ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΕΞΕΙΔΙΚΕΥΣΗ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ (CYBERSECURITY)»

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Βιομετρική και Κυβερνοασφάλεια

Γεωργίου Κωνσταντίνα – cscyb2006

Επιβλέπων: Δρ. Κωνσταντίνος Ι. Μαυρομμάτης, Καθηγητής ΠΜΣ

ΑΙΓΑΛΕΩ, 2023

Πανεπιστήμιο Δυτικής Αττικής, Τμήμα Μηχανικών Πληροφορικής Και Υπολογιστών
Γεωργίου Κωνσταντίνα

Δήλωση συγγραφέα μεταπτυχιακής εργασίας

Η κάτωθι υπογεγραμμένη Κωνσταντίνα Γεωργίου φοιτήτρια του προγράμματος μεταπτυχιακών σπουδών «κυβερνοασφάλεια» του Τμήματος μηχανικών πληροφορικής και υπολογιστών της σχολής μηχανικών του πανεπιστημίου Δυτικής Αττικής δηλώνω ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποίαν είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης οι πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών η λέξεων είτε ακριβώς είτε παραφρασμένες αναφέρονται στο σύνολό τους με πλήρη αναφορά στους συγγραφείς, στον εκδοτικό οίκο ή το περιοδικό συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.

Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από εμένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου όσο και του Ιδρύματος. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.»

Η δηλούσα

Κωνσταντίνα Γεωργίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ «ΕΞΕΙΔΙΚΕΥΣΗ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ (CYBERSECURITY)»

Θέμα

Βιομετρική τεχνολογία και Κυβερνοασφάλεια

Κωνσταντίνα Γεωργίου

A.M: cscyb2006

Εισηγητής: Κωνσταντίνος Μαυρομμάτης

Εξεταστική Επιτροπή:

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/Α	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	ΙΔΙΟΤΗΤΑ ΒΑΘΜΙΔΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	Κωνσταντίνος Μαυρομμάτης	Επιβλέπων Καθηγητής Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, Πανεπιστήμιο Δυτικής Αττικής	Konstantinos Mavrommatis Digitally signed by Konstantinos Mavrommatis Date: 2023.07.28 09:54:25 +03'00'
2	Παναγιώτης Γιαννακόπουλος	Καθηγητής Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, Πανεπιστήμιο Δυτικής Αττικής	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.08.21 13:12:51 +03'00'
3	Εμμανουήλ Μιχαηλίδης	Ακαδημαϊκός Υπότροφος Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών, Πανεπιστήμιο Δυτικής Αττικής	Emmanouil Michailidis Digitally signed by Emmanouil Michailidis Date: 2023.07.28 10:07:46 +03'00'

Ημερομηνία εξέτασης: 21/01/2023

Η έγκριση της πτυχιακής εργασίας δεν υποδηλοί την αποδοχή των γνωμών του συγγραφέα. Κατά τη συγγραφή τηρήθηκαν οι αρχές της ακαδημαϊκής δεοντολογίας.

ΠΕΡΙΛΗΨΗ

Βιομετρική και Κυβερνοασφάλεια

Γεωργίου Κωνσταντίνα

Με τις νέες τεχνολογικές εξελίξεις έρχονται παράλληλα νέες αδυναμίες και προκλήσεις, καθιστώντας την ασφάλεια στον κυβερνοχώρο πλέον πρωταρχικό μέλημα. Μαζί με αυτές τις εξελίξεις, αξιοσημείωτο είναι ότι και οι χάκερ εξελίσσονται και συνεχίζουν να αποτελούν απειλή για τον κυβερνοχώρο. Λόγω των συμβατικών μεθόδων ασφάλειας, όπως οι κωδικοί πρόσβασης, που αποδεδειγμένα είναι αναποτελεσματικές, η ασφάλεια με χρήση βιομετρικής τεχνολογίας υιοθετείται μεταξύ πολλών οργανισμών και ιδιωτών ως ο προτιμώμενος τρόπος για την προστασία του κυβερνοχώρου τους από πιθανές απειλές. Τεχνολογίες όπως η αναγνώριση προσώπου και η σάρωση δακτυλικών αποτυπωμάτων έχουν γίνει δημοφιλείς.

Κάθε μέρα φαίνεται ότι υπάρχουν περισσότερες αναφορές για παραβιάσεις δεδομένων, τόσο σε μεγάλους όσο και σε μικρούς οργανισμούς. Καθώς αυτά τα γεγονότα συνεχίζουν να εκτυλίσσονται, οι οργανισμοί συνειδητοποιούν ότι πρέπει να λάβουν γρήγορα νέα μέτρα ασφαλείας. Οι εταιρείες απομακρύνονται πλέον από τους κωδικούς πρόσβασης και αναζητούν λύσεις βιομετρικής επαλήθευσης ταυτότητας, χωρίς να αναλογίζονται όλες τις συνέπειες. Αν και υπάρχουν σίγουρα οφέλη στα βιομετρικά στοιχεία, είναι σημαντικό να μελετηθεί κάθε πιθανότητα.

Η διάρθωση της παρούσας εργασίας ακολουθεί την εξής δομή: Στο πρώτο κεφάλαιο γίνεται εισαγωγή στο πρόβλημα της αναγνώρισης ταυτότητας και πιστοποίησης χρήστη, αναφερόμενοι σε πολλαπλές περιπτώσεις χρήσης όπου εφαρμόζεται. Στο δεύτερο κεφάλαιο μελετάται η κυβερνοασφάλεια κάνοντας σε μια ιστορική αναδρομή σε αυτή, σε σημαντικές επιθέσεις που εκπονήθηκαν τα τελευταία χρόνια, αλλά και πιθανές λύσεις, όπως μέθοδοι ελέγχου ταυτότητας/ εξουσιοδότηση, κρυπτογραφία, στεγανογραφία, τείχη προστασίας κλπ. Στο τρίτο κεφάλαιο γίνεται ανάλυση του ορισμού της βιομετρίας και της τεχνολογίας που την απαρτίζει, καθώς και αναφορά σε σημαντικά βιομετρικά συστήματα, με βάση χαρακτηριστικά (βιομετρικά ή μη) του χρήστη. Αξιοσημείωτες είναι και οι προκλήσεις που έχουν να αντιμετωπίσουν τα βιομτερικά συστήματα, από κακόβουλους χρήστες, όπως πλαστογραφία κλπ. Στα κεφάλαια 4 και

5 αναφέρεται η συνεισφορά της τεχνητής νοημοσύνης και μηχανικής μάθησης στην κυβερνοασφάλεια, μέσω αλγορίθμων νευρωνικών δικτύων, μηχανών διανυσμάτων υποστήριξης κλπ. Σημαντική είναι και η μελέτη περιπτώσεων χρήσης και εφαρμογών της τεχνητής νοημοσύνης σε συνδυασμό με τη χρήση βιομετρικής τεχνολογίας σε πολλές εταιρείες. Τέλος, στο έκτο κεφάλαιο παρέχονται τελικά συμπεράσματα που εξάγονται από τη συνολική μελέτη διεθνούς βιβλιογραφίας, καθώς και προβληματισμοί που αναδύονται με τη χρήση της βιομετρικής τεχνολογίας αναφορικά με τους κανόνες προστασίας γενικών δεδομένων (GDPR).

Λέξεις κλειδιά

βιομετρία, κυβερνοασφάλεια, πιστοποίηση, έλεγχος ταυτότητας, επιθέσεις ασφαλείας

ABSTRACT

Biometrics and Cyber Security

Georgiou Konstantina

With new technological developments come new weaknesses and challenges, making cyber security a top priority. Along with these developments, it is noteworthy that hackers are also evolving and continue to pose a threat to cyberspace. Because of conventional security methods, such as passwords, which have been shown to be ineffective, security using biometric technology has been adopted by many organizations and individuals as the preferred way to protect their cyberspace from potential threats. Technologies such as face recognition and fingerprint scanning have become popular.

Every day there seem to be more reports of data breaches, both in large and small organizations. As these events continue to unfold, organizations are realizing that they need to take new security measures quickly. Companies are now moving away from passwords and looking for biometric authentication solutions, without considering all the consequences. While there are definitely benefits to biometrics, it is important to consider every possibility.

The structure of this work follows the following pattern: The first chapter introduces the problem of user identification and authentication, referring to multiple use cases where it applies. In the second chapter, cybersecurity is studied by making a historical review of it, in important attacks that have been prepared in recent years, but also possible solutions, such as methods of authentication / authorization, cryptography, sealing, firewalls, etc. In the third chapter, the definition of biometrics is analyzed and the technology that builds it up, as well as reference is made to important biometric systems, based on characteristics (biometric or not) of the user. Remarkable are the challenges that biometric systems have to face, from malicious users, such as counterfeiting, etc. Chapters 4 and 5 mention the contribution of artificial intelligence and machine learning to cybersecurity, through neural network algorithms, support vector machines, etc. and are studied the use cases and applications of artificial intelligence in combination with the use of biometric technology in many companies. Finally, the sixth chapter provides final conclusions

drawn from the overall study of international literature, as well as concerns that arise with the use of biometric technology regarding the rules of general data protection (GDPR).

Key words

biometrics, cybersecurity, certification, authentication, security attacks

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ ΚΑΙ ΕΙΚΟΝΩΝ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Η παρούσα εργασία αφιερώνεται στην οικογένειά μου, που με στήριξαν σε όλο αυτό το διάστημα.

1. ΕΙΣΑΓΩΓΗ ΣΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΝΑΓΝΩΡΙΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ

Σήμερα, ο κόσμος ζει σε μια πιο μικρή πραγματικότητα. Τα άτομα έχουν υψηλή κινητικότητα, είναι διαρκώς συνδεδεμένα μεταξύ τους και η καθημερινή τους ζωή επηρεάζεται σε μεγάλο βαθμό από τις τεχνολογίες της πληροφορίας, ιδίως τις κινητές συσκευές και την κοινωνική δικτύωση. Σε τέτοιες κοινωνίες, οι περισσότερες από τις υπηρεσίες παρέχονται ηλεκτρονικά μέσω έξυπνων συσκευών που είναι προσβάσιμες εξ' αποστάσεως. Αυτές οι υπηρεσίες μπορεί να είναι τραπεζικές υπηρεσίες, ηλεκτρονικό εμπόριο, κρατικές υπηρεσίες προς τους πολίτες, κρατήσεις ξενοδοχείων, κοινωνικοί βοηθοί και πολλοί άλλοι τομείς που σχετίζονται με την εργασία, τα ταξίδια, την άμυνα, την εκπαίδευση, τις επιχειρήσεις και τις κοινωνικές σχέσεις.

1.1 ΤΟ ΠΡΟΒΛΗΜΑ ΤΗΣ ΑΝΑΓΝΩΡΙΣΗΣ

Οι υπηρεσίες είναι πλέον πολύ πιο εύκολες και πιο άμεσες. Η κατανάλωση των υπηρεσιών βασίζεται γενικά στο μοντέλο πελάτη-διακομιστή όπου το μηχάνημα είναι ο διακομιστής και ο πελάτης είναι ο μεμονωμένος χρήστης. Η ασφάλεια τέτοιων συστημάτων πρέπει να λαμβάνεται ιδιαίτερα υπόψη, καθώς η υπηρεσία πρέπει να παρέχεται μόνο στο νόμιμο χρήστη που αρχικά πρέπει να αναγνωριστεί. Παραδοσιακά, αυτά τα συστήματα χρησιμοποιούσαν, και εξακολουθούν να χρησιμοποιούν, κλασικές πολιτικές ελέγχου ταυτότητας που βασίζονται σε διαπιστευτήρια π.χ. μυστικές πληροφορίες (όπως κωδικούς πρόσβασης) ή/και ιδιωτικά διακριτικά (πιστοποιητικά, έξυπνες κάρτες). Δυστυχώς, τέτοια συστήματα δεν είναι αρκετά ασφαλή, καθώς τα διαπιστευτήρια μπορούν να ξεχαστούν, να κλαπούν ή να αντιγραφούν. Στην πραγματικότητα, οι σοβαρές ανησυχίες αφορούσαν την ασφάλεια τέτοιων συστημάτων, καθώς κακόβουλα άτομα έχουν εκμεταλλευτεί την ευπάθειά τους, για να αποκτήσουν παράνομη πρόσβαση σε προνομιακά δικαιώματα. Αυτά τα περιστατικά απάτης είναι περιορισμένης κλίμακας σε χώρες όπως η Αλγερία όπου οι ηλεκτρονικές υπηρεσίες βρίσκονται στα πρώτα τους στάδια. Ωστόσο, αναφέρεται ότι πάνω από 17 εκατομμύρια άτομα στις ΗΠΑ ήταν θύματα ενός ή περισσότερων περιστατικών κλοπής ταυτότητας το 2014. Τα στατιστικά δείχνουν ότι οι κυβερνητικοί και μεγάλοι ιδιωτικοί οργανισμοί είναι οι πρώτοι στόχοι τέτοιων επιθέσεων. Ο αριθμός αυτών αυξάνεται χρόνο με τον χρόνο.

Τρεις είναι οι κύριοι λόγοι για την εμφάνιση τέτοιων αδυναμιών: i) ο χρήστης δεν προστάτεψε αρκετά τα διαπιστευτήριά του, ii) ο χάκερ εκμεταλλεύτηκε την απροσεξία του χρήστη

καθώς και ορισμένα ελαττώματα ασφαλείας στο σύστημα, και iii) η στρατηγική ασφαλείας που υιοθετείται από το σύστημα αναγνώρισης.

Φαίνεται ότι το σύστημα θα είναι υπεύθυνο για τις περισσότερες σχετικές αστοχίες ασφαλείας, καθώς πρέπει να λάβει υπόψη τις δύο πρώτες ελλείψεις. Στην πραγματικότητα, η στρατηγική αναγνώρισης που υιοθετείται δεν σχετίζεται με τον ίδιο τον χρήστη, αλλά βασίζεται σε αυτά που θα γνωρίζει ή σε αυτά που έχει στην κατοχή του. Αυτή είναι η κύρια πηγή ευπάθειας και τα επακόλουθα ζητήματα ασφάλειας.

Η διαπίστωση του προβλήματος αναγνώρισης δεν περιορίζεται μόνο στα συστήματα ηλεκτρονικών υπηρεσιών, αλλά συναντάται ιδιαίτερα σε ελεγχόμενες περιοχές όπως αεροδρόμια, ταξιδιωτικοί σταθμοί, κυβερνητικές και ιδιωτικές εγκαταστάσεις όπου τα άτομα θα πρέπει να ταυτοποιούνται με βάση ορισμένα δεδομένα που συλλέγονται. Το ζήτημα ανακύπτει έντονα σε ιατροδικαστικές εφαρμογές όπου τα πτώματα πρέπει να αναγνωρίζονται και να συλλέγονται αποδείξεις εγκληματικότητας. Είναι πολύ σαφές ότι τα κλασικά συστήματα αναγνώρισης δεν είναι χρήσιμα σε τέτοιες καταστάσεις.

Σε κάθε περίπτωση, οι κυβερνήσεις, οι ιδιωτικοί οργανισμοί καθώς και τα άτομα έχουν σοβαρές ανησυχίες για την αύξηση των απατών ταυτότητας. Οι ισχυρότεροι μηχανισμοί αναγνώρισης είναι η κύρια προτεραιότητά τους, [4].

2. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΗΜΕΡΑ

Είναι η εποχή της πληροφορίας· σχεδόν όλα είναι ψηφιοποιημένα και συνδεδεμένα, χάρη στο διαδίκτυο. Αυτό που χρειαζόταν ώρες πριν από μερικές δεκαετίες τώρα διαρκεί δευτερόλεπτα, αυτό που θεωρούνταν απλή επιστημονική φαντασία είναι τώρα πραγματικότητα και τα περισσότερα από αυτά που ήταν αδύνατο είναι τώρα δυνατά.

Η μαζική χρήση διαδικτύου και ηλεκτρονικών συσκευών απαιτεί και εξαρτάται σε μεγάλο βαθμό από την ασφάλεια και την ιδιωτικότητα καθώς οι άνθρωποι γίνονται πιο ενεργοί στον κόσμο του κυβερνοχώρου, μοιράζοντας μαζικές πληροφορίες ειδικά μέσω των κοινωνικών δικτύων που είναι ο νεότερος τύπος εθισμού χωρίς τον οποίο οι άνθρωποι δεν μπορούν να ζήσουν · η ιδιωτικότητα απειλείται.

Οι απλοί χρήστες πιστεύουν ότι το Διαδίκτυο είναι ασφαλές και ότι είναι απαλλαγμένοι από απειλές και δεν στοχοποιούνται από τους επιτιθέμενους, ωστόσο η αλήθεια είναι ότι αυτό δεν είναι παρά μια ψευδαίσθηση. Η κυβερνοασφάλεια απειλείται καθημερινά, τουλάχιστον ένα εκατομμύριο νέοι ιοί και κακόβουλα λογισμικά δημιουργούνται καθημερινά και περισσότερες από 100.000 επιθέσεις εξαπολύονται στον κυβερνοχώρο κάθε ώρα και κοστίζουν πάνω από 100 δισεκατομμύρια δολάρια ετησίως.

Σύμφωνα με τον Benarous [12], η διασφάλιση της ασφάλειας είναι υποχρεωτική και είναι μάλλον μια δύσκολη εργασία για πολλούς λόγους:

- Πρώτον, ο μεγάλος αριθμός των νέων κακόβουλων προγραμμάτων που κυκλοφορούν καθημερινά δυσκολεύει την παρακολούθησή τους. Επιπλέον, οι νέοι ιοί βασίζονται σε καινούριες τεχνικές για να αποφευχθεί ο εντοπισμός, όπως η αυτόματη αλλαγή κώδικα σε κάθε μόλυνση ή η χρήση της κρυπτογραφίας.
- Δεύτερον, οι επιθέσεις μπορεί να προέρχονται από το εσωτερικό των δικτύων καθιστώντας τες πιο αποτελεσματικές καθώς ο εισβολέας μπορεί να έχει υψηλότερα δικαιώματα πρόσβασης.
- Τρίτον, ο επιτιθέμενος είναι άγνωστος (το επίπεδο, οι τεχνικές και τα κίνητρά του).

- Τέλος, οι επιθέσεις και τα κακόβουλα προγράμματα εκμεταλλεύονται τα τρωτά σημεία του συστήματος και του λογισμικού, τα οποία μπορεί να περιλαμβάνουν και τα τρωτά σημεία του ίδιου του συστήματος ασφαλείας.

Ανεξάρτητα από όλες τις προκλήσεις που αναφέρθηκαν προηγουμένως, οι φορείς ασφαλείας συνεχίζουν να αναπτύσσουν νέες τεχνικές και να αναζητούν νέες λύσεις για να διατηρήσουν τα δίκτυα, τα συστήματα και τα δεδομένα ασφαλή.

Ο κύριος στόχος αυτού του κεφαλαίου είναι να ερευνήσει την ασφάλεια του κυβερνοχώρου και την εξέλιξή του καθώς αναπτύσσονται οι τεχνολογίες δικτύων, συστημάτων και ομαδοποίησης δεδομένων. Το κεφάλαιο περιλαμβάνει μια ιστορική επισκόπηση, τους στόχους ασφαλείας, τα ζητήματα και την ταξινόμησή τους.

