social engineering), ώστε να μπορούν να τις αναγνωρίζουν και να τις αποφεύγουν. Η εφαρμογή αυστηρών πολιτικών ελέγχου πρόσβασης περιορίζει την πρόσβαση σε βιομετρικά δεδομένα, ενώ η χρήση πολυπαραγοντικής ταυτοποίησης ενισχύει τη συνολική ασφάλεια του συστήματος. Τέλος, η τακτική παρακολούθηση και ο έλεγχος του βιομετρικού συστήματος για ύποπτη δραστηριότητα αποτελεί αναπόσπαστο μέρος μιας ολοκληρωμένης στρατηγικής προστασίας.

Για την αντιμετώπιση των επιθέσεων SQL Injections, είναι σημαντικό να χρησιμοποιείται επεξεργασμένο πρωτόκολλο αντί για απευθείας ερωτήματα και να εφαρμόζεται η αρχιτεκτονική MVC, ώστε να περιορίζεται η δυνατότητα εισαγωγής κακόβουλου κώδικα από τον χρήστη.

Όσον αφορά τα τρωτά σημεία και τις λανθασμένες ρυθμίσεις βάσεων δεδομένων, τα συστήματα δεν πρέπει να διαθέτουν προεπιλεγμένους λογαριασμούς και οι υπάλληλοι πληροφορικής πρέπει να είναι κατάλληλα εκπαιδευμένοι και έμπειροι, ώστε να αναγνωρίζουν και να αντιμετωπίζουν γρήγορα τις πιθανές αδυναμίες.

Για την αντιμετώπιση των επιθέσεων Άρνησης Παροχής Υπηρεσιών (DoS), συνιστάται η ενίσχυση του TCP/IP stack με τις κατάλληλες ρυθμίσεις καταχώρησης, ώστε να μεγιστοποιείται το μέγεθος της λίστας συνδέσεων TCP. Επιπλέον, πρέπει να μειώνεται ο χρόνος δημιουργίας σχέσης, να χρησιμοποιούνται δυναμικές δομές ουράς σύνδεσης ώστε η ουρά να μην εξαντλείται και να εφαρμόζεται δικτυακό Σύστημα Ανίχνευσης Εισβολών (IDS) για την παρακολούθηση ύποπτης δραστηριότητας.

Για τα μη διαχειριζόμενα ευαίσθητα δεδομένα, επιβάλλεται η κρυπτογράφηση όλων των εμπιστευτικών δεδομένων στις βάσεις δεδομένων, η εφαρμογή των κατάλληλων ελέγχων και δικαιωμάτων πρόσβασης στους διακομιστές, καθώς και η εκτέλεση τακτικών ελέγχων για τον εντοπισμό νέων σημαντικών δεδομένων στα αποθετήρια. Για τον σκοπό αυτό μπορεί να χρησιμοποιηθεί μια πλατφόρμα Τακτικής Ανακάλυψης Δεδομένων και ένας Διαχειριστής Εφαρμογής Ελέγχων, οι οποίοι μπορούν να εντοπίζουν άμεσα και να διασφαλίζουν τα νέα εμπιστευτικά δεδομένα.

Για την προστασία από έκθεση αντιγράφων ασφαλείας βάσεων δεδομένων, οι βάσεις δεδομένων και τα αντίγραφα ασφαλείας πρέπει να είναι κρυπτογραφημένα, καθώς η αποθήκευση σε

κρυπτογραφημένη μορφή διασφαλίζει τόσο τα δεδομένα παραγωγής όσο και τα αντίγραφα ασφαλείας. Απαραίτητος είναι και ο έλεγχος όλων των διακομιστών και αντιγράφων, ώστε να παρακολουθείται ποιος προσπαθεί να αποκτήσει πρόσβαση σε εμπιστευτικές πληροφορίες.

Για την αντιμετώπιση του κινδύνου από υπερβολικά δικαιώματα πρόσβασης στη βάση δεδομένων, προτείνεται η εφαρμογή και διατήρηση μιας αυστηρής πολιτικής διαχείρισης πρόσβασης και δικαιωμάτων. Δεν πρέπει να παρέχονται υπερβολικά δικαιώματα στους χρήστες και πρέπει να γίνεται άμεση ανάκληση των δικαιωμάτων που δεν χρησιμοποιούνται πλέον.

Τέλος, για την προστασία από επιθέσεις κακόβουλου λογισμικού (malware), είναι σημαντικό να διασφαλιστεί ότι τα συστήματα παραμένουν ενημερωμένα και προστατευμένα, καθώς το malware μπορεί να εκμεταλλευτεί την πρόσβαση των νόμιμων χρηστών για να αποκτήσει πρόσβαση στα δεδομένα της επιχείρησης.

Γ.5 Συγκεντρωτικά αποτελέσματα μελέτης ασφάλειας Βιομετρικών συστημάτων.

Το κεφάλαιο αυτό συνοψίζει τα ευρήματα της μελέτης σχετικά με την ασφάλεια των βιομετρικών συστημάτων, οργανωμένα με βάση τα βασικά δομικά τους στοιχεία: **Λογισμικό**, **Υλικό**, **Επικοινωνία** και **Αποθήκευση δεδομένων**. Για κάθε κατηγορία εντοπίστηκαν και καταγράφηκαν οι κυριότερες απειλές και μορφές επιθέσεων που δύνανται να τις στοχεύσουν, οι αντίστοιχες ευπάθειες που εκμεταλλεύονται, καθώς και ο πιθανός αντίκτυπος στην ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα του συστήματος.

Για κάθε δομικό στοιχείο προτείνονται αντίστοιχα **μέτρα προστασίας**, όπως η εφαρμογή τεχνικών ακυρώσιμων βιομετρικών και ανανέωσης λογισμικού, η χρήση προηγμένων αισθητήρων με δυνατότητα ανίχνευσης ζωντανού οργανισμού, η κρυπτογράφηση και ψηφιακή υπογραφή μεταδιδόμενων δεδομένων, καθώς και η ασφαλής διαχείριση προνομίων και αρχιτεκτονική MVC στις βάσεις δεδομένων. Η συγκεντρωτική αυτή παρουσίαση προσφέρει μια ολοκληρωμένη εικόνα των κύριων σημείων ευπάθειας και των βέλτιστων πρακτικών άμυνας, συμβάλλοντας στην αποτελεσματική θωράκιση των βιομετρικών συστημάτων έναντι σύγχρονων απειλών.

Table 2 Μελέτη Ασφάλειας Βιομετρικών Συστημάτων..