2.1 Ο ΚΥΒΕΡΝΟΚΟΣΜΟΣ

Ο κυβερνόκοσμος και ο εικονικός κόσμος είναι λέξεις που αναφέρονται στο διαδίκτυο. Ο απλοποιημένος ορισμός του Διαδικτύου θα ήταν: "ένα σύνολο υπολογιστών ή μηχανών που συνδέονται με μεγάλους διακομιστές που παρέχουν διαφορετικές υπηρεσίες για χρήση τους από τα μηχανήματα". Αυτός δεν είναι ο τεχνικός ορισμός, μάλλον είναι ένας εύκολος τρόπος να οριστεί η έννοια και η τεχνολογία.

Οι άνθρωποι αποτελούν χρήστες των μηχανημάτων όπως ένας υπολογιστής, smartphone, tablet, smart TV ή οποιαδήποτε άλλη συσκευή μπορεί να μας συνδέσει στο διαδίκτυο. Οι υπηρεσίες είναι οι ιστότοποι που χρησιμοποιούν, όπως τα κοινωνικά μέσα (Facebook, twitter, YouTube, κ.λπ.), ιστότοποι αλληλογραφίας (Yahoo, Gmail, Hotmail, κ.λπ.), ιστότοποι ηλεκτρονικού εμπορίου (eBay, PayPal, Alibaba, Amazon, κ.λπ.) ή οποιοιδήποτε άλλοι ιστότοποι που χρησιμοποιούν συχνά.

Ο διακομιστής για έναν απλό χρήστη δικτύου δεν είναι παρά ένα μαύρο κουτί και είναι αόρατος, το μόνο που είναι ξεκάθαρο για έναν απλό χρήστη είναι ότι επικοινωνεί με έναν πάροχο υπηρεσιών Διαδικτύου, πληρώνει έναν λογαριασμό και συνδέεται με τον κυβερνοχώρο και απολαμβάνει τις υπηρεσίες του, [12].

2.2 ΤΟ ΣΚΟΤΕΙΝΟ ΔΙΚΤΥΟ (DARKNET) Η ΒΑΘΥ ΔΙΑΔΙΚΤΥΟ (DEEP INTERNET)

Το Διαδίκτυο, όπως ορίζεται στην προηγούμενη υποενότητα, είναι αυτό που γνωρίζουν οι περισσότεροι χρήστες, αλλά υπάρχουν και άλλοι όροι όπως το Σκοτεινό Δίκτυο (Darknet) ή το

Βαθύ Διαδίκτυο (Deep Internet). Πρόκειται ένα μέρος του διαδικτύου που είναι προσβάσιμο μέσω ειδικών εργαλείων όπως το Tor ή το Riffle από το MIT, και περιέχει ιστότοπους στους οποίους δεν είναι δυνατή η απευθείας πρόσβαση από κανονικές μηχανές αναζήτησης όπως η Google. Ένας από τους ορισμούς του darknet είναι: "μια κατηγορία δικτύων που στοχεύουν να εγγυηθούν την ανώνυμη και μη ανιχνεύσιμη πρόσβαση σε περιεχόμενο ιστού και την ανωνυμία για έναν ιστότοπο". Αυτή η σκοτεινή πλευρά του διαδικτύου χρησιμοποιείται από χάκερ και επικίνδυνους εγκληματίες επειδή διασφαλίζει το μη εντοπισμό.

Παρόλο που τα εγκλήματα στον κυβερνοχώρο συμβαίνουν τόσο στο clearnet όσο και στο darknet, τα εγκλήματα του darknet δεν εμπίπτουν στο πεδίο αυτού του κεφαλαίου, αλλά αντίθετα εστιάζεται περισσότερο στις απειλές ασφάλειας για το clearnet, τα συστήματα και τις πληροφορίες, [12].

2.3 ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ

Αυτή η ενότητα περιλαμβάνει ορισμένες συχνά χρησιμοποιούμενες διαδικτυακές υπηρεσίες που κάνουν τους ανθρώπους τόσο εξαρτημένους από το διαδίκτυο και με όλα τα στοιχεία του και που θέτουν σε κίνδυνο την ιδιωτικότητα. Σύμφωνα με τους συγγραφείς, [12], [16], οι υπηρεσίες διαδικτύου που χρησιμοποιούνται περισσότερο ομαδοποιούνται ανά κατηγορία από την κατάταξη των ιστοτόπων από την Alexa:

- Μηχανές αναζήτησης και υπηρεσίες αλληλογραφίας, όπως Google, Yahoo και MSN.
- Δίκτυα μέσων κοινωνικής δικτύωσης· περιλαμβάνουν ιστότοπους κοινής χρήσης βίντεο (YouTube και Daily motion), διαδικτυακή τηλεόραση, κοινωνικές υπηρεσίες (Facebook, Twitter, Instagram, Weibo κ.λπ.) και ιστότοπους ιστολογίων (Tumbler, Blogger κ.λπ.).
- Υπηρεσίες ηλεκτρονικού εμπορίου: όλοι οι ιστότοποι που επιτρέπουν συναλλαγές ή δημιουργία επιχειρηματικών, τραπεζικών ή ιστότοποι απλώς αγοραπωλησιών όπως οι Alibaba, Amazon, eBay, PayPal.
- Ηλεκτρονική μάθηση: περιλαμβάνει ιστότοπους που χρησιμοποιούνται για μάθηση περιέχοντας διαλέξεις, διαδικτυακά σεμινάρια ή εκπαιδευτικό περιεχόμενο, επίσης εγκυκλοπαίδειες όπως η Wikipedia, forum ερωτήσεων / απαντήσεων όπως το Stack

OverFlow ή το Ask, και περιλαμβάνει επίσης επιστημονικά περιοδικά και ακαδημαϊκούς ιστότοπους.

- Ειδήσεις και ψυχαγωγία: μερικά παραδείγματα αποτελούν τα περιοδικά, η υγεία, τα αθλήματα, οι χάρτες και οι υπηρεσίες καιρού.
- Υπηρεσίες σύννεφου, αποθήκευσης και κοινής χρήσης αρχείων: περιλαμβάνουν το Google Drive, το dropbox, το media fire κ.λπ.
- Gaming: διαδικτυακοί ιστότοποι παιχνιδιών όπως το Twitch, το Battle κ.λπ.
- Διαφήμιση: όπως οι διαφημίσεις με ένα click (on click ads).
- Ιστότοποι προσώπων / οργανισμών: ιστότοποι εταιρειών και μεμονωμένων ατόμων.
- Βιομηχανική παρακολούθηση και έλεγχος, που περιλαμβάνουν υπηρεσίες απομακρυσμένης πρόσβασης· έλεγχο και παρακολούθηση βιομηχανικού εξοπλισμού κάνουν τα ρομπότ.

2.4 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Οι ιστορικοί πιστεύουν ότι τα θέματα ασφάλειας εμφανίστηκαν ήδη από τη δεκαετία του 1960. Ωστόσο, θεωρητικά εμφανίστηκε πολύ νωρίτερα, πιο συγκεκριμένα το 1949 όταν ο μαθηματικός John von Neumann όρισε τον ιό και το σκουλήκι ως αυτοαναπαραγόμενα αυτόματα.

Παρόλο που η θεωρητική ιδέα υπήρχε εδώ και πολύ καιρό, τονίστηκε η σημασία της κυβερνοασφάλειας μόνο μετά τις επιτυχείς επιθέσεις ασφαλείας. Οι επιθέσεις κόστισαν περιουσίες, αποκάλυψαν μυστικά και έθεσαν σε κίνδυνο ζωές.

Οι ιστορικοί παρατήρησαν ότι οι ανησυχίες για την κυβερνοασφάλεια ακολούθησαν διαφορετικές τάσεις μέσα στις δεκαετίες και ότι επηρεάστηκε από πολιτικά και κοινωνιολογικά γεγονότα. Για παράδειγμα, κατά τη διάρκεια της δεκαετίας του 1980, η ανησυχία για την ασφάλεια στο κυβερνοχώρο ήταν η ξένη κατασκοπεία. Κατά τη διάρκεια της δεκαετίας του 1990, η απειλή κατευθύνθηκε προς μη στρατιωτικές υποδομές ζωτικής σημασίας και αργότερα, οι όροι κυβερνοτρομοκρατία, οργανωμένο έγκλημα και hacking χρησιμοποιήθηκαν για να περιγράψουν τις επιθέσεις.

Σύμφωνα με τους συγγραφείς, [12], [17], με βάση τη χρονολογική τους σειρά, τα κύρια ζητήματα ασφάλειας που συνέβησαν τις τελευταίες πέντε δεκαετίες μπορούν να περιγραφούν ως εξής:

- Το 1964, η AT&T άρχισε να παρακολουθεί τους Phone Freaks, γνωστούς και ως Phreaks, οι οποίοι μπορούσαν να κάνουν δωρεάν τηλεφωνικές κλήσεις.
- Το 1968, δυνητικά η πρώτη στον κόσμο υπόθεση κατασκοπείας υπολογιστών πραγματοποιήθηκε από Γερμανό κατάσκοπο στη γερμανική θυγατρική της IBM.
- Το 1971, χάκερ κατασκεύασαν τον ιό σκουλήκι Creeper που μόλυνε το ARPANET.
- Το 1981 κατασκευάστηκε το Elk Cloner από τον 15χρονο Richard Skrenta.
- Το 1982, μια ομάδα εφήβων παραβίασε υπολογιστές υψηλού προφίλ στις ΗΠΑ· η επιχείρηση ονομάστηκε 414 s break-ins. Μια παρόμοια επιχείρηση με το όνομα Cuckoo's eggs έλαβε χώρα το 1986.
- Το 1988, κυκλοφόρησε το σκουλήκι Morris και το ARPANET κατέγραψε το πρώτο του σημαντικό πρόβλημα δικτύου.
- Το 1990 δημιουργήθηκαν οι πρώτοι αυτοτροποποιούμενοι ιοί.
- Το 1992, ο ιός Michelangelo κυκλοφόρησε αντικαθιστώντας τους πρώτους 100 τομείς του σκληρού δίσκου προκαλώντας αυτό που ονομάστηκε η πρώτη ψηφιακή μαζική υστερία.
- Το 1994, καταγράφηκαν δύο μεγάλες επιχειρήσεις hacking, το περιστατικό RomeLab και το περιστατικό της Citibank.
- Το 1995, δημιουργήθηκε ο πρώτος ιός που βασίζεται σε λέξεις της Microsoft.
- Το 1998 κυκλοφόρησε το Back Orifice για να παρέχει απομακρυσμένη διαχείριση συστήματος (Δούρειος Ίππος – Trojan Horse). Επίσης, καταγράφηκαν εκείνη τη χρονιά τα περιστατικά hacking των Solar Sunrise και Moonlight Maze.
- Το 1999, η Melissa εξαπλώθηκε μολύνοντας email.
- Το 2000, το I Love You εξαπλώθηκε στέλνοντας τον εαυτό του στα πρώτα πενήντα άτομα στο βιβλίο διευθύνσεων των windows. Την ίδια χρονιά, οι υπολογιστές του Πανεπιστημίου

της Καλιφόρνια χρησιμοποιήθηκαν από χάκερ για να συντρίψουν τις ιστοσελίδες των Amazon, eBay και Yahoo.

- Το 2001, τα σκουλήκια Code Red και Nimda χρησιμοποιήθηκαν για να αναλάβουν τον έλεγχο των υπολογιστών και να τους χρησιμοποιήσουν για επιθέσεις κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service – DdoS). Την ίδια χρονιά καταγράφηκε ο πρώτος παγκόσμιος πόλεμος στον κυβερνοχώρο που προκλήθηκε από μια σύγκρουση μεταξύ ΗΠΑ και Κίνας, όπου συμμετείχαν χάκερ από πολλές χώρες του κόσμου.
- Το 2003, οι Slammer και Blaster χρησιμοποιήθηκαν για να εξαπολύσουν επιθέσεις DDoS. Επίσης, ο Titan Rain είχε ως στόχο την πρόσβαση σε υπολογιστές υψηλού προφίλ στις ΗΠΑ.
- Το 2004, ο Sasser προκάλεσε την πτώση των συστημάτων και την επιβράδυνση του Διαδικτύου.
- Το 2007, ο Δίας χρησιμοποιήθηκε για να κλέψει τραπεζικές και άλλες πληροφορίες.
- Το 2008, το σκουλήκι Conficker χρησιμοποιήθηκε για τη δημιουργία botnets. Επίσης, ο ιός Koobface εξαπλώθηκε μέσω email ή υπηρεσιών μέσων κοινωνικής δικτύωσης όπως το Facebook, προκαλώντας ψεύτικες αγορές και συνεπώς κλοπή χρημάτων.
- Το 2009, έλαβαν χώρα τα περιστατικά GhostNet και Operation Aurora, εκ των οποίων το πρώτο ήταν για κυβερνοκατασκοπεία και το δεύτερο ήταν ενάντια στην Google και άλλες εταιρείες υψηλής τεχνολογίας, ώστε να έχει πρόσβαση και να τροποποιεί τους κωδικούς τους.
- Το 2010, το Stuxnet χρησιμοποιήθηκε για βιομηχανική κατασκοπεία και το WikiLeaks εξαπέλυσε μια επίθεση που ονομάζεται wikileaks cable gate όπου διέρρευσαν εμπιστευτικά διπλωματικά τηλεγραφήματα.
- Το 2011, ο Duqu κυκλοφόρησε (ένα τροποποιημένο αντίγραφο του Stuxnet) επίσης τον ιό Ramnit που κλέβει λογαριασμούς και κωδικούς πρόσβασης στο Facebook. Τη χρονιά αυτή καταγράφηκαν επιθέσεις hacking με μεγάλη δημοσιότητα, όπως: οι επιθέσεις κατά της Sony και άλλων εταιρειών, κατά κυβερνήσεων και η κλοπή δικαιωμάτων εκπομπής CO_2.

- Το 2013 και το 2014, έγιναν πολλές επιχειρήσεις hacking και οι περισσότερες επιθέσεις επικεντρώθηκαν στην κλοπή διαπιστευτηρίων Facebook και email.

2.5 ΣΤΟΧΟΙ ΑΣΦΑΛΕΙΑΣ

Οι στόχοι που παρουσιάζονται στην παρούσα ενότητα είναι οι απαιτήσεις των λύσεων ασφαλείας. Αρχικά, υπήρχαν τρεις αρχές: η διαθεσιμότητα, η εμπιστευτικότητα και η ακεραιότητα, αλλά προστέθηκαν και τρεις άλλες αρχές ως απαιτούμενες ανάγκες ασφάλειας που είναι η αυθεντικότητα, η μη απόρριψη και η δυνατότητα ελέγχου. Σύμφωνα με τους συγγραφείς, [12], [18], οι έξι στόχοι επεξηγούνται ακολούθως:

- Διαθεσιμότητα (availability): επιτρέπει στα εξουσιοδοτημένα μέρη να έχουν πρόσβαση στα συστήματα και τους απαιτούμενους πόρους δεδομένων, δηλαδή το σύστημα μπορεί πάντα να παρέχει τις υπηρεσίες του στον εξουσιοδοτημένο χρήστη που κάνει αίτημα και οι πόροι μπορούν να χρησιμοποιηθούν όταν χρειάζεται. Μία από τις πιο επικίνδυνες απειλές για τη διαθεσιμότητα είναι η επίθεση DoS που εμποδίζει τους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε ένα σύστημα (πόρος) και έτσι τους εμποδίζει να χρησιμοποιήσουν τις υπηρεσίες του.
- Εμπιστευτικότητα (ιδιωτικότητα - privacy): διασφαλίζει ότι ένα προσωπικό στοιχείο (προσωπικά δεδομένα ή πόρος) είναι προσβάσιμο μόνο από το εξουσιοδοτημένο πρόσωπο. Μία από τις σημαντικότερες απειλές για την ιδιωτικότητα είναι η έκθεση των δεδομένων.
- Ακεραιότητα (integrity): διασφαλίζει ότι τα δεδομένα τροποποιούνται μόνο από το εξουσιοδοτημένο άτομο. Αυτό σημαίνει ότι το περιεχόμενο είναι συνεπές και αυθεντικό και δεν έχει τροποποιηθεί από τρίτο μέρος.
- Αυθεντικότητα (authenticity): η ικανότητα ενός συστήματος να επιβεβαιώνει την ταυτότητα ενός αποστολέα όπου πρώτα αναγνωρίζεται και μετά εξουσιοδοτείται (ή του απαγορεύεται) να έχει πρόσβαση στο σύστημα.
- Μη άρνηση: διασφαλίζει ότι ο αποστολέας (δημιουργός του μηνύματος) δεν μπορεί να αρνηθεί την αποστολή του μηνύματος. Αυτή η αρχή προστέθηκε επειδή οι χρήστες θα αρνούνταν ότι έστειλαν το μήνυμα εάν διώκονταν νομικά, ειδικά σε περιπτώσεις όπου το

μήνυμα περιέχει παράνομο περιεχόμενο, απειλές ή στο ηλεκτρονικό εμπόριο την άρνηση αγοράς από τον χρήστη.

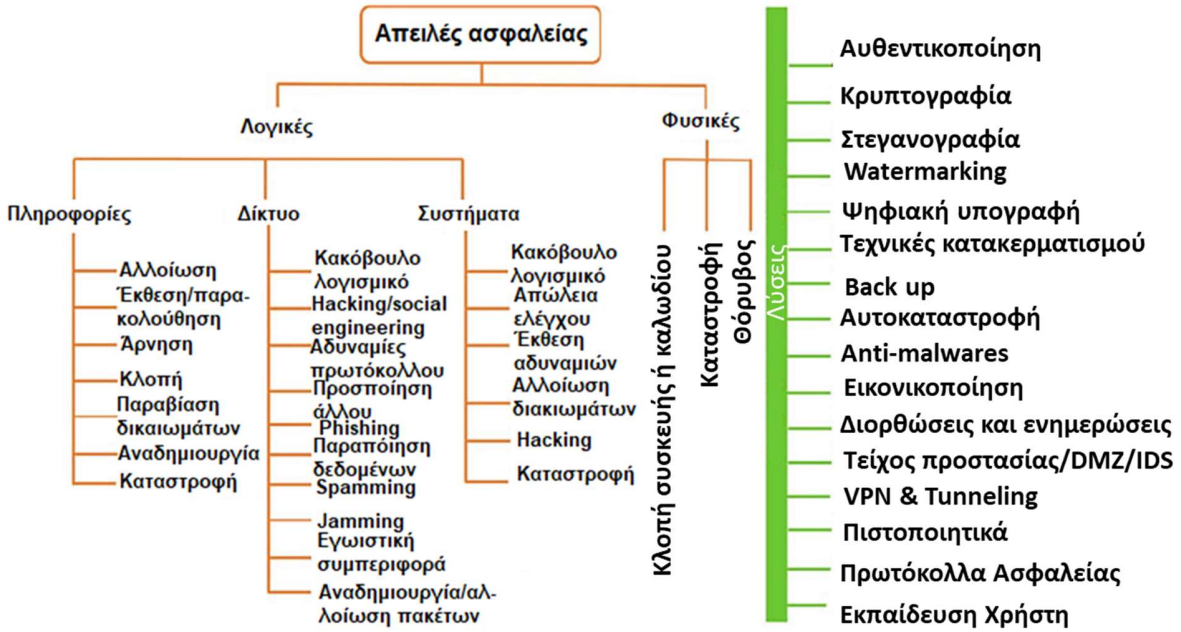
- Έλεγχος (auditability): προστέθηκε από το Υπουργείο Άμυνας των ΗΠΑ και είναι "η ικανότητα ενός συστήματος να ανιχνεύει όλες τις ενέργειες που σχετίζονται με ένα δεδομένο περιουσιακό στοιχείο". Το σύστημα καταγράφει όλα τα σημαντικά συμβάντα, όπως η αποστολή και η λήψη μηνυμάτων, οι διευθύνσεις IP και οποιεσδήποτε άλλες σχετικές πληροφορίες για τον εντοπισμό ζητημάτων ασφαλείας και σφαλμάτων, τον εντοπισμό των εισβολέων και την επίλυση και τεκμηρίωση των προβλημάτων.