Δομικό Στοιχείο	Απειλές / Επιθέσεις	Ευπάθειες	Αντίκτυπος	Μέτρα Προστασίας
1. Λογισμικό (Software)	Spoofing, Replay attacks, Data simulation, Template attacks	Αστοχίες αλγορίθμων αναγνώρισης, ψευδείς αποδοχές/απορρίψεις, ευπάθειες σε πλαστά δεδομένα	Μη εξουσιοδοτημένη πρόσβαση, απώλεια εμπιστευτικότητας & ιδιωτικότητας, παραποίηση/υποκλοπή βιομετρικών, απώλεια ακεραιότητας, μειωμένη διαθεσιμότητα, αλλοίωση μετρήσεων, οικονομικές απώλειες, νομικές κυρώσεις, μείωση αξιοπιστίας (FAR, FRR, EER, ROC)	Βελτίωση & εκπαίδευση αλγορίθμων, τακτική ενημέρωση λογισμικού, πολυπαραγοντική ταυτοποίηση, liveness detection
2. Υλικό (Hardware)	Spoofing με ψεύτικα δάχτυλα/μάσκες/ εικόνες	Χαμηλής ανάλυσης ή φθαρμένοι αισθητήρες, περιβαλλοντικοί παράγοντες		Τακτική συντήρηση, καθαρισμός αισθητήρων, χρήση υψηλής ανάλυσης & tamper-resistant hardware
3. Επικοινωνία (Communications)	Man-in-the-middle, Replay attacks, υποκλοπή/αλλοίωση δεδομένων	Μη ασφαλή πρωτόκολλα, απουσία κρυπτογράφησης		Χρήση TLS/SSL, ασφαλή κανάλια, challenge-response πρωτόκολλα, έλεγχος ταυτότητας κόμβων

4. Βάση Δεδομένων (Database; local or third party)	SQL Injections, NoSQL injections, Template attacks, DoS, Malware, κλοπή προτύπων	Μη ασφαλής αποθήκευση, προεπιλεγμένοι λογαριασμοί, υπερβολικά δικαιώματα, μη κρυπτογραφημένα backups		Κρυπτογράφηση δεδομένων/αντιγράφων, ακυρώσιμα βιομετρικά, IDS, πολιτικές ελέγχου πρόσβασης, MVC αρχιτεκτονική, τακτικός έλεγχος δικαιωμάτων

Κεφάλαιο Δ: Εφαρμογές Τεχνητής Νοημοσύνης στην ασφάλεια των Βιομετρικών συστημάτων.

Δ.1 Εισαγωγή

Η ραγδαία εξέλιξη της Τεχνητής Νοημοσύνης (AI) έχει φέρει επανάσταση σε πολλούς τομείς της καθημερινότητάς μας, αλλά ταυτόχρονα εγείρει σοβαρά ζητήματα ασφαλείας στον τομέα της αυθεντικοποίησης. Τα βιομετρικά συστήματα, όπως η αναγνώριση προσώπου, οι σαρωτές δακτυλικών αποτυπωμάτων, η αναγνώριση φωνής και η σάρωση ίριδας σχεδιάστηκαν για να παρέχουν υψηλά επίπεδα ασφάλειας και να αντικαταστήσουν τους παραδοσιακούς κωδικούς πρόσβασης, ωστόσο, η χρήση προηγμένων αλγορίθμων AI έχει αποδείξει ότι μπορεί να παρακάμψει αυτά τα μέτρα, καθιστώντας τα πιο ευάλωτα από ποτέ.

Η δημιουργία deepfake εικόνων και φωνής, οι επιθέσεις μέσω αντιγραφής βιομετρικών δεδομένων και η δυνατότητα παραποίησης ταυτοτήτων αποτελούν αυξανόμενες απειλές. Η τεχνητή νοημοσύνη μπορεί πλέον να δημιουργήσει σχεδόν τέλειες προσομοιώσεις ανθρώπινων χαρακτηριστικών, εξαπατώντας ακόμα και τα πιο εξελιγμένα συστήματα ασφαλείας. Χάρη στις τεχνικές της μηχανικής μάθησης, οι επιτιθέμενοι μπορούν να αναλύσουν και να αναπαράγουν βιομετρικά χαρακτηριστικά από ελάχιστα δείγματα, όπως μια φωτογραφία στα μέσα κοινωνικής δικτύωσης ή ένα αρχείο ηχογραφημένης φωνής.

Ακόμη πιο ανησυχητικό είναι το γεγονός ότι οι αλγόριθμοι τεχνητής νοημοσύνης μπορούν να εντοπίσουν αδυναμίες στα συστήματα ασφαλείας και να δημιουργήσουν νέες μεθόδους παραβίασης, όπως η χρήση γενετικών αλγορίθμων για την κατασκευή πλαστών βιομετρικών δεδομένων που μπορούν να παρακάμψουν αισθητήρες και ελέγχους ταυτοποίησης. Οι επιτιθέμενοι έχουν αρχίσει να εκμεταλλεύονται αυτές τις δυνατότητες, καθιστώντας τις παραβιάσεις δεδομένων πιο εύκολες και πιο επικίνδυνες από ποτέ.

Όμως, σημαντική είναι και η συνεισφορά των μοντέλων που βασίζονται στην βαθιά μάθηση (Deep learning) μιας και μπορούν με μεγάλη επιτυχία όχι μόνο να αναγνωρίζουν βιομετρικά δεδομένα αλλά και να διαχωρίζουν τα πραγματικά από τα πλαστά (liveness detection). Τα μοντέλα αυτά, αξιοποιούνται όλο και περισσότερο για τη βελτίωση της ασφάλειας διαφόρων συστημάτων βιομετρικής αναγνώρισης.

Δ.2 Η αρνητική πλευρά των εφαρμογών τεχνητής νοημοσύνης στα βιομετρικά συστήματα αυθεντικοποιήσης.

Δ.2.1 Deepfakes

Τα deepfakes είναι μια ραγδαία αναπτυσσόμενη τεχνολογία που βασίζεται στην τεχνητή νοημοσύνη (AI) και επιτρέπει τη δημιουργία ρεαλιστικών αλλά ψεύτικων πολυμεσικών περιεχομένων, όπως βίντεο, εικόνα και ήχο. Η τεχνολογία αυτή χρησιμοποιεί δίκτυα GANs (Generative adversarial networks) και προηγμένα νευρωνικά δίκτυα για να παράγει πλαστές εικόνες.

Η αυξανόμενη χρήση των deepfakes έχει προκαλέσει έντονες συζητήσεις [22][26] σχετικά με την ηθική χρήση της τεχνολογίας, την πιθανότητα παραπληροφόρησης και την ανάγκη για εργαλεία εντοπισμού τους. Από τη μία πλευρά, υπάρχουν θετικές εφαρμογές, όπως η χρήση τους στη βιομηχανία του κινηματογράφου, της ψυχαγωγίας και της εκπαίδευσης. Από την άλλη, η κακόβουλη χρήση τους μπορεί να οδηγήσει σε πολιτική προπαγάνδα, παραπληροφόρηση, εκβιασμούς και παραβίαση της ιδιωτικότητας.

- Περιγραφή των Deepfakes

Τα deepfakes αποτελούν προϊόντα προηγμένων τεχνικών τεχνητής νοημοσύνης και μηχανικής μάθησης, που επιτρέπουν την ημι-αυτοματοποιημένη δημιουργία ψεύτικου περιεχομένου, όπως εικόνες, βίντεο και ήχος, τα οποία είναι ολοένα και πιο δύσκολο να εντοπιστούν από ανθρώπινους παρατηρητές. Για παράδειγμα, υπάρχουν βίντεο όπου το πρόσωπο ενός ατόμου αντικαθίσταται με εκείνο κάποιου άλλου, δημιουργώντας την ψευδαίσθηση ότι το άτομο συμμετέχει σε καταστάσεις στις οποίες δεν έχει πραγματικά εμπλακεί.

- Λειτουργία των Deepfakes

Η πλειονότητα των σημερινών deepfakes, ακολουθούν μια διαδικασία κατά την οποία το πραγματικό βιομετρικό χαρακτηριστικό ενός ατόμου, αντικαθίσταται από ένα χαρακτηριστικό ενός άλλου ατόμου. Υπάρχουν όμως και συστήματα παραγωγής deepfake χαρακτηριστικών που παράγουν ψεύτικα βιομετρικά χαρακτηριστικά με μεγάλη ακρίβεια. Η παραγωγή των deepfakes περιλαμβάνει τη χρήση νευρωνικών δικτύων για την εκμάθηση και αναπαραγωγή χαρακτηριστικών, επιτρέποντας μια πειστική αντικατάσταση ή παραγωγή.