2.6 ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ

Αφού αναδείχτηκε η εξάρτηση των ανθρώπων από τον κυβερνόκοσμο καθώς και η σημασία της ασφάλειας, αναφέροντας μερικές από τις κύριες απειλές ασφαλείας που έχουν καταγραφεί, αυτή σε αυτή την ενότητα ταξινομούνται απειλές ασφαλείας σε δύο κύριους τύπους: φυσικές και λογικές.

Οι φυσικές επιθέσεις απαιτούν τη φυσική παρουσία του εισβολέα και την άμεση αλληλεπίδρασή του / της με το σύστημα του δικτύου. Αυτό συνήθως έχει ως αποτέλεσμα την απώλεια της συσκευής ή του εξοπλισμού, την καταστροφή τους, τη δημιουργία θορύβου ή και παρεμβολές στα ασύρματα σήματα.

Από την άλλη πλευρά, οι λογικές απειλές μπορούν να διαχωριστούν σε τρεις κατηγορίες ανάλογα με τον στόχο της καθεμιάς: τις πληροφορίες, τα δίκτυα και τα συστήματα. Οι επιθέσεις στα δίκτυα απεικονίζονται στον παρακάτω πίνακα όπου παρουσιάζονται διαφορετικά είδη δικτύων (που βασίζονται σε υποδομές και ad hoc) μαζί με σημαντικές απειλές που σχετίζονται με κάθε τύπο. Το Σχήμα 1 παρουσιάζει τα προβλήματα που αναφέρθηκαν προηγουμένως και οι λύσεις τους που θα επεξηγηθούν περαιτέρω.



Σχήμα 1: Ταξινόμηση απειλών ασφαλείας.

Σύμφωνα με τους συγγραφείς, [12], [19], [20], [21], τα ακόλουθα περιγράφουν ορισμένες από τις επιθέσεις και τις απειλές ασφαλείας που αναφέρθηκαν προηγουμένως:

- Άρνηση υπηρεσίας (Denial of Service - DoS): είναι μια επίθεση που στοχεύει να καταλάβει ένα δίκτυο ή ένα μηχάνημα και να το εμποδίσει από το να παρέχει υπηρεσίες. Αυτό το είδος επίθεσης μπορεί να γίνει μέσω επιθέσεων πλημμύρας (flooding attacks) ή εκμετάλλευσης τεχνικών ευάλωτων σημείων ενός συστήματος ή ενός πρωτοκόλλου. Η επίθεση κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service - DDoS) είναι πιο επικίνδυνη, καθώς χρησιμοποιεί πολλαπλές μηχανές για να ξεκινήσει την επίθεση, προκειμένου ο εισβολέας(εις) να καταλάβει τα μηχανήματα (συχνά αυτές οι επιθέσεις ονομάζονται επίσης ζόμπι ή μηχανή ρομπότ και φτιάχνουν ένα botnet για να ξεκινήσει την επίθεση DDoS). Οι επιθέσεις DoS μπορούν να αντιμετωπιστούν φιλτράροντας τις διευθύνσεις IP και απορρίπτοντας τα πακέτα που προέρχονται από την IP του εισβολέα. Αυτό είναι πιο δύσκολο στο DDoS, καθώς ο εισβολέας χρησιμοποιεί πολλαπλές μηχανές, η καθεμία στέλνοντας ένα συγκεκριμένο πλήθος πακέτων για να προκαλέσει την άρνηση

υπηρεσίας του διακομιστή θύματος (πρόκειται για μια συγχρονισμένη επίθεση, που στέλνει πολλά πακέτα από διαφορετικούς υπολογιστές). Σε αυτήν την περίπτωση, το φιλτράρισμα των διευθύνσεων IP και η ανίχνευση του επιτιθέμενου μηχανήματος γίνονται δύσκολα.

- Αλλοίωση δεδομένων ή προσποίηση άλλου προσώπου: είναι μια επίθεση όπου ο εισβολέας προσποιείται ότι είναι ένας άλλος κόμβος που τις περισσότερες φορές είναι ένας αξιόπιστος κόμβος. Μεταξύ των επιθέσεων πλαστογράφησης υπάρχουν:
    - Η επίθεση πλαστογράφησης IP όπου ένας κόμβος αλλάζει τη διεύθυνση IP του σε μια άλλη διεύθυνση διαφορετική από την πραγματική διεύθυνση πηγής.
    - Η πλαστογράφηση ARP, στοχεύει στην αποστολή ψεύτικων απαντήσεων σε ερωτήματα ARP, με αποτέλεσμα την αντιστοίχιση της διεύθυνσης IP σε μια ψεύτικη διεύθυνση MAC και, κατά συνέπεια, τη μόλυνση της προσωρινής μνήμης ARP.
    - Η πλαστογράφηση DNS, η οποία είναι παρόμοια με την πλαστογράφηση ARP και έχει ως αποτέλεσμα να κατευθύνει τον αιτούντα σε λάθος ιστοσελίδα ή υπηρεσία αλληλογραφίας αντιστοιχίζοντας τις σελίδες σε λάθος διευθύνσεις στην κρυφή μνήμη DNS, γνωστή και ως επίθεση Kaminsky όπου ο εισβολέας προσπαθεί να δηλητηριάσει την κρυφή μνήμη DNS κατασκευάζοντας την απάντηση σε συγκεκριμένο αίτημα· ο εισβολέας πετυχαίνει κυρίως αυτή την επίθεση επειδή μπορεί να μαντέψει τον αριθμό σειράς της απάντησης DNS που είναι γνωστό ως Query ID.
- Επίθεση πλημμύρας (flooding): είναι μια επίθεση που στοχεύει στον κορεσμό του δικτύου ή των πόρων του στοχευμένου κόμβου στέλνοντας τεράστια ποσότητα πακέτων όπως πακέτα TCP SYN ή πακέτα PING.
    - Στην επίθεση πλημμύρας SYN, ο εισβολέας στέλνει μηνύματα SYN από διαφορετικές διευθύνσεις IP στον διακομιστή θύμα, ο διακομιστής κρατά ένα χώρο στη μνήμη για τις πληροφορίες που σχετίζονται με τη ημιανοιγμένη σύνδεση, απαντά με ACK και περιμένει το ACK του εισβολέα ή τη λήξη της συνεδρίας. Με

πολλά εκκρεμή αιτήματα, ο χώρος μνήμης που διατίθεται για την αποθήκευση πληροφοριών σύνδεσης θα φτάσει στο όριο του προκαλώντας την άρνηση της υπηρεσίας.

- Στην επίθεση πλημμύρας PING, ο εισβολέας στέλνει πολλαπλά αιτήματα ping για να προκαλέσει την απουσία απάντησης του θύματος.
- Υπάρχει ένας άλλος τύπος πλημμύρας που είναι η πλημμύρα UDP, η οποία βασίζεται στην αποστολή μεγάλου αριθμού πακέτων UDP στο θύμα με αποτέλεσμα την άρνηση υπηρεσίας.

- Επίθεση Jamming: πρόκειται για επίθεση φυσικού επιπέδου που παρεμποδίζει τη ραδιοσυχνότητα που χρησιμοποιείται για την επικοινωνία μεταξύ των κόμβων του δικτύου. Ο θόρυβος που δημιουργείται διακόπτει την επικοινωνία μεταξύ των κόμβων προκαλώντας συγκρούσεις και αστοχία.
- Επίθεση ανθρώπου στη μέση (Man in the Middle): πρόκειται για μια επίθεση όπου ο υποκλοπέας δημιουργεί, αλλοιώνει ή πετάει τα πακέτα. Ο εισβολέας πρώτα παρεμποδίζει την κυκλοφορία δεδομένων, σπάει την αλυσίδα ελέγχου ταυτότητας και στη συνέχεια προσποιείται τους παραβιασμένους κόμβους – παραλήπτες χωρίς προβλήματα.
- Απομόνωση κόμβων: πρόκειται για την επίθεση στην οποία γίνεται διαμερισμός του δικτύου εμποδίζοντας έναν κόμβο ή ένα σύνολο κόμβων να επικοινωνήσει με το υπόλοιπο δίκτυο.
- Διακοπή διαδρομής (Route disruption): πρόκειται για την επίθεση στην οποία δημιουργούνται προβλήματα στη δρομολόγηση, δηλαδή οι διαδρομές τροποποιούνται με παραποίηση των απαντήσεων δρομολόγησης, έτσι ώστε να δημιουργούνται βρόχοι δρομολόγησης ή να προωθούνται πακέτα κατά μήκος λανθασμένων, μη βέλτιστων ή ανύπαρκτων διαδρομών.
- Κατανάλωση πόρων: σε αυτή την επίθεση μειώνεται η απόδοση του δικτύου καταναλώνοντας εύρος ζώνης δικτύου ή πόρων από τους κόμβους όπως η μνήμη ή η ενέργεια.

- Υποκλοπή γνωστή και ως επίθεση αποκάλυψης, όπου ο εισβολέας παρεμποδίζει και αναλύει την κίνηση του δικτύου (μεταδιδόμενα μηνύματα). Είναι μια παθητική επίθεση αφού ο χρήστης δεν αλλοιώνει, δημιουργεί ή απορρίπτει τα πακέτα.
- Σκουληκότρυπα (Wormhole tunnelling): η επίθεση σκουληκότρυπας είναι δυνατή ακόμη και αν ο εισβολέας δεν έχει θέσει σε κίνδυνο κανέναν κεντρικό υπολογιστή και ακόμη και αν όλη η επικοινωνία παρέχει αυθεντικότητα και εμπιστευτικότητα. Στην επίθεση σκουληκότρυπας, ένας εισβολέας καταγράφει τα πακέτα (ή τα bit) σε μια θέση στο δίκτυο, τα διοχετεύει (επιλεκτικά) σε μια άλλη θέση και τα επαναμεταδίδει από εκεί στο δίκτυο.
- Επιθέσεις χρονισμού (Timing attacks): ο εισβολέας προσποιείται ότι είναι πιο κοντά στους κόμβους του θύματος από ό,τι πραγματικά είναι. Αυτό μπορεί να γίνει είτε στέλνοντας μια ψεύτικη απάντηση διαδρομής είτε πλημμυρίζοντας το δίκτυο με μηνύματα hello που μεταδίδονται με υψηλή ισχύ, αρκετή για να κάνει τον κόμβο-θύμα να πιστέψει ότι ο εισβολέας είναι γειτονικός κόμβος.
- Κρυφή επίθεση (Stealthy attack): είναι παρόμοια με την επίθεση DoS, αλλά ο εισβολέας δεν ελέγχει τον κόμβο, αντίθετα χειρίζεται τον πίνακα δρομολόγησης των θυμάτων, καθώς τα δρομολογημένα πακέτα προκαλούν διακοπή στο δίκτυο. Μια άλλη μορφή κρυφής επίθεσης βασίζεται επίσης στην εκμετάλλευση του πίνακα δρομολόγησης και επιτρέπει στον εισβολέα να κρυφακούει κόμβους που βρίσκονται εκτός της εμβέλειάς του χρησιμοποιώντας τον κόμβο θύματος.
- Επίθεση μαύρης τρύπας: είναι μια επίθεση που εξαπολύεται από έναν εσωτερικό χρήστη που αποτυγχάνει να μεταδώσει μηνύματα ή πακέτα και αντ' αυτού τα απορρίπτει.
- Επίθεση καταβόθρας: ο εισβολέας ή ο κακόβουλος κόμβος προσελκύει την κυκλοφορία του δικτύου και στη συνέχεια κάνει μια επιλεκτική προώθηση.
- Spamming: οι χάκερ χρησιμοποιούν συχνά αυτή την τεχνική για να παραδίδουν στον παραλήπτη ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, όπως διαφημίσεις, για να υποκλέψουν τα διαπιστευτήρια χρήστη (phishing) ή για να καταστρέψουν τον διακομιστή αλληλογραφίας στέλνοντας εκατομμύρια ανεπιθύμητα μηνύματα, μια επίθεση γνωστή ως βομβαρδισμός αλληλογραφίας.

- Επίθεση προσποίησης θέσης και πλαστογράφησης GPS: σε αυτήν την επίθεση, ο εισβολέας παράγει ένα ισχυρότερο σήμα εντοπισμού από αυτό του σήματος GPS με ψεύτικη θέση, έτσι ώστε ο κόμβος του δέκτη να λαμβάνει πλαστές πληροφορίες.
- Επίθεση Sybil: η ικανότητα του κόμβου εισβολέα να έχει πολλαπλές ταυτότητες, κάτι που είναι επικίνδυνο, επειδή ο κόμβος μπορεί να χρησιμοποιήσει τις πολλαπλές ταυτότητες για να δημιουργήσει πρόσθετες ψήφους σε αλγόριθμους εκλογών, να δρομολογήσει πολλαπλές διαδρομές μέσω αυτού (τον κακόβουλο κόμβο) ή να αποφύγει την ανιχνευσιμότητα.
- Επίθεση μεταμφιεσμένων: ο κόμβος εισβολέα υποκρίνεται ότι είναι ένας νόμιμος κόμβος για τη διεξαγωγή άλλων επιθέσεων, όπως η έγχυση ψευδών μηνυμάτων.
- Επίθεση επανάληψης: ο κόμβος εισβολέα καταγράφει πακέτα που ανταλλάσσονται για να τα αναμεταδώσει αργότερα.
- Παραβίαση περιόδων σύνδεσης: ο εισβολέας φτιάχνει μια απροστάτευτη συνεδρία αφού έχει αρχικοποιηθεί, πλαστογραφώντας τη διεύθυνση IP και υπολογίζοντας τον αριθμό σειράς για να ξεκινήσει επιθέσεις DoS.
- Phishing: μια επίθεση εναντίον χρηστών υπολογιστών για να τους πείσει να εκτελέσουν μια ενέργεια που μπορεί να τους προκαλέσει βλάβη. Μπορεί να γίνει με την αποστολή email στο θύμα, το οποίο πρέπει να κατεβάσει ένα συνημμένο ή να κάνει κλικ σε έναν σύνδεσμο. Το συνημμένο θα μπορούσε να περιέχει κακόβουλα προγράμματα όπως ιούς, λογισμικό κατασκοπείας ή καταγραφέα κωδικών που είτε κλέβουν τις πληροφορίες του χρήστη, είτε επιβραδύνουν την απόδοση του συστήματος είτε το καταστρέφουν. Ο σύνδεσμος θα κατευθύνει τον χρήστη σε μια ψεύτικη ιστοσελίδα, όπου θα μπορούσε να του ζητηθεί να παράσχει ευαίσθητα δεδομένα.
- Χακάρισμα κωδικού πρόσβασης: μια τέτοια επίθεση μπορεί να γίνει είτε μαντεύοντας τον κωδικό πρόσβασης, είτε με κλοπή του αρχείου που περιέχει τον κωδικό πρόσβασης (αν είναι αποθηκευμένο ως καθαρό κείμενο), είτε μέσω επίθεσης brute force ή επίθεσης λεξικού είτε μέσω τεχνικών κοινωνικής μηχανικής (social engineering). Αξίζει να σημειωθεί ότι ένας κωδικός πρόσβασης γενικά δεν αποθηκεύεται ως καθαρό κείμενο, αλλά

ως τιμές κατακερματισμού και μερικές φορές ακόμη και ως αλλαγμένες τιμές κατακερματισμού (π.χ. με μια τυχαία τιμή που προστίθεται σε έναν κωδικό πρόσβασης πριν κατακερματιστεί και διασφαλίζει ότι δύο κωδικοί πρόσβασης δεν θα έχουν τον ίδιο κατακερματισμό) .

- Δάκρυ (Teardrop): επίθεση που μπορεί να χρησιμοποιηθεί για να προκαλέσει άρνηση εξυπηρέτησης. Εκμεταλλεύεται τα χαρακτηριστικά του IP datagram που είναι ότι μια μεμονωμένη μονάδα δεδομένων μπορεί να έχει μεταβλητό μήκος και μπορεί να κατακερματιστεί σε μικρότερα κομμάτια και να μεταδοθεί. Κάθε κομμάτι θα υποδεικνύει τη θέση του στην αρχική μονάδα δεδομένων και το μήκος του, έτσι ώστε ο δέκτης να συναρμολογήσει εκ νέου τα κομμάτια για να λάβει τα πλήρη δεδομένα που αποστέλλονται. Ο εισβολέας θα χρησιμοποιούσε αυτά τα χαρακτηριστικά, αλλά η θέση των κομματιών θα επικαλύπτεται προκαλώντας το κρασάρισμα του συστήματος ενώ προσπαθεί να τα συναρμολογήσει.
- Κοινωνική μηχανική (Social engineering): ο εισβολέας εξαπατά τους χρήστες για να του/της δώσουν εμπιστευτικές πληροφορίες, όπως για τον κωδικό πρόσβασης, για τη διαμόρφωση του συστήματος ή στοιχεία επικοινωνίας. Η κοινωνική μηχανική χρησιμοποιεί ψυχολογικά κόλπα, αφού ο άνθρωπος συχνά τείνει να εμπιστεύεται, να συμπάσχει και να βοηθάει ο ένας τον άλλον. Ο χάκερ μπορεί να χρησιμοποιήσει αυτά τα χαρακτηριστικά για να ξεγελάσει τα θύματά του. Ο χάκερ συχνά κάνει έρευνα ιστορικού για τη στοχευμένη εταιρεία και συλλέγει χρήσιμες πληροφορίες τις οποίες μπορεί να χρησιμοποιήσει για να κερδίσει την εμπιστοσύνη του θύματος. Ο εισβολέας που προσποιείται ότι είναι κάποιος από το εσωτερικό του συστήματος, μπορεί να επικοινωνήσει με το θύμα μέσω τηλεφώνου, email ή αυτοπροσώπως και να ζητήσει ευαίσθητες πληροφορίες. Αυτή η επίθεση είναι επίσης γνωστή ως ανθρώπινο hacking.
- Τεχνικά ευάλωτα σημεία: περιλαμβάνει ευπάθειες συστήματος, πρωτοκόλλου δικτύου και βάσης δεδομένων, για παράδειγμα: έγχυση SQL (SQL injection), υπερχείλιση buffer (buffer overflow) κ.λπ.