- Τύποι Deepfakes

Τα deepfakes ταξινομούνται σε διάφορες κατηγορίες, συμπεριλαμβανομένων των φωτογραφιών, για παράδειγμα deepfakes προσώπου και δαχτυλικών αποτυπωμάτων, του ήχου όπως αυτά της

φωνής, των βίντεο όπως η μορφοποίηση προσώπου και του συνδυασμού ήχου και βίντεο. Αυτές οι τεχνικές εξελίσσονται ραγδαία, προσφέροντας νέες δυνατότητες αλλά και προκλήσεις.

- Επιπτώσεις των Deepfakes

Τα deepfakes έχουν τη δυνατότητα να επηρεάσουν αρνητικά άτομα, οργανισμούς και κυβερνήσεις. Μπορούν να χρησιμοποιηθούν για τη δημιουργία παραπλανητικών πληροφοριών, την παραβίαση της ιδιωτικότητας και την υπονόμευση της εμπιστοσύνης στο ψηφιακό περιεχόμενο. Παραδείγματα περιλαμβάνουν ψεύτικα βίντεο πολιτικών προσωπικοτήτων που κάνουν δηλώσεις που ποτέ δεν έγιναν από τους ίδιους, οδηγώντας σε παραπληροφόρηση και κοινωνική αναταραχή.

- Το Πλαίσιο R.E.A.L. για τη Διαχείριση των Κινδύνων των Deepfakes

Για την αντιμετώπιση των κινδύνων που προκύπτουν από τα deepfakes, οι συγγραφείς προτείνουν στο [22] το πλαίσιο R.E.A.L., το οποίο περιλαμβάνει:

1. **Record (Καταγραφή):** Καταγραφή αυθεντικού περιεχομένου, για να διασφαλιστεί η δυνατότητα διάψευσης ψεύτικων ισχυρισμών.
2. **Expose (Ανακάλυψη):** Έγκαιρη ανακάλυψη των deepfakes μέσω της ανάπτυξης τεχνολογιών ανίχνευσης.
3. **Advocate (Υποστήριξη):** Υποστήριξη νομικής προστασίας και ρυθμίσεων για την αντιμετώπιση της κακόβουλης χρήσης των deepfakes.
4. **Leverage (Αξιοποίηση):** Αξιοποίηση της εμπιστοσύνης για την αντιμετώπιση της ευπιστίας, προωθώντας την κριτική σκέψη και την επαλήθευση πληροφοριών.

Ακολουθώντας αυτές τις αρχές, η κοινωνία μπορεί να προετοιμαστεί καλύτερα για να αντιμετωπίσει τις προκλήσεις που θέτουν τα deepfakes, ενώ παράλληλα να εκμεταλλευτεί τις θετικές τους εφαρμογές.

- Συμπεράσματα

Τα deepfakes αντιπροσωπεύουν μια σημαντική εξέλιξη στην τεχνολογία ψηφιακής επεξεργασίας, με βαθιές επιπτώσεις στην κοινωνία. Ενώ προσφέρουν νέες ευκαιρίες για δημιουργικότητα και καινοτομία, ενέχουν επίσης σοβαρούς κινδύνους για την παραπληροφόρηση, την ιδιωτικότητα και την εμπιστοσύνη στο ψηφιακό περιεχόμενο. Η κατανόηση της τεχνολογίας πίσω από τα deepfakes, η αναγνώριση των διαφόρων μορφών τους και η εφαρμογή στρατηγικών εντοπισμού τους είναι ζωτικής σημασίας για την προστασία της κοινωνίας από την κακόβουλη χρήση τους.

Δ.2.2 Spoofing

- **Εισαγωγή στις Επιθέσεις Spoofing**

Οι επιθέσεις spoofing στα συστήματα Βιομετρικής Αυθεντικοποιήσης, αποτελούν μία από τις πιο κρίσιμες απειλές στον τομέα της βιομετρικής αυθεντικοποιήσης. Καθώς τα βιομετρικά δεδομένα αποκτούν ολοένα και μεγαλύτερη σημασία στην αυθεντικοποίηση των χρηστών, οι επιτιθέμενοι αναπτύσσουν εξελιγμένες τεχνικές για να παρακάμψουν τα συστήματα αυτά. Οι επιθέσεις spoofing αποσκοπούν στο να εξαπατήσουν τον αισθητήρα βιομετρικών με πλαστά ή παραποιημένα δεδομένα, ώστε να επιτευχθεί μη εξουσιοδοτημένη πρόσβαση.

- **Μορφές Επιθέσεων Spoofing**

Υπάρχουν διάφορες μορφές spoofing επιθέσεων που στοχεύουν τα συστήματα βιομετρικής αυθεντικοποιήσης, μερικές εκ των οποίων είναι ιδιαίτερα δύσκολο να εντοπιστούν:

- **Απομιμήσεις φυσικών δειγμάτων**: Οι επιτιθέμενοι κατασκευάζουν ρεαλιστικά αντίγραφα δακτυλικών αποτυπωμάτων από υλικά όπως ζελατίνη, σιλικόνη ή πλαστικό, με στόχο να ξεγελάσουν αισθητήρες δακτυλικών αποτυπωμάτων. Αντίστοιχα, για την αναγνώριση προσώπου, χρησιμοποιούνται εκτυπώσεις υψηλής ανάλυσης, βίντεο ή ακόμα και τρισδιάστατες μάσκες.
- **Επιθέσεις παρουσίασης (Presentation Attacks)**: Σε αυτή τη μέθοδο, ένας επιτιθέμενος παρουσιάζει έναν πλαστό ή αλλοιωμένο βιομετρικό στοιχείο απευθείας στον αισθητήρα. Για παράδειγμα, 3D μάσκες προσώπου, ψηφιακά βίντεο ή οι φωτογραφίες μπορούν να χρησιμοποιηθούν για να μιμηθούν ένα πρόσωπο και να περάσουν την επαλήθευση ως νόμιμος χρήστης.
- **Επιθέσεις επανάληψης (Replay Attacks)**: Σε αυτές τις επιθέσεις, βιομετρικά δεδομένα που έχουν καταγραφεί νωρίτερα (π.χ. φωνητικές εντολές) επαναχρησιμοποιούνται με σκοπό να παρακαμφθεί η αυθεντικοποίηση. Αυτού του είδους οι επιθέσεις είναι συχνές στα συστήματα φωνητικής αναγνώρισης.
- **Ψηφιακή παραποίηση μέσω deepfake**: Η πρόοδος στην τεχνητή νοημοσύνη έχει επιτρέψει τη δημιουργία εξαιρετικά ρεαλιστικών deepfake μέσων, τα οποία μπορούν να ξεγελάσουν ακόμα και προηγμένα συστήματα αναγνώρισης προσώπου ή φωνής. Η απειλή αυτή αυξάνεται συνεχώς λόγω της ευκολίας διάθεσης αυτών των εργαλείων online.