- Εξόρυξη δεδομένων: αναφέρεται σε μια διαδικασία μη τετριμμένης εξαγωγής σημαντικών, προηγουμένως άγνωστων και δυνητικά χρήσιμων πληροφοριών από βάσεις δεδομένων.
- Η "βουτιά στα σκουπίδια" (dumpster diving / trashing) και είναι μία από τις τεχνικές κοινωνικής μηχανικής. Ο εισβολέας συλλέγει τα σκουπίδια των εταιρειών για να αναζητήσει χρήσιμες πληροφορίες, όπως επαφές, κωδικό πρόσβασης, παλιούς σκληρούς δίσκους, εκτυπώσεις πηγαίου κώδικα, σχεδιασμό συστήματος ασφαλείας, διαμόρφωση συστήματος κ.λπ. Ο χάκερ μπορεί να χρησιμοποιήσει τις συλλεγόμενες πληροφορίες για να παραβιάσει το σύστημα ή δίκτυο.
- Επιθέσεις κατακερματισμού: σε αυτή την επίθεση γίνεται κατακερματισμός ενός πακέτου σε μικρά κομμάτια, μερικές φορές επικαλυπτόμενα, για να δημιουργηθούν προβλήματα στο δέκτη εάν δεν υπάρχει ελάχιστο μέγεθος κομματιού και offset.
- Κακόβουλο λογισμικό: είναι ένα τμήμα κωδικών που προορίζονται να προκαλέσουν βλάβη. Περιλαμβάνει:
    - Ιοί: "Ο όρος ιός υπολογιστή ορίζεται ως ένα πρόγραμμα που μπορεί να "μολύνει" άλλα προγράμματα τροποποιώντας τα ώστε να περιλαμβάνουν ένα πιθανώς εξελιγμένο αντίγραφο του εαυτού του".
    - Ad ware: εργαλεία για διαφήμιση· αυτό το λογισμικό ενδέχεται να εγκαταστήσει άλλα εργαλεία χωρίς άδεια.
    - Spyware: εργαλεία που χρησιμοποιούνται για τη συλλογή πληροφοριών σχετικά με έναν χρήστη ή έναν οργανισμό εν αγνοία του.
    - Rootkit (rootkit λειτουργεί ως root): ένας κακόβουλος κώδικας που κρύβει την παρουσία του στο σύστημα παρεμποδίζοντας και φιλτράροντας εντολές λειτουργικών συστημάτων που μπορεί να οδηγήσουν στην ανακάλυψή του, και όταν ανακαλυφθεί και αφαιρεθεί, θα μπορούσε να ξαναεγκαταστήσει τον ευατό του.

- Σκουκλήκι (Worm): σε αντίθεση με τον ιό που απαιτεί από τον χρήστη να λάβει μέτρα, όπως η εκτέλεση ή η αντιγραφή του φέροντος προγράμματος για τη διάδοσή του, τα σκουλήκια είναι κακόβουλα προγράμματα που αυτοδιαδίδονται σε ένα δίκτυο εκμεταλλευόμενα τα ελαττώματα ασφαλείας στις χρησιμοποιούμενες υπηρεσίες.
- Scripts: γνωστά και ως ευπάθειες μεταξύ ιστότοπων scripting, που επιτρέπουν στον εισβολέα να συμπεριλάβει κακόβουλο κώδικα που συνήθως γράφεται με JavaScript στον ιστότοπο που αποστέλλεται στο πρόγραμμα περιήγησης ενός θύματος. Ο κώδικας μπορεί να καταγράψει την είσοδο του πληκτρολογίου, να κλέψει ευαίσθητα δεδομένα ή το αναγνωριστικό περιόδου λειτουργίας και πολλές να εκπονήσει άλλες μορφές επιθέσεων.
- Δούρειοι ίπποι (Trojans): ένα πρόγραμμα με φανερές και κρυφές λειτουργίες, η φανερή συνάρτηση είναι αυτό που αναμένεται από το πρόγραμμα, η κρυφή είναι η ανεπιθύμητη και απροσδόκητη λειτουργία που αντιπροσωπεύει την απειλή για τον χρήστη ή το σύστημα. Παραδείγματα κρυφής λειτουργίας: καταγραφή κλειδιών, κλοπή διαπιστευτηρίων κ.λπ. Σε αντίθεση με τους ιούς, ένας trojan δεν αναπαράγεται.
- Backdoor: χρησιμοποιείται συχνά από το χάκερ για τον έλεγχο των υπολογιστών για τη δημιουργία δικτύων bot και την εκπόνηση επιθέσεων DoS, είναι μια μέθοδος πρόσβασης σε ένα σύστημα παρακάμπτοντας ελέγχους ταυτότητας και ασφάλειας.

- Αλλοίωση δικαιωμάτων: εάν ένας εισβολέας αποκτήσει πρόσβαση στο σύστημα ως διαχειριστής ή ως root, θα μπορούσε να αλλάξει τα δικαιώματα των νόμιμων χρηστών δίνοντάς τους λιγότερα δικαιώματα.
- Άρνηση και παραβίαση δικαιωμάτων: ένας χρήστης μπορεί να αρνηθεί ότι είναι ο δημιουργός δεδομένων (άρνηση), ενώ η παραβίαση δικαιωμάτων είναι όταν κάποιος προσπαθεί να κλέψει τα πιστοποιητικά ενός ψηφιακού έργου προσποιούμενος ότι είναι ο πραγματικός κάτοχος.

- Καταστροφή: μπορεί να είναι είτε φυσική επίθεση, όπως η διάλυση των ηλεκτρονικών συσκευών, ο μαγνητισμός τους, η χρήση χημικών προϊόντων ή η πυρκαγιά ή μπορεί επίσης να είναι λογική επίθεση, όπως η παραβίαση ή η καταστροφή των αρχείων και των δεδομένων.
- Απάτη και κλοπή: η απάτη μεταβάλλει την ακεραιότητα των δεδομένων για όφελος, π.χ. η παραποίηση συναλλαγών. Η κλοπή περιλαμβάνει κλοπή λογισμικού και υλικού και είναι η πράξη διαπραγμάτευσης πληροφοριών, μυστικών ή κλεμμένου υλικού με σκοπό το κέρδος.

2.7 ΛΥΣΕΙΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Αυτή η ενότητα περιγράφει ορισμένες από τις λύσεις και τα μέτρα ασφαλείας που αναφέρονται στο Σχήμα 1, όπως: έλεγχος ταυτότητας, στεγανογραφία, κρυπτογραφία, anti-malware, συστήματα ανίχνευσης και πρόληψης εισβολής, τείχη προστασίας, εικονικοποίηση, δημιουργία αντιγράφων ασφαλείας, ενημερώσεις κώδικα και εκπαίδευση χρηστών.

2.7.1 Έλεγχος ταυτότητας/ Εξουσιοδότηση/ Έλεγχος

Είναι το πρώτο μέτρο ασφαλείας έναντι εισβολέων συστημάτων, δικτύων και βάσεων δεδομένων, καθώς προσδιορίζει τον εξουσιοδοτημένο χρήστη, του εκχωρεί συγκεκριμένα δικαιώματα πρόσβασης και καταγράφει ό,τι συμβαίνει στο σύστημα.

Ο έλεγχος ταυτότητας είναι η διαδικασία ταυτοποίησης ενός χρήστη ή ενός ατόμου και οι μηχανισμοί του μπορούν να χρησιμοποιούν τρεις ιδιότητες, [23], [24]:

- Πιστοποίηση με βάση τη γνώση: με βάση δηλαδή κάποιο όνομα χρήστη ή κωδικό που γνωρίζει μόνο ο νόμιμος χρήστης.
- Πιστοποίηση με βάση την κατοχή: με βάση δηλαδή κάποιο αντικείμενο/ χαρακτηριστικό που έχει ο χρήστης, π.χ. κάποια έξυπνη κάρτα, token κλπ.
- Πιστοποίηση με βάση την φυσιολογία: με βάση δηλαδή κάτι με το οποίο χαρακτηρίζει το χρήστη, π.χ. κάποιο βιομετρικό χαρακτηριστικό όπως μάτια, πρόσωπο, ίριδα, κλπ.

Η εξουσιοδότηση επιτρέπει τον προσδιορισμό του χρήστη που, αφού εντοπιστεί, επιτρέπεται να έχει τους πόρους. Υλοποιείται μέσω της χρήσης μηχανισμών ελέγχου πρόσβασης

με την παραχώρηση ή την άρνηση της πρόσβασης σε έναν πόρο σύμφωνα με ένα σύνολο κριτηρίων. Διαφοροποιεί τους χρήστες παραχωρώντας διαφορετικό σύνολο δικαιωμάτων και προνομίων.

Έλεγχος: Η παρακολούθηση και η ανίχνευση της δραστηριότητας που σχετίζεται με τη χρήση ενός πόρου δίνει στον διαχειριστή ασφαλείας τη δυνατότητα να γνωρίζει τι πραγματικά συμβαίνει στο σύστημα και στο δίκτυο. Αυτό του/ της επιτρέπει να έχει μια ξεκάθαρη άποψη για το τι υποτίθεται ότι θα συμβεί, δίνοντάς του έτσι περισσότερες πιθανότητες να εντοπίσει τα τρωτά σημεία και να τα διορθώσει.

2.7.2 Κρυπτογραφία

Η κρυπτογραφία είναι η επιστήμη της διασφάλισης μηνυμάτων μέσω κρυπτογράφησης του περιεχομένου, ώστε να μην γίνεται κατανοητό από τρίτους. Σύμφωνα με τον Benarous [12], έχει δύο τύπους:

- τη συμμετρική κρυπτογραφία και
- την ασύμμετρη κρυπτογραφία.

Χρονολογικά, η κρυπτογραφία μυστικού κλειδιού ήρθε πρώτη, αλλά δεδομένου ότι η ασφαλής διανομή και διαχείριση αυτών των κλειδιών ήταν τα μειονεκτήματα αυτής της μεθόδου, η ασύμμετρη κρυπτογραφία ήρθε να επιλύσει αυτό το πρόβλημα βασιζόμενη στη χρήση ενός ζεύγους κλειδιών που το ένα είναι δημόσιο και χρησιμοποιείται για κρυπτογράφηση και το άλλο είναι ιδιωτικό που χρησιμοποιείται για αποκρυπτογράφηση, [13].

2.7.3 Στεγανογραφία

Η ψηφιακή στεγανογραφία περιλαμβάνει την απόκρυψη δεδομένων ψηφιακής μορφής σε ένα εξώφυλλο, όπως εικόνες, βίντεο, αρχεία ήχου, έγγραφα (word, PDF, ιστοσελίδες κ.λπ.), συμπιεσμένα αρχεία (rar, zip, κ.λπ.), αρχείο δίσκου εικονικής μηχανής, πρωτόκολλα δικτύου (κεφαλίδες) ή αρχεία λειτουργικού συστήματος κ.λπ.

Για κάθε τύπο αρχείου "κάλυμμα" που χρησιμοποιείται, η ιδέα στοχεύει στην ενσωμάτωση του μηνύματος με τέτοιο τρόπο ώστε η αλλαγή να μην ανιχνεύεται οπτικά. Η αλλαγή μπορεί να έχει ως αποτέλεσμα το αρχείο που προκύπτει με τα ενσωματωμένα δεδομένα να είναι μεγαλύτερο

σε μέγεθος, με χαμηλότερη ποιότητα ή να περιλαμβάνει θόρυβο που μπορεί να γίνει αντιληπτός από το ανθρώπινο μάτι ή το αυτί.

Σύμφωνα με τους συγγραφείς, [12], [25], μερικές από τις υπάρχουσες τεχνικές στεγανογραφίας είναι οι ακόλουθες:

- Στεγανογραφία στις εικόνες: η συνηθέστερη μέθοδος είναι η απόκρυψη των δεδομένων στο λιγότερο σημαντικό bit του pixel.
- Στεγανογραφία στον ήχο: με απόκρυψη δεδομένων στο ηχητικό σήμα με ανεπαίσθητο τρόπο (μη ανιχνεύσιμο από το ανθρώπινο αυτί).
- Στεγανογραφία στο βίντεο: εκμεταλλεύονται το γεγονός ότι ένα βίντεο αποτελείται από ένα σύνολο εικόνων, συνεπώς βασίζονται στην ενσωμάτωση δεδομένων κατά τη διαδικασία κωδικοποίησης/ αποκωδικοποίησης ή στον ήχο και στις εικόνες του βίντεο.
- Στεγανογραφία στα πρωτόκολλα: με προσάρτηση των δεδομένων στις κεφαλίδες των πακέτων.
- Γραπτή και προφορική στεγανογραφία: στην προφορική γλώσσα μπορεί να γίνει ανάλογα με την προφορά των λέξεων αι στη γραπτή γλώσσα αλλοιώνοντας κάποιες λέξεις κειμένου.

2.7.4 Anti-Malware

Το anti-malware σχετίζεται με ένα σύνολο εργαλείων για τον εντοπισμό και την αφαίρεση κακόβουλων προγραμμάτων (ιούς, worms, adware, spyware, rootkit, κ.λπ.). Σύμφωνα με τους συγγραφείς, [12], [26], η αναζήτηση για κακόβουλο λογισμικό μπορεί να γίνει με δύο τεχνικές:

- Ευρετικές μεθόδους, που επιτρέπουν τον εντοπισμό νέων απειλών με βάση τη συμπεριφορά του κακόβουλου λογισμικού και τις επιπτώσεις που έχουν στο σύστημα.
- Μεθόδους υπογραφής, με αναζήτηση για υπογραφή κακόβουλου λογισμικού από τη βάση δεδομένων του anti-malware, η οποία ενημερώνεται τακτικά κάθε φορά που εντοπίζεται και αναλύεται ένα κακόβουλο λογισμικό. Αυτή η μέθοδος είναι γρήγορη, αλλά εντοπίζει μόνο γνωστές απειλές.

Το anti-malware εντοπίζει ένα σύνολο από κακόβουλα λογισμικά διαφορετικών τύπων. Υπάρχουν συγκεκριμένα εργαλεία για κάθε τύπο κακόβουλου λογισμικού, όπως: το antivirus που

εντοπίζει ιούς, worms και Trojans κ.λπ. το anti-spyware που αφαιρεί λογισμικό κατασκοπείας που έχει βάλει χάκερ και προγράμματα αφαίρεσης adware που αφαιρούν το adware από το σύστημα. Αξίζει να σημειωθεί ότι μερικές φορές ένα κακόβουλο λογισμικό μπορεί να είναι ένα adware, ένα λογισμικό υποκλοπής spyware ή ένας trojan και ένα rootkit που συνδυάζονται μεταξύ τους για να είναι πιο διακριτικό και καταστροφικό.

Οι αλγόριθμοι ανίχνευσης κακόβουλου λογισμικού περιλαμβάνουν: ευρετικούς αλγόριθμους ανίχνευσης, στατιστική ανάλυση (συχνότητα και μοτίβο εντολών), προσομοίωση βάσει εντολών και προσομοίωση με βάση το περιβάλλον.

2.7.5 Συστήματα ανίχνευσης και αποτροπής εισβολών

Το σύστημα ανίχνευσης εισβολής (Intrusion Detection System - IDS) παρακολουθεί τα συμβάντα που συμβαίνουν σε ένα σύστημα ή ένα δίκτυο και τα αναλύει για να εντοπίσει προβλήματα ασφαλείας. Το σύστημα είναι παθητικό, που σημαίνει ότι αποθηκεύει τις λεπτομέρειες των προβλημάτων ασφαλείας σε αρχεία καταγραφής και ειδοποιεί τον διαχειριστή ασφαλείας, αλλά δεν προσπαθεί να σταματήσει ή να αποτρέψει την επίθεση. Το σύστημα αποτροπής εισβολής (Intrusion Prevention System - IPS) ανιχνεύει την εισβολή και προσπαθεί να τη σταματήσει. Οι βασικές λειτουργίες που εκτελεί ένα σύστημα IDS/ IPS (IDPS) είναι: καταγραφή και αναφορά συμβάντων ασφαλείας, ειδοποίηση του διαχειριστή ασφαλείας και αποτροπή επιθέσεων.

Σύμφωνα με τους συγγραφείς, [12], [27], [28], μερικά από τα υπάρχοντα συστήματα IDPS είναι τα ακόλουθα:

- Αυτά που βασίζονται στην υπογραφή: ανιχνεύουν τις γνωστές απειλές συγκρίνοντας το μοναδικό τους μοτίβο που είναι γνωστό ως υπογραφή με τη βάση δεδομένων των γνωστών απειλών.
- Αυτά που βασίζονται σε ανωμαλίες: συγκρίνουν την κανονική συμπεριφορά με τα παρατηρούμενα συμβάντα για τον εντοπισμό απειλών.
- Αυτά που αναλύουν τα πρωτόκολλα κατάστασης: το IDPS παρακολουθεί την κατάσταση των πρωτοκόλλων δικτύου, μεταφοράς και εφαρμογών που έχουν μια έννοια κατάστασης, δηλαδή μπορεί να συνδέσει αιτήματα με απαντήσεις και να εντοπίσει απροσδόκητη ακολουθία εντολών.

- Αυτά που είναι βασισμένα σε host: το IDPS παρακολουθεί τον κεντρικό υπολογιστή (host), ο οποίος μπορεί να είναι μηχάνημα ή διακομιστής, παρακολουθώντας την κυκλοφορία του δικτύου, τις διεργασίες που εκτελούνται, την πρόσβαση και την τροποποίηση αρχείων/ καταλόγων (επεξεργασία/ διαγραφή) και τα αρχεία καταγραφής του συστήματος για τον εντοπισμό ύποπτης δραστηριότητας που μπορεί ενδεχομένως να αποτελεί τοπική απειλή.
- Αυτά που είναι βασισμένα σε δίκτυο: το IDPS παρακολουθεί την κυκλοφορία του δικτύου και αναλύει τη δραστηριότητα του πρωτοκόλλου δικτύου και εφαρμογών για να εντοπίσει και να εξαλείψει ύποπτη δραστηριότητα.
- Τα υβριδικά IDPS (βασισμένα σε host/ δίκτυο): το IDPS έχει δύο μέρη, μια διεπαφή που παρακολουθεί το δίκτυο και μια διεπαφή που παρακολουθεί τον τοπικό κεντρικό υπολογιστή.

2.7.6 Τείχη προστασίας

Το τείχος προστασίας έχει στόχο να ασφαλίσει το τοπικό δίκτυο και να το απομονώσει από τις απειλές εντοπίζοντας την εισβολή στο σύστημα, ελέγχοντας την πρόσβαση στους πόρους και αναλύοντας την επερχόμενη κίνηση. Υπάρχουν διάφορες κατηγορίες τειχών προστασίας, [29]:

- Stateless τείχος προστασίας: η παλαιότερη και βασική μέθοδος, στην οποία κάθε πακέτο ελέγχεται ανεξάρτητα, με βάση τους προκαθορισμένους κανόνες του διαχειριστή. Φιλτράρει το πακέτο με βάση τις διευθύνσεις IP και τον αριθμό θύρας τους.
- Stateful τείχος προστασίας: ένα τείχος προστασίας που βασίζεται στη μνήμη. Τα πακέτα δεν ελέγχονται μόνο βάσει των κανόνων του διαχειριστή (IP, αριθμός θύρας) αλλά και την κατάσταση της συνεδρίας· αυτό επιτρέπει τον εντοπισμό και την αποτροπή ορισμένων επιθέσεων DoS, όπως η πλημμύρα SYN.
- Τείχος προστασίας εφαρμογής (proxy): αυτό το τείχος προστασίας πρέπει να γνωρίζει όλα τα πρωτόκολλα και τους κανόνες της εφαρμογής, κάθε εφαρμογή, έχει μια ειδική διεργασία στον διακομιστή μεσολάβησης που είναι υπεύθυνος για το φιλτράρισμα.
- Τείχος προστασίας αυθεντικοποίησης: το φιλτράρισμα δεν βασίζεται μόνο στις διευθύνσεις μηχανήματος (IP) αλλά και στους χρήστες.

- Προσωπικό τείχος προστασίας: εργαλεία anti-malware και anti-spyware που είναι εγκατεστημένα στους κεντρικούς υπολογιστές.
- Τείχος προστασίας επόμενης γενιάς: Χάρη στις σημαντικές βελτιώσεις στο χώρο αποθήκευσης, τη μνήμη και στην ταχύτητα επεξεργασίας, τα τείχη προστασίας επόμενης γενιάς βασίζονται σε χαρακτηριστικά των παραδοσιακών τειχών προστασίας με επιπλέον κρίσιμες λειτουργίες ασφαλείας, όπως πρόληψη εισβολών, VPN, anti-malware και ακόμη και κρυπτογραφημένη παρακολούθηση κυκλοφορίας.