- **Αδυναμίες των Συστημάτων Βιομετρικής Αυθεντικοποιήσης έναντι του Spoofing**

Τα βιομετρικά συστήματα είναι σχεδιασμένα ώστε να προσφέρουν βιομετρική αναγνώριση σε πολλαπλές πλατφόρμες και συσκευές μέσω cloud. Αυτή η αρχιτεκτονική, αν και ευέλικτη και επεκτάσιμη, δημιουργεί νέες αδυναμίες:

- **Απομακρυσμένη πρόσβαση**: Οι χρήστες δεν χρειάζεται να βρίσκονται φυσικά στον χώρο όπου λαμβάνει χώρα η αναγνώριση, κάτι που διευκολύνει τις spoofing επιθέσεις με στατικά ή ψηφιακά μέσα.
- **Ανεπαρκής έλεγχος εισόδου**: Ορισμένα βιομετρικά συστήματα δεν εφαρμόζουν αυστηρούς μηχανισμούς ελέγχου ζωτικότητας ή άλλες μεθόδους επαλήθευσης γνησιότητας, επιτρέποντας έτσι την παρουσίαση πλαστών δειγμάτων.
- **Ετερογένεια παρόχων**: Τα συστήματα βιομετρικής αυθεντικοποίησης προσφέρονται από πολλούς διαφορετικούς παρόχους, με αποτέλεσμα η ποιότητα και η αυστηρότητα των μέτρων ασφαλείας διαφέρουν σημαντικά. Αυτό καθιστά ορισμένα συστήματα πιο ευάλωτα από άλλα.

- **Επιπτώσεις των Επιθέσεων Spoofing**

Οι επιθέσεις spoofing δεν είναι απλώς τεχνικές προκλήσεις – έχουν σημαντικές επιπτώσεις σε επίπεδο ιδιωτικότητας, εμπιστοσύνης και ασφάλειας:

- **Παραβίαση προσωπικών δεδομένων**: Η επιτυχής είσοδος μέσω spoofing σημαίνει ότι ο εισβολέας μπορεί να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες και να τις εκμεταλλευτεί χωρίς εξουσιοδότητηση.
- **Απώλεια εμπιστοσύνης των χρηστών**: Η μη ασφαλής αυθεντικοποίηση πλήττει την αξιοπιστία της υπηρεσίας και αποθαρρύνει τους χρήστες από τη χρήση βιομετρικών τεχνολογιών και των υπηρεσιών που αυτά προστατεύουν.
- **Νομικές και κανονιστικές συνέπειες**: Σε ορισμένες περιπτώσεις, οι παραβιάσεις που οφείλονται σε ανεπαρκή προστασία βιομετρικών δεδομένων ενδέχεται να παραβιάζουν νομοθεσίες περί απορρήτου και να επιφέρουν κυρώσεις.

- **Συμπεράσματα**

Οι επιθέσεις spoofing συνιστούν μια διαρκώς εξελισσόμενη απειλή για τα βιομετρικά συστήματα. Η φύση των επιθέσεων αυτών είναι πολυμορφική και ολοένα πιο προσβάσιμη σε κακόβουλους

χρήστες. Ο αυξανόμενος κίνδυνος καθιστά σαφές ότι οι οργανισμοί που υιοθετούν ή παρέχουν υπηρεσίες βιομετρικής αυθεντικοποιήσης οφείλουν να κατανοήσουν βαθύτερα τους τύπους αυτών των επιθέσεων και τις ευπάθειες που εκμεταλλεύονται. Μόνο με αυτή τη γνώση μπορεί να χαραχθεί ένας αξιόπιστος δρόμος για την ασφάλεια της βιομετρικής αυθεντικοποίησης στο μέλλον.

Δ.2.3 Επιθέσεις (Adversarial Attacks)

Τα βιομετρικά συστήματα εξαρτώνται από μοντέλα μηχανικής μάθησης (ML) για να κατηγοριοποιούν και να επαληθεύουν αποτελεσματικά τα άτομα με βάση τα διακριτικά βιομετρικά χαρακτηριστικά τους. Αυτά τα μοντέλα, ωστόσο, είναι ευάλωτα σε επιθέσεις αντιπάλου, οι οποίες επιδιώκουν να τροποποιήσουν ή να διαταράξουν τα δεδομένα εισόδου με τέτοιο τρόπο ώστε το μοντέλο να τα ταξινομεί λανθασμένα.

Στον τομέα της βιομετρίας, οι επιθέσεις αντιπάλου μπορεί να λάβουν πολλές διαφορετικές μορφές. Η δημιουργία ψεύτικων δειγμάτων είναι μια τυπική μέθοδος. Ένας επιτιθέμενος μπορεί να δημιουργήσει ψεύτικα βιομετρικά δεδομένα που αντιγράφουν τα χαρακτηριστικά εξουσιοδοτημένων ατόμων ή νέες ταυτότητες. Για να ξεγελάσει το μοντέλο και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση, ο επιτιθέμενος εισάγει αυτά τα ψεύτικα δείγματα στο σύστημα. Για παράδειγμα, παρουσιάζοντας ένα συνθετικό αλλά φαινομενικά ρεαλιστικό πρόσωπο που ταιριάζει στενά με το πρόσωπο ενός εξουσιοδοτημένου χρήστη, μπορεί να προσπαθήσει να εξαπατήσει ένα σύστημα αναγνώρισης προσώπου.

Η αλλοίωση ακριβών βιομετρικών πληροφοριών αποτελεί διαφορετικό είδος επίθεσης αντιπάλου. Ένας επιτιθέμενος μπορεί να προσπαθήσει να παρακάμψει τη διαδικασία επαλήθευσης του συστήματος τροποποιώντας τα χαρακτηριστικά των βιομετρικών στοιχείων ενός ατόμου, όπως τα δακτυλικά αποτυπώματα ή τα μοτίβα ομιλίας. Αυτή η παραποίηση μπορεί να περιλαμβάνει φυσικές αλλαγές, όπως η εφαρμογή συνθετικών δακτυλικών αποτυπωμάτων, ή ψηφιακές αλλαγές στα βιομετρικά δεδομένα που έχουν καταγραφεί σε μια βάση δεδομένων. Ο στόχος είναι να ξεγελαστεί το σύστημα ώστε να θεωρήσει λανθασμένα τα τροποποιημένα βιομετρικά δεδομένα, επιτρέποντας ανεπιθύμητη πρόσβαση ή διευκολύνοντας την κλοπή ταυτότητας.

Ο αντίκτυπος τέτοιων επιθέσεων είναι σημαντικός, καθώς θέτει σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του συστήματος. Η λανθασμένη ταξινόμηση που προκαλείται αυξάνει τον δείκτη False Accept Rate και επηρεάζει το Equal Error Rate, μειώνοντας την αξιοπιστία του συστήματος. Για τον χρήστη, οι επιπτώσεις μπορεί να είναι ιδιαίτερα σοβαρές, καθώς ενδέχεται να υπάρξει μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα ή να διευκολυνθεί η κλοπή ταυτότητας.

Ένα χαρακτηριστικό παράδειγμα αποτελεί η δημιουργία ενός συνθετικού προσώπου, το οποίο παρουσιάζεται στο σύστημα αναγνώρισης προσώπου και καταφέρνει να αναγνωριστεί λανθασμένα ως εξουσιοδοτημένος χρήστης. Με τον ίδιο τρόπο, η παραποίηση της φωνής μέσω ειδικών εργαλείων μπορεί να ξεγελάσει ένα σύστημα αναγνώρισης ομιλίας.