2.7.7 Εικονικοποίηση

Η εικονικοποίηση επιτρέπει την ύπαρξη πολλαπλών λειτουργικών συστημάτων στον ίδιο διακομιστή ή κεντρικό σύστημα. Μπορεί να χρησιμοποιηθεί για λόγους ασφαλείας, όπως για δοκιμή μη αξιόπιστου λογισμικού, επειδή τα εικονικά συστήματα καταλαμβάνουν συγκεκριμένα κομμάτια μόνο του δίσκου. Επομένως, εάν το σύστημα έχει παραβιαστεί, τα μολυσμένα κομμάτια μπορούν να απομονωθούν και η πρόσβαση σε πόρους, όπως ο δίσκος ή τα δίκτυα μπορεί να διακοπεί. Συνιστάται η δημιουργία αντιγράφων ασφαλείας του εικονικού συστήματος για την επαναφορά του σε περίπτωση σοβαρών προβλημάτων ασφαλείας, [30].

2.7.8 Δημιουργία αντιγράφων ασφαλείας, ενημερώσεις κώδικα και εκπαίδευση χρηστών

Σε πολλές περιπτώσεις, το πρόβλημα ασφαλείας οφείλεται σε λανθασμένη διαμόρφωση, όπως μια συνεχώς ανοιχτή θύρα ή μια εσφαλμένη διαμόρφωση τείχους προστασίας (λάθη του διαχειριστή ασφαλείας). Η εκπαίδευση του διαχειριστή ασφαλείας να δημιουργεί αντίγραφα ασφαλείας, να παρακολουθεί την κυκλοφορία του δικτύου και να εφαρμόζει ενημερώσεις κώδικα σε ευπάθειες που έχουν εντοπιστεί είναι υποχρεωτική για τη διατήρηση της ασφάλειας ενός συστήματος ή ενός δικτύου. Μερικές φορές το σύστημα ασφαλείας μπορεί να έχει ρυθμιστεί σωστά και βασίζεται στον συνδυασμό νέων τεχνολογιών, όπως τη βιομετρία, τη χρήση tokens, έξυπνων καρτών, τειχών προστασίας, IDPS και anti-malware. Ωστόσο, εξαιτίας του χρήστη μπορεί να παραβιαστούν, καθώς ο χρήστης μπορεί να υποστεί επίθεση κοινωνικής μηχανικής, επίθεση δηλαδή από εξωτερικούς χρήστες για να αποκτήσουν εξουσιοδοτημένη πρόσβαση. Έτσι, οι χρήστες πρέπει να γνωρίζουν αυτήν την επίθεση και να διδάσκονται για να προστατεύονται κατάλληλα.

2.8 ΣΥΝΟΨΗ

Στην παρούσα ενότητα παρουσιάστηκε η έννοια του διαδικτύου και οι διάφορες πτυχές του από πλευράς ασφάλειας. Πιο συγκεκριμένα, μελετήθηκε η κυβερνοασφάλεια και πώς εξελίχθηκε αυτή μέχρι σήμερα, σαν συνοδοιπόρος με την εξέλιξη της τεχνολογίας. Αναπτύχθηκαν οι στόχοι που έχει η κυβερνοασφάλεια, που είναι η διαθεσιμότητα, η εμπιστευτικότητα, η ακεραιότητα, η αυθεντικότητα, η μη άρνηση και ο έλεγχος. Με βάση αυτές τις παραμέτρους, σημειώθηκαν μέχρι και σήμερα σημαντικές απειλές/ επιθέσεις προς αυτές, κρίνοντας αναγκαία την ανάπτυξη λύσεων/ πρόληψης απέναντί τους. Σημειώθηκαν και αναλύθηκαν αρκετές λύσεις που εφαρμόζονται για την αντιμετώπιση των παραπάνω, ωστόσο στις επόμενες ενότητες θα δοθεί ιδιαίτερη σημασία στις λύσεις που παρέχει η βιομετρική τεχνολογία, εξηγώντας πρωταρχικά τι είναι και πώς μπορεί να εφαρμοστεί στην κυβερνοασφάλεια.

3. ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΤΗΣ ΒΙΟΜΕΤΡΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

Την τελευταία δεκαετία σημειώθηκε δραματική αύξηση της υιοθέτησης βιομετρικών τεχνολογιών. Αυτό οφείλεται στη σημαντική βελτίωση τεχνολογιών όπως αισθητήρες και των δυνατοτήτων επεξεργασίας δεδομένων (δηλαδή, υπολογιστική ισχύς, αλγόριθμοι). Η πρόοδος στον τομέα των φορητών υπολογιστών, με την εμφάνιση των έξυπνων συσκευών και οι αυξανόμενες ανάγκες ασφάλειας σε κρίσιμους τομείς όπως η οικονομία και η κυβέρνηση αποτελούν βασικούς μοχλούς στον τομέα της βιομετρικής ασφάλειας. Την τελευταία δεκαετία, οι περιπτώσεις χρήσης άμεσων ή έμμεσων βιομετρικών εργαλείων έχουν αυξηθεί δραματικά. Στο παρόν κεφάλαιο, μελετάται η βιομετρική τεχνολογία, τα πλεονεκτήματα και μειονεκτήματα που προκύπτουν από τη χρήση της, καθώς και συγκεκριμένες χαρακτηριστικές περιπτώσεις χρήσης της.

3.1 ΟΡΙΣΜΟΣ ΤΗΣ ΒΙΟΜΕΤΡΙΑΣ

Ορισμός της βιομετρίας που προτάθηκε από το Oxford English Dictionary, πριν από περίπου δύο δεκαετίες, η βιομετρία είναι η "εφαρμογή της στατιστικής ανάλυσης σε βιολογικά δεδομένα". Ενώ αυτός ο ορισμός περιλαμβάνει με ευρύ τρόπο την πρακτική της βιομετρικής ανάλυσης, αποτυγχάνει να αναδείξει το σημαντικό χαρακτηριστικό της εξειδίκευσης. Ένας πιο πρόσφατος ορισμός, διαθέσιμος στο διαδικτυακό λεξικό Dictionary.com, γεφυρώνει αυτό το χάσμα, με τον ακόλουθο ορισμό:

"η διαδικασία με την οποία τα μοναδικά φυσικά και άλλα χαρακτηριστικά ενός ατόμου ανιχνεύονται και καταγράφονται από μια ηλεκτρονική συσκευή ή σύστημα ως μέσο επιβεβαίωσης της ταυτότητας".

Η βιομετρία αποτελείται από τη μέτρηση βιολογικών σημάτων με σκοπό την ταυτοποίηση του ανθρώπου. Υπάρχουν πολλά βιολογικά σήματα που μπορούν να χρησιμοποιηθούν για την ταυτοποίηση του ανθρώπου, αλλά μόνο μερικά από αυτά μπορούν να προσμετρηθούν. Οι διαφορετικοί τρόποι με τους οποίους ένας άνθρωπος μπορεί να αναγνωρίσει αποτελεσματικά άλλους ανθρώπους είναι πάρα πολλοί, π.χ. με βάση τα αισθητήρια συστήματα (π.χ. όραση, ακοή, αφή, γεύση, όσφρηση, κ.λπ.). Ωστόσο, μόνο μερικά από αυτά τα συστήματα ανθρώπινης ταυτοποίησης χαρακτηρίζονται ως βιομετρικά. Το κύριο εμπόδιο είναι η πρόκληση που σχετίζεται με τη συλλεκτικότητα και τη δυνατότητα μέτρησης. Η αδυναμία μέτρησης πολλών από αυτών των

σημάτων, λόγω της έλλειψης επαρκών αισθητήρων, τα αποκλείει ως αποδεκτά βιομετρικά στοιχεία, [11].

3.2 ΚΑΤΗΓΟΡΙΕΣ ΒΙΟΜΕΤΡΙΑΣ

Οι βιομετρικές τεχνολογίες μπορούν να κατηγοριοποιηθούν με βάση τον τύπο των σημάτων στα οποία βασίζονται, και είναι κυρίως από τα ακόλουθα είδη:

- Βιομετρικές τεχνολογίες φυσιολογίας,
- Βιομετρικές τεχνολογίες συμπεριφοράς και
- Γνωστικές βιομετρικές τεχνολογίες.

Τα φυσιολογικά χαρακτηριστικά είναι εγγενή στην ανθρώπινη φυσιολογία. Παραδείγματα φυσιολογικών χαρακτηριστικών περιλαμβάνουν τη γεωμετρία των χεριών, τις μικρολεπτομέρειες των δακτύλων και τα χαρακτηριστικά του προσώπου.

Τα χαρακτηριστικά της συμπεριφοράς είναι γνωρίσματα που μαθαίνονται ή αποκτώνται με βάση τις ανθρώπινες ενέργειες. Παραδείγματα χαρακτηριστικών συμπεριφοράς περιλαμβάνουν το είδος πληκτρολόγησης (π.χ. ταχύτητα), το είδος χρήσης του ποντικιού, τη δυναμική χειρονομιών, τη δυναμική υπογραφής, τη φωνή και τα χαρακτηριστικά βάδισης.

Η γνωστική βιομετρία βασίζεται στη γνωστική, συναισθηματική και συγγενική κατάσταση ενός ατόμου ως βάση για την αναγνώριση των ατόμων. Γενικά, αυτές οι καταστάσεις του νου εξάγονται με την καταγραφή φυσιολογικών ή συμπεριφορικών βιο-σημάτων, όπως το ηλεκτροεγκεφαλογράφημα (ElectroEncephaloGram - EEG), το ηλεκτροκαρδιογράφημα (EleCtrocardioGram - ECG) και η ηλεκτροδερμική απόκριση (Electro-Dermal Response - EDR) του ατόμου ως απόκριση στην παρουσίαση ενός ερεθίσματος για λόγους πιστοποίησης ταυτότητας, π.χ. μια εικόνα που απεικονίζει ένα σημαντικό γεγονός, [11], [31].

3.3 ΑΠΑΙΤΗΣΕΙΣ ΒΙΟΜΕΤΡΙΑΣ ΚΑΙ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Οποιοδήποτε ανθρώπινο φυσιολογικό, συμπεριφορικό ή γνωστικό χαρακτηριστικό μπορεί να χρησιμοποιηθεί ως βιομετρικό χαρακτηριστικό, εφόσον πληροί τις ακόλουθες απαιτήσεις, [31], [32]:

- Καθολικότητα: Το χαρακτηριστικό ή το γνώρισμα πρέπει να είναι εφαρμόσιμο σε κάθε άνθρωπο.
- Διακριτικότητα: Οποιαδήποτε δύο άτομα πρέπει να είναι αρκετά διαφορετικά ως προς το χαρακτηριστικό αυτό.
- Μονιμότητα: Το χαρακτηριστικό θα πρέπει να είναι αρκετά αμετάβλητο σε μια χρονική περίοδο.
- Συλλεκτικότητα: Το χαρακτηριστικό να μπορεί να μετρηθεί ποσοτικά.

Η συλλεκτικότητα είναι μια βασική απαίτηση που συχνά παραβλέπεται υπέρ των άλλων απαιτήσεων (π.χ. διακριτικότητα) που είναι πιο προφανείς. Ωστόσο, αρκετές τεχνολογίες απέτυχαν να βρουν την τομή των παραπάνω, λόγω της έλλειψης πρακτικών τρόπων μέτρησης των βιο-σημάτων. Εκτός από τα προαναφερθέντα κριτήρια, ένα πρακτικό βιομετρικό χαρακτηριστικό απαιτείται να πληροί και τις των ακόλουθες απαιτήσεις:

- Απόδοση: επιτεύξιμη ακρίβεια αναγνώρισης και ταχύτητα με τους απαιτούμενους πόρους.
- Αποδεκτότητα: βαθμός στον οποίο οι άνθρωποι είναι πρόθυμοι να υιοθετήσουν ένα συγκεκριμένο βιομετρικό αναγνωριστικό στην καθημερινή τους ζωή.
- Αντίσταση στην εξαπάτηση: αντικατοπτρίζει πόσο εύκολα μπορεί να εξαπατηθεί το σύστημα χρησιμοποιώντας κακόβουλες μεθόδους, όπως πλαστογραφίες που βασίζονται σε συνθετικά δείγματα και άλλες τεχνικές αποφυγής να αναγνώρισης.
- Διατήρηση απορρήτου: προστασία των ιδιωτικών πληροφοριών χρήστη που είναι ενσωματωμένα στα βιομετρικά πρότυπα και στις υποκείμενες τεχνολογίες

3.4 ΧΡΗΣΗ ΒΙΟΜΕΤΡΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

Οι βιομετρικές τεχνολογίες παρέχουν τη βάση για εξαιρετικά ασφαλείς λύσεις ανθρώπινης ταυτοποίησης και επαλήθευσης. Αυτές περιλαμβάνουν:

- Φυσικός έλεγχος και παρακολούθηση πρόσβασης,
- Αυθεντικοποίηση,
- Ψηφιακή εγκληματολογία,

- Ώρα προσέλευσης,
- Ασφάλεια των συνόρων,
- Ακεραιότητα διαβατηρίου,
- Ηλεκτρονική ψηφοφορία και από κοντά.

Ένας από τους μεγαλύτερους τομείς εφαρμογής είναι τα αυτοματοποιημένα συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων (Automated Fingerprint Identification Systems - AFIS), τα οποία χρησιμοποιούνται στην εγκληματολογική έρευνα, στον έλεγχο ποινικού μητρώου, στον έλεγχο ακεραιότητας διαβατηρίου και στην ασφάλεια των συνόρων.

Η βιομετρία χρησιμοποιείται σε διάφορους κλάδους, συμπεριλαμβανομένων των κυβερνητικών και αρχών επιβολής του νόμου, του εμπορίου και του λιανικού εμπορίου, της υγειονομικής περίθαλψης, των ταξιδιών και της μετανάστευσης, των χρηματοοικονομικών και τραπεζών κ.λπ.

Οι κυβερνητικές εφαρμογές αφορούν εθνικές ταυτότητες, διαβατήρια, άδειες οδήγησης, κάρτες κοινωνικής ασφάλισης, εγγραφή ψηφοφόρων, εγγραφή κοινωνικής πρόνοιας κ.λπ. Οι τεχνολογίες χρησιμοποιούνται ως ενίσχυση ή αντικατάσταση ορισμένων αυτών των κρίσιμων διαδικασιών.

Πολλαπλά βιομετρικά στοιχεία, συνδυασμένα μεταξύ τους για να προσφέρουν βελτιωμένη ακρίβεια και ευρωστία, χρησιμοποιούνται για την ασφάλεια περιορισμένων περιοχών σε αεροδρόμια, εγκαταστάσεις εθνικής ασφάλειας κ.λπ.

Με τη δραματική βελτίωση των υπολογιστικών δυνατοτήτων και την πρόοδο που έχει σημειωθεί στην ανάπτυξη έξυπνων αισθητήρων, το τοπίο της βιομετρικής τεχνολογίας είναι επίσης κίνητρο για μετατόπιση από τα συστήματα που βασίζονται κυρίως στο υλικό προς σε λύσεις βασισμένες σε λογισμικό που χρησιμοποιούν smartphone και υπολογιστικό νέφος.

Συνοψίζοντας η βιομετρία έχει τρεις βασικές λειτουργικότητες, [1]:

- Επαλήθευση: Με βάση τα βιομετρικά δεδομένα που είναι αποθηκευμένα στους διακομιστές, η τεχνολογία μπορεί, με υψηλή βεβαιότητα, να επαληθεύσει μια διεκδικούμενη επαλήθευση εγγραφής.

- Αναγνώριση: Με βάση τα βιομετρικά δεδομένα το βιομετρικό σύστημα καθορίζει αν το άτομο είναι μέσα ή όχι στη βάση δεδομένων. Μπορεί να υπάρχουν εκατομμύρια εγγεγραμμένες ταυτότητες στη βάση δεδομένων. Το σύστημα ελέγχει τα βιομετρικά δεδομένα και τι αποθηκεύεται για να εντοπίσει αν υπάρχει συσχέτιση.
- Επιτήρηση: Οι υπηρεσίες ελέγχου μπορούν να χρησιμοποιηθούν ως ασφάλεια σε δημόσιες συγκεντρώσεις, ασφάλεια αεροδρομίου και άλλες δραστηριότητες επιτήρησης.

3.5 ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ

Μεταξύ των καθιερωμένων λύσεων φυσιολογικής βιομετρίας, με μεγάλους πληθυσμούς χρηστών, είναι το δακτυλικό αποτύπωμα, η αναγνώριση ίριδας, η αναγνώριση προσώπου, η γεωμετρία χεριού, η αναγνώριση φλέβας, η αναγνώριση υπογραφής και η αναγνώριση αποτυπωμάτων παλάμης.

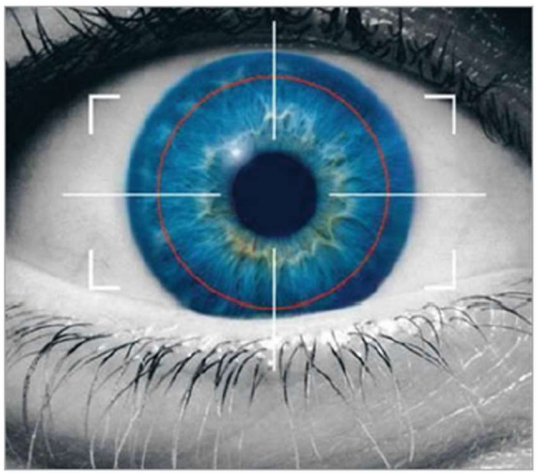
Οι καθιερωμένες λύσεις συμπεριφοράς περιλαμβάνουν την αναγνώριση φωνής και τη δυναμική αναγνώριση υπογραφών.

Εκτός από τις προαναφερθείσες τεχνολογίες, υπάρχουν αρκετές αναδυόμενες βιομετρικές λύσεις, όπως η αναγνώριση οσμής σώματος, μοτίβου αυτιών και αποτυπωμάτων χειλιών στη φυσιολογική κατηγορία καθώς και ταχύτητα πληκτρολόγησης, ή οθόνης αφής, δυναμική ποντικιού, στυλομετρία και αναγνώριση βάδισης στην κατηγορία συμπεριφοράς. Στην αγορά έχουν κυκλοφορήσει αρκετά προϊόντα που σχετίζονται με αυτές τις τεχνολογίες που καλύπτουν μια ποικιλία βιομηχανιών όπως ο τραπεζικός και ο χρηματοοικονομικός τομέας, ο διαδικτυακός εντοπισμός απάτης, η υγειονομική περίθαλψη κ.λπ., [11], [31]. Στις επόμενες υποενότητες αναλύονται περαιτέρω οι προαναφερθείσες τεχνολογίες πιστοποίησης ταυτότητας, [15].

3.5.1 Μάτια

Αναγνώριση ίριδας: Η ίριδα (Σχήμα 2) αντιπροσωπεύει μια πολύ αξιόλογη βιομετρική λύση για έλεγχο ταυτότητας, επειδή είναι μικρή (11 mm), η αναγνώριση ως αναζήτηση αντιστοιχίας από τη βάση δεδομένων είναι γρήγορη, είναι ευδιάκριτη, σταθερή με την πάροδο του χρόνου, δεν είναι εξαρτάται από τη γωνία φωτισμού και το χαρακτηριστικό δακτυλιοειδές σχήμα του διευκολύνει την αξιόπιστη και ακριβή απομόνωση αυτού. Τα κύρια βήματα για το σύστημα αναγνώρισης ίριδας είναι, [31]:

1. Χρησιμοποιώντας μια κάμερα, το μάτι αποτυπώνεται.
2. Η εικόνα στη συνέχεια επεξεργάζεται, έτσι ώστε να απομονωθεί η ίριδα ανιχνεύοντας τα όριά της (κόρη, βλεφαρίδα και βλέφαρα).
3. Αποδιαμόρφωση του κώδικα ίριδας.
4. Σύγκριση με λογικό XOR δύο κωδικών ίριδας.



Σχήμα 2: Ίριδα ματιού.

Η ίριδα θεωρείται ως ένα από τα πιο ακριβή βιομετρικά δεδομένα. Παρά την ήδη ισχυρή ακρίβειά της, οι ερευνητές εργάζονται ενεργά για να ενσωματώσουν την τελευταία λέξη της τεχνολογίας στη βιομετρική αναγνώριση ίριδας, βελτιώνοντας τις τεχνικές παρακολούθησης και εντοπισμού ίριδας και άλλες πτυχές των τεχνικών απόκτησης και προεπεξεργασίας δεδομένων καθώς και των αλγορίθμων αντιστοίχισης, αντιμετωπίζοντας προκλήσεις που σχετίζονται με μη παραδοσιακές πλατφόρμες όπως τα smartphone.

Έλεγχος ταυτότητας αμφιβληστροειδούς: ο έλεγχος ταυτότητας βασίζεται στα αιμοφόρα αγγεία του αμφιβληστροειδή του ματιού, τα οποία έχουν μοναδικά μοτίβα που μπορούν να χρησιμοποιηθούν για την αναγνώριση ενός ατόμου. Δεδομένου ότι τα αιμοφόρα αγγεία βρίσκονται στο πίσω μέρος του ματιού, η σάρωση αμφιβληστροειδούς απαιτεί τη χρήση φωτός χαμηλής έντασης πριν από τη φωτογράφηση και την ανάλυσή του.

Ο αμφιβληστροειδής χιτώνας παραμένει αμετάβλητος καθ' όλη τη διάρκεια της ανθρώπινης ζωής. Σε αντίθεση με την ίριδα, η βιομετρία του αμφιβληστροειδούς θεωρείται επεμβατική και απαιτεί πολύ κοντινή απόσταση από την κάμερα για σωστή σάρωση. Οι συσκευές

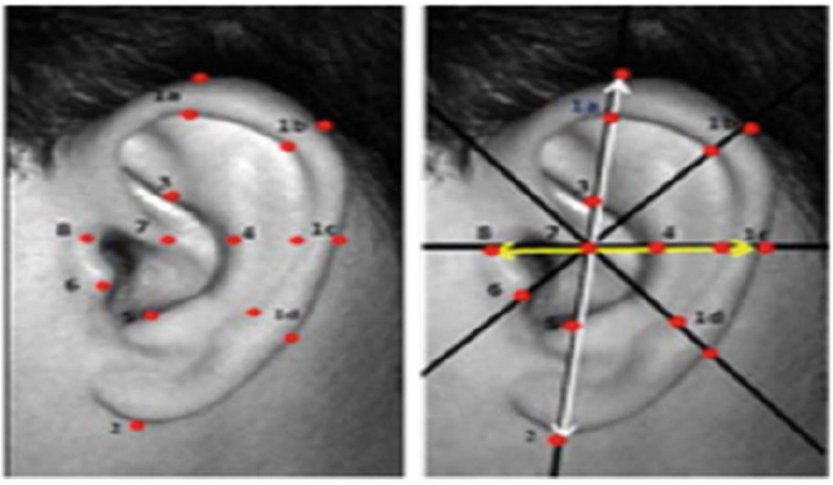
σάρωσης αμφιβληστροειδούς χρησιμοποιούνται για εφαρμογές φυσικής πρόσβασης σε περιβάλλοντα που έχουν αυστηρές απαιτήσεις ασφάλειας, π.χ. για την εθνική ασφάλεια και στις στρατιωτικές εγκαταστάσεις.

3.5.2 Αυτιά

Ο έλεγχος ταυτότητας αυτιού έχει περισσότερα πλεονεκτήματα από την αναγνώριση προσώπου, καθώς αλλάζει ελάχιστα με το χρόνο και επομένως θεωρείται πιο σταθερό από το πρόσωπο. Η διαδικασία ελέγχου ταυτότητας γενικά γίνεται σε πέντε στάδια, [33]:

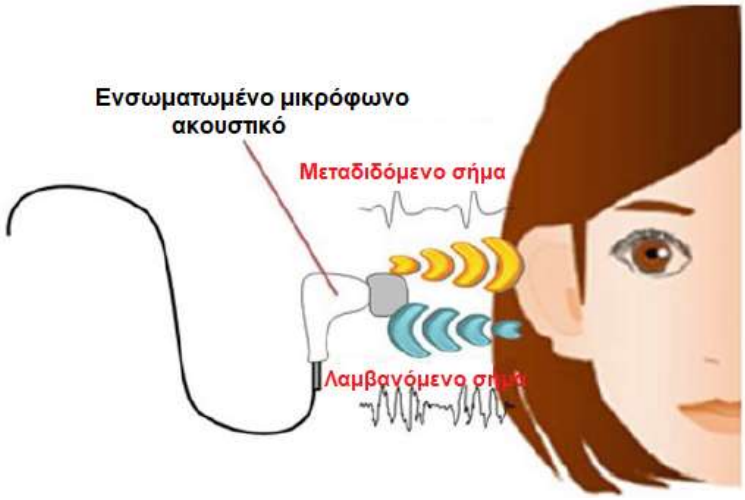
1. Ανίχνευση αυτιού: περιλαμβάνει τον εντοπισμό της θέσης του αυτιού σε μια εικόνα.
2. Ομαλοποίηση και βελτίωση αυτιού: το ανιχνευμένο τμήμα (αυτί) έχει ενισχυθεί από άποψη πιστότητας και μπορεί να υποβληθεί σε γεωμετρική ή φωτομετρική διόρθωση.
3. Εξαγωγή χαρακτηριστικών: το τμηματοποιημένο αυτί ανάγεται σε ένα μαθηματικό μοντέλο (π.χ. διάνυσμα χαρακτηριστικών) που συνοψίζει τις πληροφορίες που προκαλούν τη διακριτότητα.
4. Αντιστοίχιση: τα χαρακτηριστικά που εξάγονται πρέπει να συγκριθούν με τα χαρακτηριστικά που είναι αποθηκευμένα στη βάση δεδομένων.
5. Απόφαση: μετά την αντιστοίχιση, η απόφαση καθορίζεται ως (ναι) ή ως (όχι).

Αυτή η μέθοδος ελέγχου ταυτότητας βασίζεται στη γεωγραφία του αυτιού και η απεικόνιση μπορεί να είναι είτε 2D (Σχήμα 3) είτε 3D.



Σχήμα 3: Βιομετρία αυτιού, πιστοποίηση με βάση τη γεωμετρία.

Ένας άλλος τύπος ελέγχου ταυτότητας αυτιού, ο οποίος βασίζεται στη χρήση ακουστικών κυμάτων για τη διάκριση του μοναδικού σχήματος κοιλότητας του αυτιού, έχει αναπτυχθεί από την NEC Corporation, στην Ιαπωνία. Η τεχνολογία αυτή χρησιμοποιεί ακουστικά με ενσωματωμένο μικρόφωνο για να στέλνει και να λαμβάνει ήχους κυμάτων και να εξάγει χαρακτηριστικά από τα λαμβανόμενα σήματα που είναι μοναδικά για κάθε άτομο με βάση τη μοναδική δομή του αυτιού (Σχήμα 4).



Σχήμα 4: Βιομετρία αυτιού, πιστοποίηση με βάση ακουστικά κύματα.

Το ακουστικό χρησιμοποιείται για την εξάλειψη του θορύβου και για τη διασφάλιση φυσικού ελέγχου ταυτότητας ακόμα και ο χρήστης κινείται ή εργάζεται.

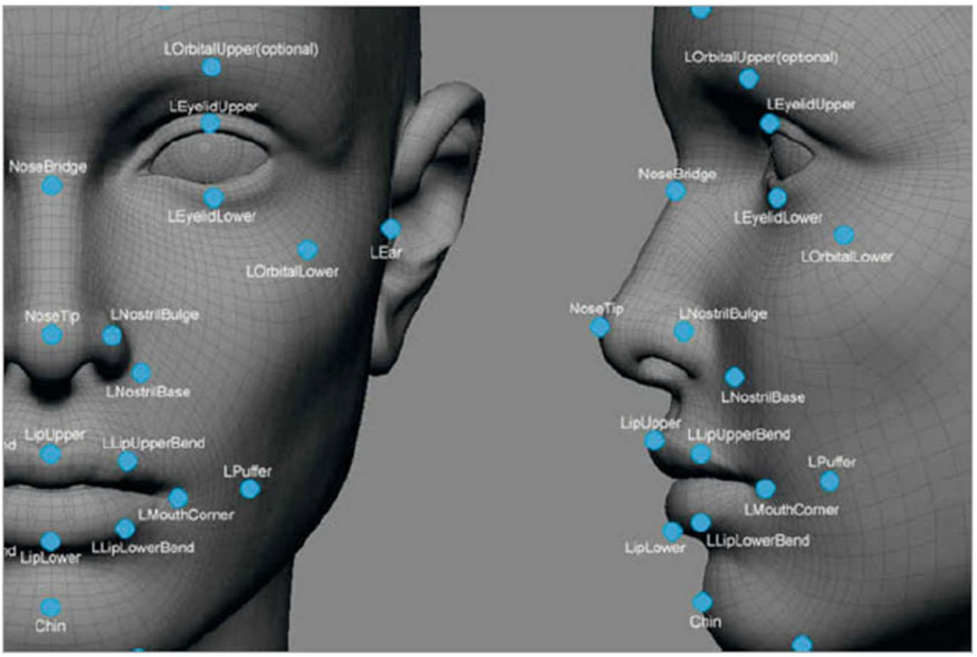
3.5.3 Αναγνώριση προσώπου

Οι άνθρωποι χρησιμοποιούν τις εικόνες του προσώπου ως έναν κοινό τρόπο αναγνώρισης και διάκρισης των ατόμων μεταξύ τους. Επομένως, η εικόνα του προσώπου είναι μία από τις πιο κοινές βιομετρικές μεθόδους για την αναγνώριση ατόμου. Τα βιομετρικά χαρακτηριστικά του προσώπου περιλαμβάνουν τη θέση και το σχήμα των χαρακτηριστικών του προσώπου όπως τα φρύδια, η μύτη, τα μάτια, τα χείλη, η γραμμή της γνάθου και το πηγούνι. Οι λειτουργίες βιομετρίας προσώπου χωρίζονται σε στατικές ως λήψεις εικόνας και σε δυναμικές ως μη ελεγχόμενη αναγνώριση προσώπου στο αεροδρόμιο.

Ο έλεγχος ταυτότητας προσώπου εξακολουθεί να είναι αποτελεί ένα δύσκολο πρόβλημα. Αυτό οφείλεται στη μεταβλητότητα των ανθρώπινων προσώπων κάτω από διαφορετικές συνθήκες

όπως φωτισμό, περιστροφή, εκφράσεις, οπτική γωνία κάμερας, γήρανση, μακιγιάζ και γυαλιά. Η μέθοδος αναγνώρισης προσώπου ταξινομείται σε δύο είδη:

- Μέθοδοι βασισμένες σε χαρακτηριστικά.
- Μέθοδοι που βασίζονται στην εμφάνιση.



Σχήμα 5: Πιστοποίηση με βιομετρία προσώπου.

Οι τεχνικές αναγνώρισης προσώπου μπορεί να είναι είτε 2D (Σχήμα 5) είτε 3D και χρησιμοποιούν ιδιότητες και γεωμετρικές σχέσεις όπως οι περιοχές, οι αποστάσεις και οι γωνίες μεταξύ των σημείων χαρακτηριστικών του προσώπου όπως τα μάτια, η μύτη και το στόμα.

Η βιομετρία προσώπου δεν απαιτεί φυσική επαφή με τη συσκευή λήψης (δηλαδή, την κάμερα), και αυτό την καθιστά εύκολη στη χρήση. Χρησιμοποιείται επίσης ευρέως αν και δεν παρουσιάζει πολλά μοναδικά χαρακτηριστικά όπως τα βιομετρικά στοιχεία ματιών στην αναγνώριση ίριδας. Η αναγνώριση προσώπου εμποδίζεται από το γεγονός ότι η φυσιογνωμία αλλάζει με την ηλικία, και τα χαρακτηριστικά αλλά και η έκφραση του προσώπου μπορούν να παραποιηθούν σκόπιμα, [31].

3.5.4 Θερμογραφήματα προσώπου

Ο οπτικός έλεγχος ταυτότητας προσώπου αντιμετωπίζει το πρόβλημα του φωτισμού, της αλλαγής στάσης και προσανατολισμού. Αυτοί είναι οι λόγοι για τους οποίους αναπτύσσονται νέες τεχνικές για την αναγνώριση προσώπου γνωστές ως θερμογράμματα προσώπου (Σχήμα 6) που σχηματίζονται από τη θερμότητα που εκπέμπεται από το πρόσωπο και επηρεάζονται λιγότερο από την ανάπτυξη του προσώπου, τη στάση και τις εκφράσεις. Η θερμογραφία προσώπου λειτουργεί ανιχνεύοντας μοτίβα θερμότητας που δημιουργούνται από τη διακλάδωση των αιμοφόρων αγγείων που εκπέμπονται από το δέρμα. Αυτά τα μοτίβα, γνωστά ως θερμογράμματα, είναι εξαιρετικά μοναδικά· ακόμα και τα πανομοιότυπα δίδυμα έχουν διαφορετικά θερμογράμματα.

Σχήμα 6: Πιστοποίηση με θερμογραφήματα προσώπου.

Η τεχνολογία περιλαμβάνει τη χρήση δεδομένων βιοαισθητήρα για τη μοναδική και αυτόματη αναγνώριση ατόμων. Λόγω της συνδεσιμότητας των φυσιολογικών συστημάτων του ανθρώπινου σώματος, τα βασικά σχήματα μπορούν γενικά να προκύψουν από οποιαδήποτε δεδομένα βιολογικών αισθητήρων που μπορούν να παρουσιαστούν ως εικόνα. Τα στοιχειώδη σχήματα και οι τοποθεσίες τους παρέχουν μια ικανότητα αναγνώρισης.

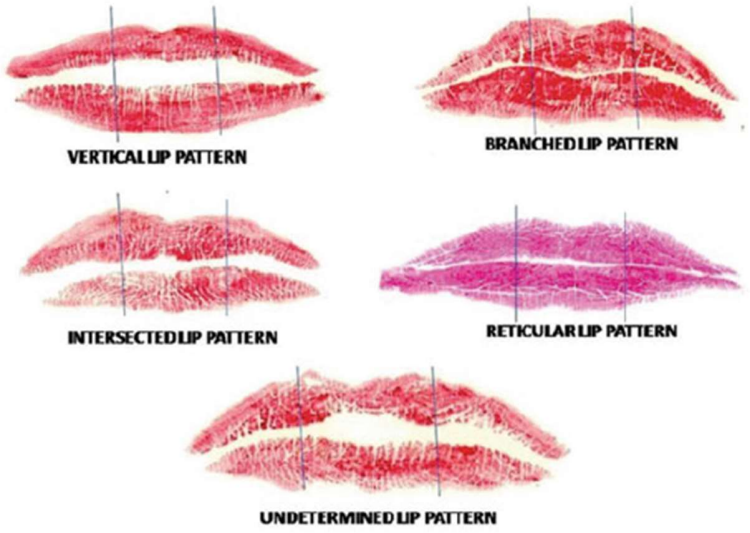
Οι βιοαισθητήρες που παράγουν πολύ λεπτομερή εντοπισμένα δεδομένα, όπως συσκευές απεικόνισης υπέρυθρων υψηλής ανάλυσης, μπορούν να οδηγήσουν σε μοναδική αναγνώριση ενός ατόμου από τον προσδιορισμό των βασικών σχημάτων και την κατανομή τους.

Τα θερμογράμματα ως μηχανισμός βιομετρικής ταυτοποίησης έχουν το πλεονέκτημα ότι αυτή η τεχνολογία δεν είναι παρεμβατική. Αν και δεν χρησιμοποιείται ευρέως, η ηλεκτρονική

θερμογραφία χρησιμοποιείται όλο και περισσότερο ως μη ιονίζουσα, μη επεμβατική εναλλακτική λύση για ιατρικές διαγνώσεις. Πιστεύεται ότι οι εκπομπές αγγειακής θερμότητας που υπάρχουν στο ανθρώπινο πρόσωπο μπορούν να παρέχουν φυσιολογικούς δείκτες για την υγεία ή ασθένεια του χρήστη. Η γενική θερμογραφία έχει χρησιμοποιηθεί στην προσπάθεια διάγνωσης των καρκίνων του μαστού, καθώς η αποτελεσματικότητα της χρήσης της τεχνολογίας για αυτόν τον σκοπό έχει αμφισβητηθεί επιστημονικά, [34].

3.5.5 Βιομετρία χειλιών

Το αποτύπωμα των χειλιών διαφέρει από άτομο σε άτομο, επομένως μπορεί να χρησιμοποιηθεί για την αναγνώριση ενός ατόμου, με τα μοναδικά του χαρακτηριστικά που σχηματίζονται από τις γραμμές, τις ρυτίδες, τις σχισμές, τις αυλακώσεις, το χρώμα και το σχήμα (Σχήμα 7).



Σχήμα 7: Μοτίβα χειλιών.

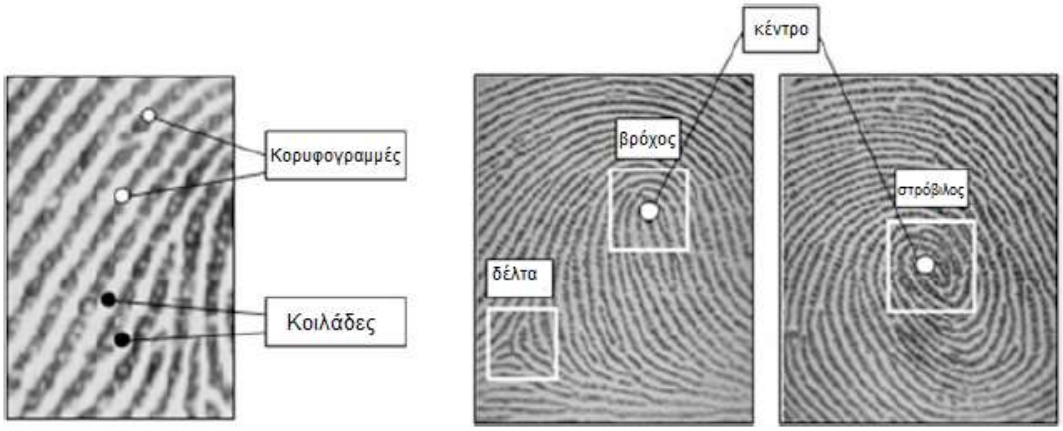
Η βιομετρία χειλιών δεν έχει χρησιμοποιηθεί ευρέως όπως άλλα βιομετρικά συστήματα από την ανθρώπινη φυσιολογία, όπως το δακτυλικό αποτύπωμα, το πρόσωπο ή η φωνή. Ως εκ τούτου, οι έρευνες βρίσκονται ακόμη σε πολύ πρώιμο στάδιο στον τομέα αυτό. Ενώ η ιδέα της χρήσης αποτυπωμάτων χειλιών ως αναγνώριση για τον άνθρωπο προτάθηκε για πρώτη φορά τη δεκαετία του 1950, μόλις στη δεκαετία του 1990 οι ερευνητές άρχισαν να εξερευνούν τη δυνατότητα μιας τέτοιας τεχνολογίας. Το 1998, ο Wark και ο Sridharan πρότειναν έναν νέο τύπο εξαγωγής βιομετρικών χαρακτηριστικών χειλιών για την αναγνώριση των ομιλητή.