Δ.2.4 Δηλητηρίαση Δεδομένων (Data Poisoning)

Οι αλγόριθμοι μηχανικής μάθησης (ML) χρησιμοποιούν δεδομένα εκπαίδευσης για να εντοπίζουν πρότυπα και να παρέχουν ακριβείς προβλέψεις. Στα βιομετρικά συστήματα, τα δεδομένα εκπαίδευσης συνήθως αποτελούνται από ατομικά βιομετρικά δείγματα.

Η απόδοση του βιομετρικού συστήματος μπορεί να υπονομευθεί εάν ένας επιτιθέμενος καταφέρει να εισαγάγει μεροληψίες ή κακόβουλα μοντέλα μέσω χειραγώγησης των δεδομένων εκπαίδευσης που χρησιμοποιούνται για την ανάπτυξη της μεθόδου. Οι επιθέσεις που είναι γνωστές ως «δηλητηρίαση δεδομένων» περιλαμβάνουν την προσθήκη λανθασμένων ή κακόβουλων δειγμάτων στα δεδομένα εκπαίδευσης. Ένας επιτιθέμενος ελπίζει να επηρεάσει τη διαδικασία μάθησης του μοντέλου με τρόπο που να παράγει ανακριβείς ή μεροληπτικές εξόδους.

Ο αντίκτυπος είναι σημαντικός τόσο για το σύστημα όσο και για τον χρήστη. Η ακεραιότητα και η εμπιστευτικότητα των δεδομένων παραβιάζονται, ενώ επηρεάζεται η ακρίβεια του μοντέλου, αυξάνοντας τους δείκτες False Reject Rate και False Accept Rate. Αυτό οδηγεί σε πτώση της συνολικής απόδοσης, κάτι που αντικατοπτρίζεται στον δείκτη Equal Error Rate. Για τον χρήστη, οι συνέπειες περιλαμβάνουν άδικη απόρριψη πρόσβασης ή μη εξουσιοδοτημένη παραχώρηση πρόσβασης σε τρίτους.

Ένα χαρακτηριστικό παράδειγμα είναι η εισαγωγή πλήθους δειγμάτων από μια συγκεκριμένη δημογραφική ομάδα, με αποτέλεσμα το σύστημα να αποτυγχάνει να αναγνωρίσει σωστά τα μέλη αυτής της ομάδας. Παράλληλα, μέσω της εισαγωγής κρυφών triggers, ένας επιτιθέμενος μπορεί να καταφέρει μη εξουσιοδοτημένη πρόσβαση απλά προβάλλοντας ένα συγκεκριμένο μοτίβο.

Για την αποτροπή επιθέσεων δηλητηρίασης δεδομένων, πρέπει να διασφαλίζεται η ασφάλεια και η ακεραιότητα των δεδομένων εκπαίδευσης. Αυτό συνεπάγεται την εφαρμογή μεθόδων όπως η επικύρωση δεδομένων, η ανίχνευση ανωμαλιών και ο καθαρισμός δεδομένων, ώστε να εντοπίζονται και να απομακρύνονται πιθανώς επιβλαβή δείγματα. Τα δεδομένα εκπαίδευσης θα πρέπει να παρακολουθούνται και να ελέγχονται τακτικά ώστε να ανιχνεύονται πιθανές επικίνδυνες μεροληψίες ή ασυνήθιστα μοτίβα.

Δ.2.5 Μεταφερσιμότητα Επιθέσεων (Transferability of Attacks)

Η κατάσταση κατά την οποία μια επίθεση που εκμεταλλεύεται αδυναμίες σε ένα βιομετρικό σύστημα μπορεί να χρησιμοποιηθεί και σε άλλα παρόμοια συστήματα είναι γνωστή ως

μεταφερσιμότητα επιθέσεων. Στο πλαίσιο των βιομετρικών συστημάτων που βασίζονται στη μηχανική μάθηση (ML), αυτή η έννοια είναι ιδιαίτερα σημαντική.

Αν ένας χάκερ καταφέρει να εντοπίσει και να εκμεταλλευτεί αποτελεσματικά ευπάθειες σε ένα από αυτά τα συστήματα, τότε μπορεί να χρησιμοποιήσει την ίδια μέθοδο επίθεσης για να διεισδύσει και σε άλλα συστήματα που βασίζονται σε παρόμοια μοντέλα ή αλγορίθμους ML. Η επίδραση των ευπαθειών ενισχύεται από την «φορητότητα» των επιθέσεων μεταξύ πολλών συστημάτων, με πιθανή συνέπεια την επηρεασμό διαφορετικών πλατφορμών.

Ωστόσο, τα μοντέλα αυτά δεν είναι αλάνθαστα και μπορεί να είναι εκτεθειμένα σε διάφορες μορφές επιθέσεων. Για παράδειγμα, ένας επιτιθέμενος μπορεί να προσπαθήσει να ξεγελάσει το σύστημα παρέχοντας ένα βιομετρικό δείγμα που έχει αλλοιωθεί με τέτοιον τρόπο ώστε να φαίνεται συμβατό με το μοντέλο, αλλά να διαφέρει από το πραγματικό βιομετρικό χαρακτηριστικό. Αυτό μπορεί να οδηγήσει σε μιμητισμό ταυτότητας ή σε μη εξουσιοδοτημένη πρόσβαση.

Όταν μια επίθεση είναι επιτυχής εναντίον ενός συστήματος, αυτό δείχνει ότι τα μοντέλα ή οι αλγόριθμοι ML που χρησιμοποιούνται εμπεριέχουν βαθύτερες αδυναμίες. Αυτές οι ελλείψεις μπορεί να οφείλονται σε αδυναμίες του συνόλου εκπαίδευσης, σε λάθη σχεδιασμού του μοντέλου ή σε περιορισμούς της συνολικής αρχιτεκτονικής του συστήματος. Γνωρίζοντας αυτές τις ευπάθειες, οι χάκερ μπορούν να τις εκμεταλλευτούν και σε παρόμοια συστήματα.

Η μεταφερσιμότητα των επιθέσεων επηρεάζει σοβαρά την ασφάλεια των βιομετρικών συστημάτων. Διότι οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν την ίδια τεχνική για να παραβιάσουν άλλα συστήματα με παρόμοια χαρακτηριστικά, πράγμα που σημαίνει ότι ο εντοπισμός και η εκμετάλλευση μιας ευπάθειας σε ένα σύστημα μπορεί να έχει ευρύτερες συνέπειες. Αυτό μεταθέτει την ευθύνη στους προγραμματιστές και τους ερευνητές όχι μόνο να αντιμετωπίζουν τις ευπάθειες στα δικά τους συστήματα, αλλά και να λαμβάνουν υπόψη τον πιθανό αντίκτυπο σε ολόκληρο τον τομέα.

Ο αντίκτυπος είναι ιδιαίτερα σοβαρός, καθώς δεν διακυβεύεται μόνο η ασφάλεια ενός μεμονωμένου συστήματος αλλά και η αξιοπιστία μιας ολόκληρης κατηγορίας βιομετρικών εφαρμογών. Η εμπιστευτικότητα και η διαθεσιμότητα τίθενται σε κίνδυνο, ενώ αυξάνονται οι δείκτες FAR και FRR σε διαφορετικά συστήματα. Για τον χρήστη, αυτό σημαίνει ότι μια παραβίαση σε ένα σύστημα μπορεί να οδηγήσει σε έκθεση δεδομένων και απώλεια ιδιωτικότητας σε πολλαπλές πλατφόρμες.