Τα οπτικά χαρακτηριστικά των χειλιών χωρίζονται σε τρεις κατηγορίες, οι οποίες είναι χαρακτηριστικά που βασίζονται στο σχήμα, χαρακτηριστικά που βασίζονται στην εμφάνιση και συνδυασμός και των δύο προηγούμενων κατηγοριών χαρακτηριστικών.

Έχουν προταθεί διαφορετικές μέθοδοι για εξέταση των χειλιών. Αυτές οι μέθοδοι χρησιμοποιούν στατιστικές αναλύσεις, μετασχηματισμό Hough, αναλύσεις σχήματος χειλιών, δυναμική στρέβλωση χρόνου, τμηματοποίηση δομών κελιών και συντελεστές ομοιότητας, [31].

3.5.6 Βιομετρία δαχτυλικού αποτυπώματος

Κάθε άτομο έχει ένα μοναδικό δακτυλικό αποτύπωμα, επομένως η χρήση του δακτυλικού αποτυπώματος για έλεγχο ταυτότητας έχει υιοθετηθεί ευρέως πλέον. Το δακτυλικό αποτύπωμα έχει τρία μοτίβα: βρόχο, δέλτα και στρόβιλο, άλλα χαρακτηριστικά όπως οι κοιλάδες, οι κορυφογραμμές και οι μικρολεπτομέρειες που αναφέρονται στους διάφορους τρόπους με τους οποίους οι κορυφογραμμές μπορούν να είναι ασυνεχείς (τερματισμός και διακλάδωση). Οι λεπτομέρειες είναι ένα βασικό χαρακτηριστικό για την αναγνώριση (αυθεντικοποίηση) των ατόμων (Σχήμα 8).



Σχήμα 8: Δακτυλικό αποτύπωμα.

Το δακτυλικό αποτύπωμα θεωρείται το πιο χρησιμοποιούμενο βιομετρικό σύστημα για πολλούς λόγους: Πρώτον, είναι η πιο οικεία μέθοδος για τους περισσότερους χρήστες και είναι απλό στη χρήση. Επιπλέον, η υλοποίηση, η εγκατάσταση και η συντήρηση συστημάτων δακτυλικών αποτυπωμάτων πιο εύκολες. Στα μειονεκτήματά του συγκαταλέγονται η ευαισθησία του συστήματος σε περιβαλλοντολογικούς παράγοντες και η παρεμβατικότητα που έχει για να παραβιαστεί.

Οι περισσότερες από τις πρόσφατες εργασίες για τα βιομετρικά συστήματα δακτυλικών αποτυπωμάτων έχουν επικεντρωθεί στη βελτίωση της ακρίβειας των συστημάτων αναγνώρισης μέσω της βελτίωσης των τεχνικών επεξεργασίας δεδομένων και των μεθόδων και αλγορίθμων αντιστοίχισης.

Υπάρχουν τέσσερις κύριοι τύποι υλικού ανάγνωσης δακτυλικών αποτυπωμάτων, [35]:

- Οι οπτικοί αναγνώστες είναι ο πιο κοινός τύπος συσκευών ανάγνωσης δακτυλικών αποτυπωμάτων. Ο τύπος του αισθητήρα σε έναν οπτικό αναγνώστη είναι μια ψηφιακή κάμερα που αποκτά μια οπτική εικόνα του δακτυλικού αποτυπώματος. Τα πλεονεκτήματά τους είναι ότι οι οπτικοί αναγνώστες ξεκινούν από πολύ χαμηλές τιμές. Τα μειονεκτήματα είναι ότι οι μετρήσεις επηρεάζονται από βρώμικα ή σημαδεμένα δάχτυλα και αυτός ο τύπος συσκευής ανάγνωσης δακτυλικών αποτυπωμάτων είναι πιο εύκολο να ξεγελαστεί από άλλους.

- Οι χωρητικές συσκευές ανάγνωσης, που αναφέρονται επίσης ως αναγνώστες CMOS, δε διαβάζουν το δακτυλικό αποτύπωμα χρησιμοποιώντας φως. Αντίθετα, ένας αναγνώστης CMOS χρησιμοποιεί πυκνωτές και επομένως ηλεκτρικό ρεύμα για να σχηματίσει μια εικόνα του δακτυλικού αποτυπώματος. Οι αναγνώστες CMOS είναι πιο ακριβοί από τους οπτικούς αναγνώστες, αν και εξακολουθούν να είναι σχετικά φθηνοί με τιμές που ξεκινούν το λιγότερο στα 100 ευρώ.Ένα σημαντικό πλεονέκτημα των χωρητικών αναγνωστών έναντι των οπτικών αναγνωστών είναι ότι ένας χωρητικός αναγνώστης απαιτεί ένα πραγματικό σχήμα δακτυλικών αποτυπωμάτων και όχι μόνο μια οπτική εικόνα. Αυτό κάνει τους αναγνώστες CMOS πιο δύσκολο να εξαπατηθούν.

- Οι συσκευές ανάγνωσης υπερήχων είναι ο πιο πρόσφατος τύπος συσκευών ανάγνωσης δακτυλικών αποτυπωμάτων, και χρησιμοποιούν ηχητικά κύματα υψηλής συχνότητας για να διεισδύσουν στο επιδερμικό (εξωτερικό) στρώμα του δέρματος. Διαβάζουν το δακτυλικό αποτύπωμα στο στρώμα του δέρματος, το οποίο εξαλείφει την ανάγκη για μια καθαρή, χωρίς ουλές επιφάνεια. Όλοι οι άλλοι τύποι συσκευών ανάγνωσης δακτυλικών αποτυπωμάτων αποκτούν μια εικόνα της εξωτερικής επιφάνειας, απαιτώντας έτσι τα χέρια να καθαρίζονται και να απαλλαγούν από ουλές πριν από την ανάγνωση. Αυτός ο τύπος συσκευής ανάγνωσης δακτυλικών αποτυπωμάτων είναι πολύ πιο ακριβός από τους δύο

προηγούμενους, ωστόσο λόγω της ακρίβειάς τους και του γεγονότος ότι είναι δύσκολο να ξεγελαστούν οι συσκευές ανάγνωσης υπερήχων είναι ήδη πολύ δημοφιλείς.

- Οι θερμικοί αναγνώστες αντιλαμβάνονται, σε μια επιφάνεια επαφής, τη διαφορά θερμοκρασίας μεταξύ των κορυφών και των κοιλάδων δακτυλικών αποτυπωμάτων. Οι θερμικοί αναγνώστες δακτυλικών αποτυπωμάτων έχουν μια σειρά από μειονεκτήματα, όπως υψηλότερη κατανάλωση ενέργειας και απόδοση που εξαρτάται από τη θερμοκρασία περιβάλλοντος.

Μετά τη λήψη μιας εικόνας δακτυλικού αποτυπώματος από το υλικό της συσκευής ανάγνωσης δακτυλικών αποτυπωμάτων, αυτό το δακτυλικό αποτύπωμα πρέπει να ερμηνευτεί. Θα πρέπει να υποβληθεί σε επεξεργασία με τέτοιο τρόπο ώστε οι αναγνώσεις να μπορούν να συγκριθούν αποτελεσματικά και να αντιστοιχιστούν μεταξύ τους.

Γενικά υπάρχουν δύο τύποι λογισμικού αντιστοίχισης:

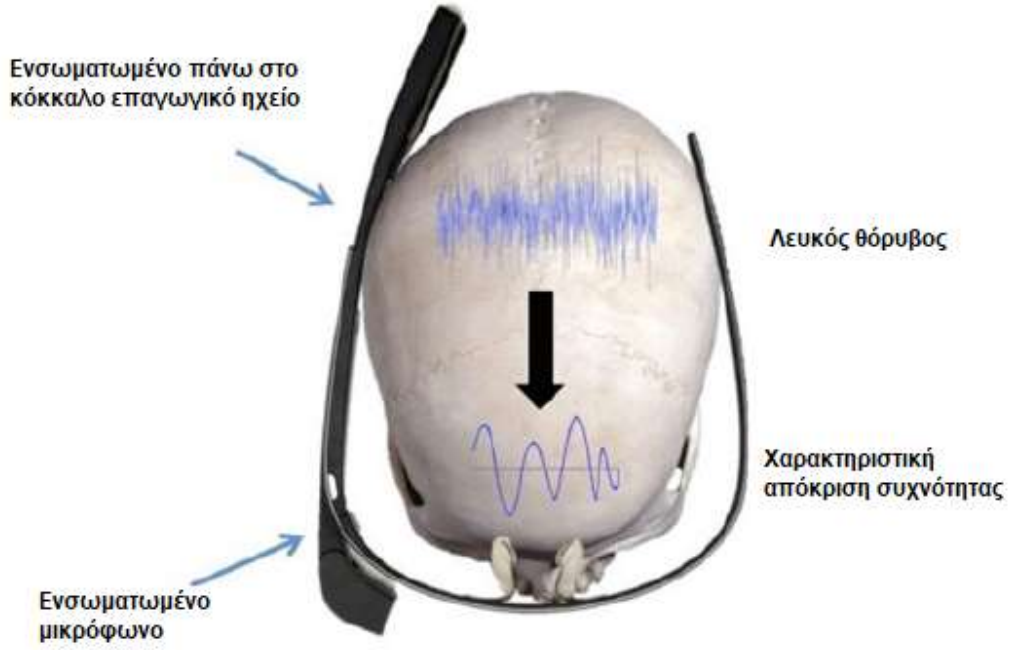
- Η αντιστοίχιση μικροσκοπικών σημείων βασίζεται στην αναγνώριση των μικρολεπτομερειών, αυτή είναι η πιο ευρέως χρησιμοποιούμενη τεχνική.
- Η αντιστοίχιση μοτίβων απλώς συγκρίνει δύο εικόνες για να δει πόσο όμοιες είναι, που χρησιμοποιούνται συχνά σε συστήματα δακτυλικών αποτυπωμάτων για τον εντοπισμό διπλότυπων.

3.5.7 Νύχι

Ορισμένες εφαρμογές απαιτούν ασφαλή βραχυπρόθεσμο έλεγχο ταυτότητας και συνιστάται η χρήση βιομετρικών λύσεων. Όπως αναφέρθηκε, βιομετρικά χαρακτηριστικά όπως ο αμφιβληστροειδής, η ίριδα ή το δακτυλικό αποτύπωμα θεωρούνται μόνιμα χαρακτηριστικά ενός ατόμου. Όμως οι άνθρωποι πιθανότατα θα είχαν αντίρρηση να αποθηκεύονται οι βιομετρικές τους παράμετροι για μη κρίσιμες εφαρμογές που χρησιμοποιούν προσωρινά. Γι' αυτό το λόγο, δημιουργήθηκε η προσωρινή βιομετρική λύση που περιλαμβάνει τη χρήση βιομετρικών χαρακτηριστικών που θα άλλαζαν φυσικά μετά από μια χρονική περίοδο, όπως τα νύχια των χεριών που θα άλλαζαν σε 3-6 μήνες. Το μοναδικό στρώμα νυχιών, το σχήμα, το χρώμα, τα όρια, οι γρατσουνιές, οι λευκές κουκκίδες και η υφή των νυχιών χρησιμοποιούνται για τη δημιουργία μιας μοναδικής υπογραφής που μπορεί να χρησιμοποιηθεί για τον έλεγχο ταυτότητας, [36].

3.5.8 Κρανίο

Ο έλεγχος ταυτότητας κρανίου μπορεί να γίνει είτε με απεικόνιση (2D, 3D) όπου επιλέγεται ένα σύνολο σημείων και συγκρίνεται για την αναγνώριση ενός ατόμου είτε με χρήση ηχητικών κυμάτων, όπως στην πιο πρόσφατη έρευνα SkullConduct (Σχήμα 9) που στέλνει ηχητικά κύματα (δόνηση) με μια συγκεκριμένη συχνότητα στο κρανίο και καταγράφει τα ανακλόμενα κύματα για την αναγνώριση ενός ατόμου.



Σχήμα 9: SkullConduct: μια λύση πιστοποίησης κρανίου.

Η εγκατάσταση του "SkullConduct" εκπονήθηκε από ερευνητές πανεπιστημίου στη Γερμανία πάνω σε ένα τροποποιημένο ζεύγος γυαλιών Google. Χρησιμοποιώντας το ενσωματωμένο ηχείο οστικής αγωγιμότητας και το μικρόφωνο, η συσκευή έπαιζε έναν ανεπαίσθητο ήχο που στη συνέχεια ανιχνεύθηκε από το μικρόφωνο. Στα πειράματα που έγιναν αναγνωρίστηκε σωστά ο χρήστης στο 97 τοις εκατό των περιπτώσεων, [37].

3.5.9 Πιστοποίηση κυμάτων εγκεφάλου

Μελέτες έχουν δείξει ότι τα άτομα παρουσιάζουν μοναδικά μοτίβα εγκεφάλου για παρόμοιες εργασίες και αυτά τα μοναδικά μοτίβα μπορούν να χρησιμοποιηθούν ως υπογραφές για βιομετρικό έλεγχο ταυτότητας. Τα μοτίβα αυτά είναι ηλεκτρικές δραστηριότητες που παράγονται από δομές του εγκεφάλου και μετρώνται με το ηλεκτροεγκεφαλογράφημα. Ο έλεγχος ταυτότητας γίνεται

όταν το άτομο κάνει μια συγκεκριμένη εργασία που απαιτεί σκέψη (το ίδιο έκανε όταν πήρε την ταυτότητά του από το σύστημα) και αυτή η εργασία μπορεί να είναι ανάγνωση, πολλαπλασιασμός, κ.λπ., και το ηλεκτροεγκεφαλογράφημα μετρά την ηλεκτρική δραστηριότητα του εγκεφάλου και τη συγκρίνει με την αποθηκευμένη υπογραφή για να αποδεχτεί ή να απορρίψει το άτομο. Σύμφωνα με τον Benarous [12], αυτός ο τύπος ελέγχου ταυτότητας είναι νέος και παρουσιάζει πολλά πλεονεκτήματα:

- Εμπιστευτικότητα (νοητικές εργασίες).
- Δύσκολο να μιμηθεί (κάθε άτομο έχει ένα μοναδικό μοτίβο).
- Αδύνατη η κλοπή (τα άτομα εκπέμπουν διαφορετικά εγκεφαλικά μοτίβα όταν βρίσκονται υπό άγχος, απειλή ή αλλαγή διάθεσης).

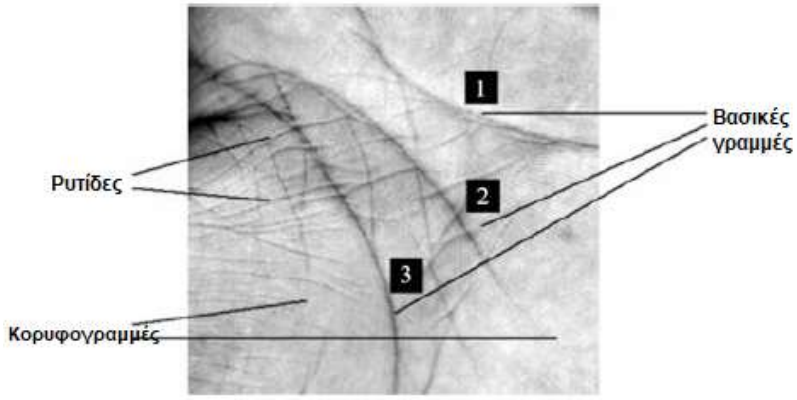
3.5.10 Οσμή σώματος

Οι οσμές του σώματος μπορούν να ταξινομηθούν σε τρία επίπεδα ή τύπους: το πρώτο περιέχει συστατικά που είναι σταθερά με την πάροδο του χρόνου ανεξάρτητα από τη διατροφή ή τους περιβαλλοντικούς παράγοντες, το δεύτερο περιέχει συστατικά που υπάρχουν λόγω της διατροφής και των περιβαλλοντικών παραγόντων και το τρίτο περιέχει συστατικά που υπάρχουν λόγω της επιρροής εξωτερικών πηγών, όπως τα αρώματα. Ο πρώτος τύπος οσμής είναι μοναδικός για κάθε άτομο και χρησιμοποιείται στον έλεγχο ταυτότητας που χρησιμοποιεί ηλεκτρονικό θόρυβο για την αναγνώριση της οσμής και των ατόμων.

Η αναγνώριση οσμών σώματος είναι μια φυσική βιομετρική τεχνολογία χωρίς επαφή, που επιχειρεί να αναγνωρίσει άτομα αναλύοντας και μελετώντας τις οσφρητικές ιδιότητες του αρώματος του σώματός τους. Εφαρμόζονται ειδικοί αισθητήρες για να συλλάβουν τη μυρωδιά του ανθρώπου παίρνοντας την οσμή από μη παρεμβατικά μέρη του σώματος, όπως το πίσω μέρος του χεριού, [31].

3.5.11 Αποτύπωμα παλάμης

Ο έλεγχος ταυτότητας με το αποτύπωμα της παλάμης είναι μια βιομετρική τεχνολογία που βασίζεται στο χέρι. Η παλάμη καλύπτεται από το ίδιο δέρμα με τις άκρες των δακτύλων και χρησιμοποιείται για την μοναδική αναγνώριση ενός ατόμου.



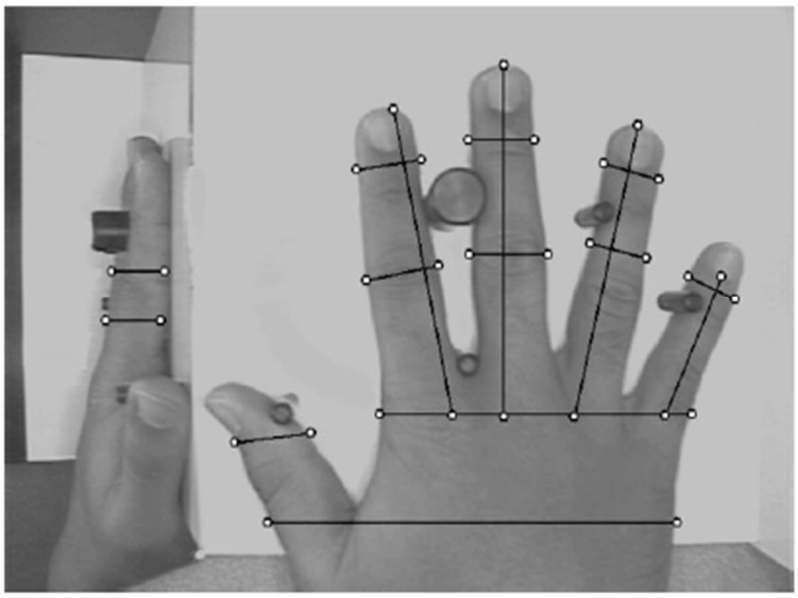
Σχήμα 10: Πιστοποίηση με βιομετρία αποτυπώματος παλάμης.