Ένα παράδειγμα είναι η χρήση ενός παραποιημένου δείγματος προσώπου που έχει σχεδιαστεί να ξεγελά ένα συγκεκριμένο σύστημα αναγνώρισης, το οποίο στη συνέχεια καταφέρνει να εξαπατήσει και άλλα συστήματα που στηρίζονται στον ίδιο τύπο αλγορίθμου.

Δ.2.6 Αντιστροφή Μοντέλου (Model Inversion).

Μια επίθεση γνωστή ως *«model inversion attack»* μπορεί να χρησιμοποιηθεί για την εκμετάλλευση μοντέλων μηχανικής μάθησης (ML), ιδιαίτερα εκείνων που εφαρμόζονται σε βιομετρικά συστήματα. Αυτές οι επιθέσεις περιλαμβάνουν έναν κακόβουλο παράγοντα που υποβάλλει ερωτήματα στο μοντέλο με σκοπό την ανακατασκευή ή την απόκτηση ευαίσθητων δεδομένων.

Ένα μοντέλο μαθαίνει να πραγματοποιεί προβλέψεις ή να κατηγοριοποιεί δεδομένα εξετάζοντας πρότυπα και συσχετίσεις κατά τη διάρκεια της εκπαίδευσης. Ωστόσο, οι εσωτερικές λειτουργίες του μοντέλου συχνά δεν είναι διαφανείς ή εύκολα προσβάσιμες. Αυτό το χαρακτηριστικό αδιαφάνειας αποκαλείται *«μαύρο κουτί» (black box)* των μοντέλων ML.

Ένας αντίπαλος χρησιμοποιεί μια επίθεση αντιστροφής μοντέλου για να προσπαθήσει να το ανακατασκευάσει εκμεταλλευόμενος αυτά τα χαρακτηριστικά «μαύρου κουτιού». Ο επιτιθέμενος στοχεύει να ανακτήσει προσωπικά δεδομένα που το μοντέλο έχει μάθει κατά τη φάση της εκπαίδευσης, εισάγοντας προσεκτικά σχεδιασμένα δεδομένα εισόδου και παρατηρώντας τις αποκρίσεις του. Οι εξαγόμενες πληροφορίες μπορεί να περιλαμβάνουν προσωπικά στοιχεία ή συγκεκριμένα χαρακτηριστικά που σχετίζονται με τα βιομετρικά δεδομένα που χρησιμοποιούνται.

Οι επιθέσεις αντιστροφής μοντέλου αποτελούν σοβαρή απειλή για την ιδιωτικότητα στα βιομετρικά συστήματα. Για την ταυτοποίηση ή την επαλήθευση, τα βιομετρικά βασίζονται σε διακριτικά φυσικά ή συμπεριφορικά χαρακτηριστικά, όπως τα δακτυλικά αποτυπώματα ή τα χαρακτηριστικά του προσώπου. Εάν ένας επιτιθέμενος καταφέρει να αναδημιουργήσει τα αρχικά βιομετρικά δεδομένα μέσω ερωτήσεων στο μοντέλο, τα μέτρα ασφαλείας του συστήματος μπορεί να παρακαμφθούν, επιτρέποντας παράνομη πρόσβαση ή μιμητισμό ταυτότητας.

Ο αντίκτυπος είναι εξαιρετικά υψηλός, καθώς η επίθεση παραβιάζει την εμπιστευτικότητα και την ακεραιότητα των βιομετρικών δεδομένων. Οι δείκτες ασφάλειας επηρεάζονται άμεσα, καθώς αυξάνεται η πιθανότητα αποτυχίας αναγνώρισης (FRR) και λανθασμένης αποδοχής (FAR) εξαιτίας της κακής χρήσης ανακατασκευασμένων δεδομένων. Για τον χρήστη, οι συνέπειες περιλαμβάνουν απώλεια ιδιωτικότητας, μη εξουσιοδοτημένη χρήση της βιομετρικής ταυτότητας και αυξημένο κίνδυνο μιμητισμού ταυτότητας.

Ένα χαρακτηριστικό παράδειγμα είναι η ανακατασκευή μιας εικόνας προσώπου από το μοντέλο μέσω σταδιακής εισαγωγής δεδομένων εισόδου και παρατήρησης των αποκρίσεών του. Το αποτέλεσμα μπορεί να είναι μια φωτορεαλιστική εικόνα που αναπαριστά τον πραγματικό χρήστη, την οποία ο επιτιθέμενος μπορεί να αξιοποιήσει για spoofing επιθέσεις.

Δ.3 Πως ενισχύουν οι εφαρμογές της τεχνητής νοημοσύνης την ασφάλεια των βιομετρικών συστημάτων.

Τα τελευταία χρόνια, μοντέλα που βασίζονται στην βαθιά μάθηση (Deep learning) μπορούν με μεγάλη επιτυχία όχι μόνο να αναγνωρίζουν βιομετρικά δεδομένα αλλά και να διαχωρίζουν τα πραγματικά από τα πλαστά (liveness detection). Τα μοντέλα αυτά, αξιοποιούνται όλο και περισσότερο για τη βελτίωση της ασφάλειας διαφόρων συστημάτων βιομετρικής αναγνώρισης.

Αρχικά, η τεχνητή νοημοσύνη και ιδίως η βαθιά μάθηση, αναλύει τα μοτίβα των βιομετρικών δεδομένων, για να ανιχνεύσει λεπτομέρειες που υποδηλώνουν ζωντάνια, όπως μικροεκφράσεις ή κίνηση των ματιών με αποτέλεσμα να μπορούν να διαχωρίζουν τα βιομετρικά χαρακτηριστικά σε πραγματικά ή μη.

Επίσης, πολλά εργαλεία που βασίζονται στη τεχνητή νοημοσύνη παρακολουθούν τη συμπεριφορά του χρήστη, όπως πληκτρολόγηση, βάδισμα ή ταχύτητα αλληλεπίδρασης σε πραγματικό χρόνο. Αυτές οι συμπεριφορές είναι δύσκολο να αναπαραχθούν, και προσθέτουν ένα ακόμη επίπεδο επιβεβαίωσης της ζωντάνιας του βιομετρικού χαρακτηριστικού. Τα συστήματα ανίχνευσης ζωντάνιας, μπορούν επίσης να βελτιώνονται με την πάροδο του χρόνου, μαθαίνοντας από νέες τεχνικές παραποίησης και προσαρμόζοντας τις στρατηγικές ανίχνευσής τους ώστε να παραμένουν ‘’μπροστά’’ από τους επιτιθέμενους.

Τέλος, πολλές τεχνολογίες τεχνητής νοημοσύνης έχουν καταστεί ουσιαστικό στοιχείο για την προώθηση της ανίχνευσης ζωντάνιας, παρέχοντας τα δεδομένα που απαιτούνται για τη διάκριση μεταξύ γνήσιων και πλαστών βιομετρικών εισόδων με μεγάλη ακρίβεια. Μέσω της βαθιάς μάθησης η τεχνητή νοημοσύνη ενισχύει την ευρωστία, την αποτελεσματικότητα και την αξιοπιστία των σύγχρονων βιομετρικών συστημάτων. Καθώς οι τεχνικές spoofing συνεχίζουν να εξελίσσονται, η συνεχής έρευνα και ανάπτυξη στην ανίχνευση ζωντάνιας με βάση την τεχνητής νοημοσύνη θα είναι ζωτικής σημασίας για τη ασφάλεια των βιομετρικών συστημάτων.

Δ.4 Πίνακας μελέτης ασφάλειας Βιομετρικών συστημάτων με επιρροές από τεχνολογίες τεχνητής νοημοσύνης.

Το κεφάλαιο αυτό συνοψίζει τα ευρήματα της μελέτης σχετικά με την ασφάλεια των βιομετρικών συστημάτων, οργανωμένα με βάση τα βασικά δομικά τους στοιχεία: **Λογισμικό**, **Υλικό**, **Επικοινωνία** και **Αποθήκευση δεδομένων**., εστιάζοντας στις επιρροές που προκύπτουν από τη χρήση και την ενσωμάτωση τεχνολογιών τεχνητής νοημοσύνης (ΤΝ). Η μελέτη λαμβάνει υπόψη ότι διάφορες τεχνικές τεχνητής νοημοσύνης χρησιμοποιούνται ολοένα και περισσότερο για τη βελτίωση της ακρίβειας αναγνώρισης και την ανίχνευση ζωντανότητας, αλλά ταυτόχρονα εισάγουν νέες πιθανές επιθέσεις και μορφές ευπάθειας.

Η ανάλυση περιλαμβάνει την καταγραφή των βασικών **δομικών στοιχείων** των συστημάτων, των **απειλών** και **επιθέσεων** που ενδέχεται να στοχεύσουν μοντέλα μηχανικής μάθησης, των **ευπαθειών** που προκύπτουν από την εκπαίδευση, την ποιότητα και τη διαχείριση των δεδομένων, καθώς και του **αντίκτυπου** τέτοιων περιστατικών στην ασφάλεια και την αξιοπιστία του συστήματος.

Για κάθε καταγεγραμμένη περίπτωση προτείνονται **μέτρα προστασίας** που συνδυάζουν παραδοσιακές μεθόδους ασφάλειας με τεχνικές ανθεκτικής μηχανικής μάθησης, όπως η χρήση συνόλων δεδομένων υψηλής ποιότητας, η τακτική επανεκπαίδευση μοντέλων, η ανίχνευση αντιπαραδειγμάτων, η κρυπτογράφηση παραμέτρων μοντέλου και η εφαρμογή μηχανισμών πιστοποίησης της αυθεντικότητας των δεδομένων εισόδου.

Η παρουσίαση αυτή αποσκοπεί στο να παρέχει μια ολοκληρωμένη εικόνα της κατάστασης ασφάλειας βιομετρικών συστημάτων σε ένα περιβάλλον όπου η τεχνητή νοημοσύνη αποτελεί αναπόσπαστο αλλά και περίπλοκο παράγοντα, επιτρέποντας την εκτίμηση τόσο των ευκαιριών όσο και των προκλήσεων που αυτή εισάγει.

Table 3 Επιρροή τεχνολογιών Τεχνητής Νοημοσύνης στα βιομετρικά συστήματα.

Δομικό Στοιχείο	Απειλές / Επιθέσεις	Ευπάθειες	Αντίκτυπος	Μέτρα Προστασίας
1. Software	Spoofing, Replay attacks, Data simulation, Template attacks, **Deepfakes, Adversarial Attacks, Data Poisoning, Transferability of Attacks, Model Inversion**	Αστοχίες αλγορίθμων αναγνώρισης, ψευδείς αποδοχές/απορρίψεις, ευπάθειες σε πλαστά δεδομένα **μεροληψία ή παραποίηση δεδομένων εκπαίδευσης, αδυναμία ανίχνευσης αντιπαλικών εισόδων**	Μη εξουσιοδοτημένη πρόσβαση, απώλεια εμπιστευτικότητας & ιδιωτικότητας, παραποίηση/υποκλοπή βιομετρικών, απώλεια ακεραιότητας, μειωμένη διαθεσιμότητα, αλλοίωση μετρήσεων, οικονομικές απώλειες,	Βελτίωση & εκπαίδευση αλγορίθμων, τακτική ενημέρωση λογισμικού, πολυπαραγοντική ταυτοποίηση, liveness detection, **AI-based anomaly detection, έλεγχος δεδομένων εκπαίδευσης, αντίμετρα adversarial attacks**

2. Hardware	Spoofing με ψεύτικα δάχτυλα/μάσκες/ εικόνες , **Presentation Attacks**	Χαμηλής ανάλυσης ή φθαρμένοι αισθητήρες, περιβαλλοντικοί παράγοντες, **ανεπαρκής έλεγχος ζωτικότητας**	νομικές κυρώσεις, μείωση αξιοπιστίας (FAR, FRR, EER, ROC) **Παραπληροφόρηση μέσω deepfakes**	Τακτική συντήρηση, καθαρισμός αισθητήρων, χρήση υψηλής ανάλυσης & tamper-resistant hardware **ανίχνευση 3D δομών και μικροεκφράσεων**
3. Communications	Man-in-the-middle, Replay attacks, υποκλοπή/αλλοίωση δεδομένων, **Replay Attacks, Deepfakes (ήχος/βίντεο σε real-time επικοινωνία)**	Μη ασφαλή πρωτόκολλα, απουσία κρυπτογράφησης		Κρυπτογράφηση, ασφαλή πρωτόκολλα, ψηφιακή υπογραφή μεταδιδόμενων δεδομένων, **real-time deepfake detection**
4. Database (local or third party)	SQL Injections, NoSQL injections, Template attacks, DoS, Malware, κλοπή προτύπων, **Data Poisoning, Model Inversion, Transferability of Attacks**	Μη ασφαλής αποθήκευση, προεπιλεγμένοι λογαριασμοί, υπερβολικά δικαιώματα, μη κρυπτογραφημένα backups, **πιθανότητα διαρροής ή αλλοίωσης δεδομένων εκπαίδευσης**		Κρυπτογράφηση δεδομένων/αντιγράφων, ακυρώσιμα βιομετρικά, IDS, πολιτικές ελέγχου πρόσβασης, MVC αρχιτεκτονική, τακτικός έλεγχος δικαιωμάτων **παρακολούθηση datasets, έλεγχος πρόσβασης στα δεδομένα εκπαίδευσης**

Κεφάλαιο Ε: Συμπεράσματα

Η παρούσα εργασία εξέτασε τη σχέση μεταξύ των βιομετρικών συστημάτων αυθεντικοποίησης και της τεχνητής νοημοσύνης, εστιάζοντας στα οφέλη και στις προκλήσεις που προκύπτουν στην ασφάλεια. Τα βιομετρικά συστήματα, αν και προσφέρουν υψηλό επίπεδο ασφάλειας σε σύγκριση με τις παραδοσιακές μεθόδους ταυτοποίησης, δεν είναι απροσπέλαστα. Οι κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν τις ευπάθειες τους, θέτοντας σε κίνδυνο τους χρήστες που τα χρησιμοποιούν. Η επιρροή όμως της τεχνητής νοημοσύνης είναι σημαντική και ως μέσω για την ενίσχυση της ασφάλειας και ως ‘όπλο’ στα χέρια των κακόβουλων χρηστών.

Η τεχνητή νοημοσύνη, ενισχύει την ασφάλεια των βιομετρικών συστημάτων μέσω τεχνικών όπως η ανίχνευση ζωντανότητας (liveness detection) και η βελτίωση των αλγορίθμων αναγνώρισης. Μέτρα που αν εφαρμοστούν μπορούν να ενισχύουν σημαντικά την ασφάλεια και να αποτρέψουν πιθανές επιθέσεις.

Από την άλλη πλευρά όμως, η τεχνητή νοημοσύνη, μπορεί να χρησιμοποιηθεί για τη δημιουργία πλαστών βιομετρικών δεδομένων, όπως deepfakes, που καθιστούν τα συστήματα πιο ευάλωτα. Αυτά τα πλαστά βιομετρικά μέσα, χρησιμοποιούνται για την προσπέλαση των βιομετρικών συστημάτων, προκαλώντας πολύ σοβαρές συνέπειες τόσο στους απλούς χρήστες όσο και σε πολλούς οργανισμούς.

Για να διασφαλιστεί η αξιοπιστία των βιομετρικών συστημάτων, είναι απαραίτητη η εφαρμογή πολυστρωματικών μέτρων ασφαλείας. Αυτά περιλαμβάνουν την κρυπτογράφηση των δεδομένων, τη χρήση πολυπαραγοντικής ταυτοποίησης, την τακτική ενημέρωση του λογισμικού και την εκπαίδευση των χρηστών. Επιπλέον, η ανάπτυξη νέων τεχνολογιών, όπως τα ακυρώσιμα βιομετρικά (cancelable biometrics) και οι προηγμένοι αισθητήρες με δυνατότητες ανίχνευσης ζωντανότητας, αποτελεί κρίσιμο βήμα για την αντιμετώπιση των εκλεπτυσμένων απειλών.

Συνοψίζοντας, η συνύπαρξη βιομετρικών συστημάτων και τεχνητής νοημοσύνης δημιουργεί τόσο οφέλη όσο και προκλήσεις όσον αφορά την ασφάλεια. Η μελλοντική έρευνα και ανάπτυξη θα πρέπει να εστιάσει στην εξισορρόπηση αυτών των δύο πλευρών, ώστε να εξασφαλιστεί η ασφάλεια και η ιδιωτικότητα των χρηστών, διατηρώντας παράλληλα την ευκολία χρήσης και την αποτελεσματικότητα των συστημάτων. Μόνο μέσα από μια ολοκληρωμένη προσέγγιση μπορεί να επιτευχθεί μια ασφαλής και βιώσιμη εφαρμογή των βιομετρικών τεχνολογιών στον ψηφιακό κόσμο.

Βιβλιογραφία

1. Alrawili, Reem, et al. “Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion.” *Computers and Electrical Engineering*, vol. 119, Oct. 2024, p. 109485.

2. Boodoo-Jahangeer, Nazmeen, and Sunilduth Baichoo. *Choice of Biometrics*. 2014.

3. Hemalatha, S. “A Systematic Review on Fingerprint Based Biometric Authentication System.” *2020 International Conference on Emerging Trends in Information Technology and Engineering (Ic-ETITE)*, vol. 975, Feb. 2020, pp. 1–4, https://doi.org/10.1109/ic-etite47903.2020.342. Accessed 24 Oct. 2024.

4. Kodituwakku, S. “Biometric Authentication: A Review.” *International Journal of Trend in Research and Development*, vol. 2, no. 4. Accessed 26 Oct. 2024.

5. Yuan, Wang, et al. “A Real Time Fingerprint Recognition System Based on Novel Fingerprint Matching Strategy.” IEEE Xplore, 1 Aug. 2007, ieeexplore.ieee.org/abstract/document/4350576/. Accessed 16 Oct. 2022.

6. Kumari, Yachna, and Mrs.Rohini Sharma. “Iris Recognition System Using Gabor Filter & Edge Detection”

7. Meghana, K., et al. “Retina Based Biometric Recognition System.” *SSRN Electronic Journal*, 2020, https://doi.org/10.2139/ssrn.3919343. Accessed 22 Aug. 2022.

8. Kortli, Yassin, et al. “Face Recognition Systems: A Survey.” *Sensors*, vol. 20, no. 2, 7 Jan. 2020, p. 342, https://doi.org/10.3390/s20020342.

9. Tolba, A. S., et al. *Face Recognition: A Literature Review*.

10. Meena, Divya, and Ravi Sharan. “An Approach to Face Detection and Recognition.” *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, Dec. 2016, https://doi.org/10.1109/icraie.2016.7939462. Accessed 26 Apr. 2022.

11. Sidlauskas, David P, and Samir M Tamer. “Hand Geometry Recognition.” *Springer EBooks*, 1 Jan. 2008, pp. 91–107, https://doi.org/10.1007/978-0-387-71041-9_5.

12. Sanchez-Reillo, R., et al. “Biometric Identification through Hand Geometry Measurements.” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, 2000, pp. 1168–1171, https://doi.org/10.1109/34.879796. Accessed 9 Dec. 2020.

13. Nguyen, Kien, et al. “Long Range Iris Recognition: A Survey.” *Pattern Recognition*, vol. 72, Dec. 2017, pp. 123–143, https://doi.org/10.1016/j.patcog.2017.05.021.

14. Taha, Mohammed A, and Hanaa M Ahmed. “A Brief Survey on Modern Iris Feature Extraction Methods.” *Engineering and Technology Journal*, vol. 39, no. 1part(A) Engineering, 2021, www.iasj.net/iasj/article/218303.

15. Patwari, Manjiri B, et al. *Personal Identification Algorithm Based on Retinal Blood Vessels Bifurcation*. 1 Mar. 2014, https://doi.org/10.1109/icica.2014.51. Accessed 6 Nov. 2023.

16. Varchol, Peter, et al. *Using of Hand Geometry in Biometric Security Systems*.

17. Qinghan Xiao. “Security Issues in Biometric Authentication.” *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005.*, 2020, ieeexplore.ieee.org/abstract/document/1495927, https://doi.org/10.1109/iaw.2005.1495927. Accessed 12 Jan. 2020.

18. Abdullayeva, Fargana, et al. *ANALYSIS of SECURITY VULNERABILITIES in BIOMETRIC SYSTEMS*.

19. Sabaghi, Arian, et al. “Deep Learning Meets Liveness Detection: Recent Advancements and Challenges.” *ArXiv:2112.14796 [Cs]*, 29 Dec. 2021, arxiv.org/abs/2112.14796.

20. Minaee, Shervin, et al. “Biometrics Recognition Using Deep Learning: A Survey.” *Artificial Intelligence Review*, 13 Jan. 2023, https://doi.org/10.1007/s10462-022-10237-x.

21. Mousa, Abdulazeez, et al. “Database Security Threats and Challenges.” *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, June 2020, https://doi.org/10.1109/isdfs49300.2020.9116436. Accessed 15 Aug. 2020.

22. Kietzmann, Jan, et al. “Deepfakes: Trick or Treat?” *Business Horizons*, vol. 63, no. 2, Mar. 2020, pp. 135–146, www.sciencedirect.com/science/article/pii/S0007681319301600, https://doi.org/10.1016/j.bushor.2019.11.006.

23. Naveen Singh, Dilip Gandhi & Krishna Pal Singh, “Iris Recognition System Using ACanny Edge Detection and a Circular Hough Transform”, International Journal of Advances in Engineering & Technology, Volume 1, Issue 2, Pages 221- 228, May 2011

24. https://www.bleepingcomputer.com/news/security/new-gold-pickaxe-android-ios-malware-steals-your-face-for-fraud/

25. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

26. Milkias Ghilom, and Shahram Latifi. “The Role of Machine Learning in Advanced Biometric Systems.” *Electronics*, vol. 13, no. 13, 7 July 2024, pp. 2667–2667, www.mdpi.com/2079-9292/13/13/2667, https://doi.org/10.3390/electronics13132667.