Σύμφωνα με τον Benarous [12], η παλάμη έχει ένα σύνολο μοναδικών χαρακτηριστικών (Σχήμα 10) που μπορούν να χρησιμοποιηθούν για τον έλεγχο ταυτότητας ενός ατόμου, όπως:

- Σχήμα παλάμης (χαρακτηριστικό γεωμετρίας).
- Μορφή και θέση των βασικών γραμμών (χαρακτηριστικό γραμμής).
- Ρυτίδες που είναι οι πιο λεπτές ακανόνιστες γραμμές (χαρακτηριστικό ρυτίδων).
- Χαρακτηριστικά σημείου δέλτα στη ρίζα των δακτύλων.
- Χαρακτηριστικές μικρολεπτομέρειες.

3.5.12 Γεωμετρία χεριού

Αυτή η τεχνική μετρά την επιφάνεια της παλάμης, το μήκος, το πλάτος και το σχήμα, το μέγεθος και το σχήμα των δακτύλων και υπολογίζει τις αποστάσεις μεταξύ ενός συνόλου σημείων προκειμένου να εξάγει τα μοναδικά χαρακτηριστικά του χεριού (Σχήμα 11).



Σχήμα 11: Λύση βασισμένη στη γεωμετρία του χεριού.

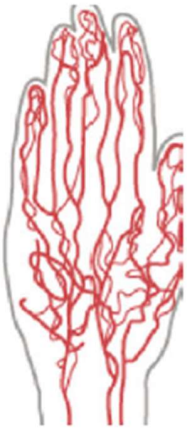
Αυτή η μέθοδος δεν είναι ευαίσθητη σε αλλαγές στα χαρακτηριστικά της επιφάνειας όπως τατουάζ, μαλλιά, κοψίματα, γρατζουνιές, εγκαύματα ή βρωμιά. Ωστόσο, δεν αποδίδει καλά εάν υπάρχουν μεγάλοι επίδεσμοι ή γύψοι στα δάχτυλα, όταν το χέρι έχει παραμορφωθεί σημαντικά ή όταν λείπει ένα δάχτυλο.

Σε αντίθεση με άλλες παραδοσιακές φυσιολογικές βιομετρικές τεχνολογίες (π.χ. δακτυλικό αποτύπωμα, ίριδα), η ακρίβεια της γεωμετρίας του χεριού ήταν μέχρι στιγμής σχετικά χαμηλή. Ως εκ τούτου, οι περισσότερες από τις ερευνητικές προσπάθειες έχουν στοχεύσει στη βελτίωση της ακρίβειας ανίχνευσης αυτού του χαρακτηριστικού, με την επέκταση του χώρου χαρακτηριστικών και την εξερεύνηση εναλλακτικών αλγορίθμων αντιστοίχισης.

Είναι επίσης δυνατή η χρήση της γεωμετρίας και του αποτυπώματος του ποδιού ή των αποτυπωμάτων των δακτύλων για τον έλεγχο ταυτότητας ενός χρήστη, [12], [31].

3.5.13 Φλέβες

Οι φλέβες ή το αγγειακό μοτίβο (Σχήμα 12) μπορούν να χρησιμοποιηθούν για τον έλεγχο της ταυτότητας ενός ατόμου, καθώς είναι μοναδικό για κάθε άτομο.



Σχήμα 12: Πιστοποίηση με βάση τη βιομετρία της φλέβας.

Η τεχνολογία σχεδιάστηκε για πρώτη φορά από τη Fujitsu και σχεδιάστηκε για να είναι μια τεχνολογία ανέπαφης αναγνώρισης. Βασίζεται σε συγκεκριμένο χαρακτηριστικό του αίματος στις φλέβες γνωστό ως αποοξειδωμένη αιμοσφαιρίνη. Το αίμα που μεταφέρεται πίσω στους πνεύμονες στερείται οξυγόνου καθώς τα κύτταρα του σώματος το έχουν ήδη καταναλώσει από αυτό. Η αποοξειδωμένη αιμοσφαιρίνη εμφανίζεται μαύρη όταν εκτίθεται σε φωτεινά κύματα μήκους κύματος κοντά στο υπέρυθρο. Η ικανότητα του αποοξειδωμένου να απορροφά τέτοια κύματα και να αλλάζει χρώμα καθιστά εύκολο τον εντοπισμό των μοναδικών μοτίβων φλεβών που μπορούν στη συνέχεια να αποτυπωθούν, να αποθηκευτούν ως πρότυπο αναφοράς και τελικά ως βιομετρικός έλεγχος πρόσβασης.

Αυτός ο τύπος ελέγχου ταυτότητας μπορεί να βασίζεται είτε στις φλέβες στην παλάμη του χεριού είτε στα δάχτυλα, [12], [31].

3.5.14 Πληκτρολόγηση και κινήσεις ποντικιού

Αν και ορισμένοι ερευνητές είναι αντίθετοι με τη χρήση της πληκτρολόγησης ως μεθόδου ελέγχου ταυτότητας, υποστηρίζοντας ότι δεν είναι μοναδική όλη την ώρα, άλλοι ερευνητές εξακολουθούν να ενδιαφέρονται να αναπτύξουν συστήματα ελέγχου ταυτότητας που με βάση την πληκτρολόγηση και στηρίζονται σε ορισμένα χαρακτηριστικά όπως: η ταχύτητα πληκτρολόγησης, ο χρόνος μεταξύ δύο πλήκτρων, η συχνότητα των σφαλμάτων πληκτρολόγησης, ο χρόνος που πατιέται ένα πλήκτρο κ.λπ.

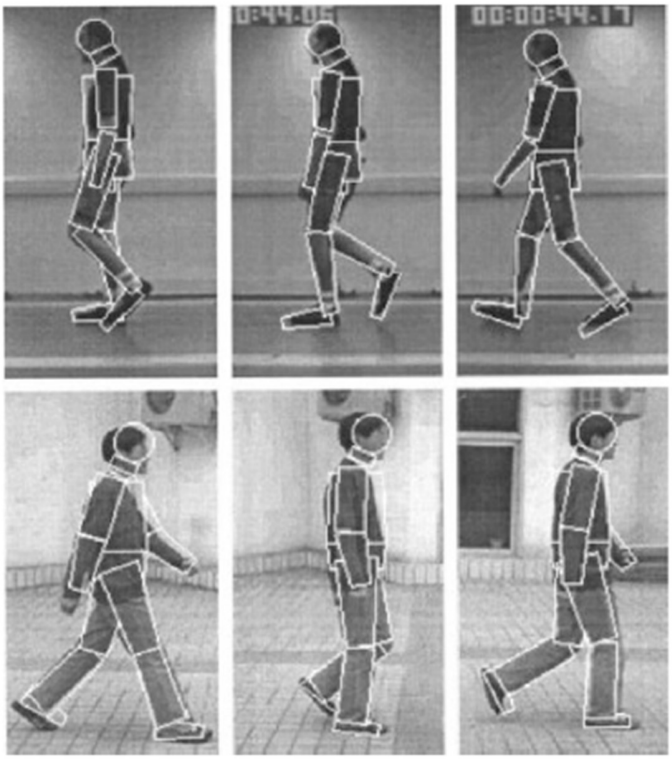
Η δυναμική του ποντικιού είναι επίσης μια μέθοδος ελέγχου ταυτότητας που βασίζεται στη συμπεριφορά, όπου οι ερευνητές καταγράφουν τις κινήσεις και τα κλικ του ποντικιού (δεξί,

μεσαίο και αριστερό κουμπί, σύρσιμο, ακινησία, μεμονωμένα ή διπλά κλικ) για να δημιουργήσουν το πρότυπο χρήστη που θα χρησιμοποιηθεί αργότερα για αυθεντικοποίηση, [12], [31].

3.5.15 Βάδισμα

Ο τρόπος βαδίσματος του ανθρώπου είναι μοναδικός για κάθε άτομο και χρησιμοποιείται για την πιστοποίηση της ταυτότητας του ατόμου στο σύστημα. Σύμφωνα με τους συγγραφείς [12], [31], ο έλεγχος ταυτότητας μπορεί να γίνει με τρεις τρόπους:

- Μηχανική όραση: βασίζεται στη χρήση καμερών για την καταγραφή της βόλτας του ατόμου και την αναγνώρισή του. Υπάρχουν δύο προσεγγίσεις για τη μηχανική όραση, η βασισμένη στο μοντέλο (Σχήμα 13) και η βασισμένη στη σιλουέτα.



Σχήμα 13: Πιστοποίηση με βάση το βάδισμα (με βάση το μοντέλο).

- Φορητοί αισθητήρες: ένα σύνολο μη παρεμβατικών φορητών αισθητήρων μπορεί να προσαρτηθεί στο άτομο για να αναγνωρίσει το βάδισμά του, όπως smartphone, έξυπνα ρολόγια ή παπούτσια με αισθητήρες.

- Προσέγγιση αισθητήρα δαπέδου: το βάδισμα ενός ατόμου αποθηκεύεται και αναγνωρίζεται καθώς περπατά σε δάπεδο που παρακολουθείται από αντίστοιχο αισθητήρα, καθώς παράγονται σήματα από τους πατούμενους αισθητήρες.

Το βάδισμα είναι μια από τις σχετικά νέες βιομετρικές τεχνολογίες και ως εκ τούτου έχει μια ερευνητική κοινότητα που το ερευνά συνεχώς. Όπως τα περισσότερα βιομετρικά στοιχεία συμπεριφοράς, η ακρίβεια και η σταθερότητα είναι βασικές προκλήσεις που αντιμετωπίζουν τα συστήματα αναγνώρισης βαδίσματος. Οι συνεχιζόμενες μελέτες προσπαθούν να αντιμετωπίσουν αυτές τις προκλήσεις.

3.5.16 Αναγνώριση ομιλητή

Η ανθρώπινη φωνή είναι ένα μοναδικό αναγνωριστικό ενός ατόμου και διαφέρει από άτομο σε άτομο λόγω της διαφορετικής ανατομίας (σχήμα λαιμού) και των μαθησιακών μοτίβων συμπεριφοράς. Ο χρήστης θα παρείχε μια φωνητική φράση πρόσβασης για να αναγνωρίσει τον εαυτό του στο σύστημα.

Η αναγνώριση φωνής χρησιμοποιεί τεχνικές μηχανικής μάθησης (Machine Learning – ML) για να μάθει και να αναγνωρίσει την ανθρώπινη φωνή και να θυμάται τον τρόπο που λέει ο άνθρωπος κάθε λέξη. Αυτή η προσαρμογή επιτρέπει στην αναγνώριση φωνής να διακρίνει τη φωνή των ανθρώπων, αν και κάθε άτομο μιλά με διαφορετική προφορά και κλίση. Τα βιομετρικά χαρακτηριστικά της φωνής περιλαμβάνουν φυσικά χαρακτηριστικά όπως φωνητικές οδούς, ρινικές κοιλότητες, στόμα και χείλη. Ωστόσο, δεδομένου ότι η φωνή του χρήστη μπορεί να αλλάξει λόγω ασθενειών όπως το κρύο και ορισμένα άτομα είναι ειδικευμένα στη μίμηση φωνών, αυτό το σύστημα ενδέχεται να μην έχει καλή απόδοση σε αυτές τις περιπτώσεις και θα ήταν σκόπιμο να το χρησιμοποιηθεί σε ένα πολυεπίπεδο βιομετρικό σύστημα ασφαλείας αντί να χρησιμοποιηθεί αυτό από μόνο του, [12], [31].

3.5.17 Παλμοί καρδιάς

Το μοτίβο των καρδιακών παλμών (Σχήμα 14) είναι μοναδικό για κάθε άτομο και αντιπροσωπεύει μια ισχυρή βιομετρική λύση ασφάλειας. Μία από τις προσεγγίσεις πιστοποίησης χρησιμοποιεί το ηλεκτροκαρδιογράφημα που περιγράφει την ηλεκτρική δραστηριότητα της καρδιάς με την πάροδο του χρόνου για την αναγνώριση του ατόμου.

Σχήμα 14: Πιστοποίηση με βάση τους παλμούς της καρδιάς.

Σύμφωνα με τους συγγραφείς [12], [31], το ηλεκτροκαρδιογράφημα μπορεί να καταγραφεί από εξωτερικούς αισθητήρες που είναι προσαρτημένοι στον καρπό ή από τα δάχτυλα για να παρέχουν ευκολία και αποδοχή, καθώς αυτή η λύση χρησιμοποιείται σε smartphone και άλλες συσκευές.

3.5.18 Υπογραφή και τύπος γραφής

Ο τύπος γραφής και οι υπογραφές (Σχήμα 15) είναι μια από τις παλαιότερες και πιο κοινές συμπεριφορικές βιομετρικές λύσεις όπου η ιδέα της υπογραφής και εξουσιοδότησης εγγράφων υιοθετείται ως μέθοδος ελέγχου ταυτότητας.

Σχήμα 15: Πιστοποίηση βασισμένη στην υπογραφή.

Αυτή η λύση γίνεται είτε online όπου ο αισθητήρας συγκρίνει όχι μόνο τη γραπτό κείμενο αλλά και την ταχύτητα, την επιτάχυνση και την πίεση που εφαρμόζεται στο στυλό, είτε εκτός

σύνδεσης όπου η εικόνα της φράσης πρόσβασης συγκρίνεται με αυτήν που είναι αποθηκευμένη. Το κύριο πρόβλημα αυτής της προσέγγισης είναι οι πλαστογράφοι που μπορούν να μιμηθούν τα χειρόγραφα, [12], [31].

3.6 ΠΡΟΚΛΗΣΕΙΣ ΒΙΟΜΕΤΡΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τα βιομετρικά συστήματα εισήχθησαν για την προστασία της ασφάλειας των χώρων από μη εξουσιοδοτημένους χρήστες. Η πρόοδος της τεχνολογίας έχει κάνει αυτά τα συστήματα πολύ ασφαλή και αξιόπιστα. Ωστόσο, καμία τεχνολογία δεν μπορεί να ανταγωνιστεί τον ανθρώπινο νου. Υπάρχουν πάρα πολλοί κίνδυνοι που ενέχουν τα βιομετρικά συστήματα, π.χ. η επίθεση πλαστογράφησης, η επίθεση από κακόβουλους χρήστες κ.ο.κ. Αυτοί οι κίνδυνοι είναι σοβαροί και για την ασφάλεια στον κυβερνοχώρο. Μερικές από αυτές τις προκλήσεις περιγράφονται στις ακόλουθες υποενότητες.

3.6.1 Επιθέσεις από κακόβουλους χρήστες (imposter attacks)

Οι επιθέσεις από κακόβουλους χρήστες μπορεί να έχουν σημαντικό κίνδυνο για ένα σύστημα/ εγκατάσταση που χρησιμοποιεί βιομετρικά συστήματα για ορθολογική ή φυσική είσοδο. Οι επιθέσεις από κακόβουλους χρήστες προσπαθούν να κάνουν κακή χρήση των αδυναμιών ενός βιομετρικού συστήματος. Οι βιομετρικές συσκευές έχουν μικρές πιθανότητες να αντιμετωπίσουν έναν κακόβουλο χρήστη ως πραγματικό πρόσωπο. Αυτές οι πιθανότητες εκφράζονται με τη βοήθεια ενός βιομετρικού πίνακα απόδοσης, γνωστής ως FAR (Ρυθμός Λανθασμένης Αποδοχής - False Acceptance Rate). Παρόλο που τα βιομετρικά συστήματα έχουν την ελάχιστη δυνατή FAR, δεν είναι ποτέ μηδενική και ενέχει πάντα τον κίνδυνο να εισέλθει ένας κακόβουλος χρήστης. Αυτή η προσπάθεια του κακόβουλου χρήστη μπορεί να είναι σκόπιμη για να επηρεάσει δεδομένα ή την ίδια την ιδιοκτησία. Καθώς αυτός ο κίνδυνος συνδέεται με τη δράση ενός βιομετρικού συστήματος, μπορεί να αντιμετωπιστεί με τις λύσεις που παρέχει η εξέλιξη της τεχνολογίας. Η μείωση του FAR μπορεί επίσης να βελτιώσει άλλους πίνακες βιομετρικής απόδοσης που ονομάζονται FRR (Ρυθμός Λανθασμένης Απόρριψης - False Rejection Rate), όπου ένα βιομετρικό σύστημα απορρίπτει την είσοδο σε έναν επιτρεπόμενο χρήστη.

3.6.2 Επιθέσεις πλαστογραφίας (spoof attacks)

Σε μια συναλλαγή υψηλής αξίας, όπως σε τραπεζικά και χρηματοπιστωτικά ιδρύματα, η βιομετρία είναι ένα συνηθισμένο εργαλείο. Η χρήση των βιομετρικών στοιχείων έχει δημιουργήσει κίνητρα για εγκληματικές βλέψεις, καθώς ένας εγκληματίας πάντα αναζητά ευκαιρίες και τρωτά σημεία για να εισβάλει σε ένα σύστημα για να κλέψει χρήματα. Έχει αυξημένο κίνδυνο πλαστογραφίας, ιδιαίτερα σε παλαιότερα ή βιομετρικά συστήματα χαμηλής ασφάλειας.

Στην επίθεση πλαστογραφίας, δημιουργούνται διπλότυπα βιομετρικά αναγνωριστικά εξουσιοδοτημένου χρήστη. Για παράδειγμα, τα δακτυλικά αποτυπώματα βρίσκονται σε χερούλια θυρών, τραπέζια, κούπες καφέ και πολλές επιφάνειες που εκτίθενται στο κοινό, και μπορούν να ληφθούν και να χρησιμοποιηθούν με δόλιο τρόπο από πλαστογράφους. Οι φωτογραφίες υψηλής ποιότητας μπορούν να χρησιμοποιηθούν ως εργαλείο απατεώνων ή οι ίδιες οι φωτογραφίες μπορούν να χρησιμοποιηθούν στην περίπτωση των συσκευών αναγνώρισης προσώπου. Σε ένα πιο σοβαρό είδος επιθέσεων πλαστογραφίας σε συσκευές αναγνώρισης προσώπου, μπορούν να χρησιμοποιηθούν τα βίντεο κλιπ ή οι μάσκες των χαρακτηριστικών του προσώπου ενός εξουσιοδοτημένου χρήστη.

Ο κίνδυνος πλαστογραφίας είναι υψηλότερος όταν οι οικονομικές συναλλαγές επαληθεύονται με βιομετρικά στοιχεία. Όσον αφορά τα χρήματα, τέτοιες συναλλαγές διατρέχουν διαρκώς κίνδυνο βιομετρικών επιθέσεων πλαστογράφησης. Η σύγχρονη γενιά βιομετρικών συσκευών έχει βελτιώσει την ασφάλεια κατά της πλαστογράφησης, ωστόσο, οι δράστες συνεχίζουν να αναζητούν μέσα για την κακή χρήση των συστημάτων και, τελικά, όλες οι πιθανές λύσεις δεν είναι επαρκείς. Αυτός ο κίνδυνος μπορεί να μετριαστεί με την αναγνώριση δομών και προτύπων επιθέσεων πλαστογραφίας και την επίτευξη τεχνολογικών αντίμετρων, αλλά και με συνδυαστική χρήση τους, [3], [5].

3.7 ΣΥΝΟΨΗ

Σε αυτό το κεφάλαιο έγινε μια ανασκόπηση των τελευταίων τεχνολογιών στις βιομετρικές τεχνολογίες, επισημαίνοντας την πρόοδο που έχει σημειωθεί στην παραδοσιακή βιομετρία και παρουσιάζοντας τα χαρακτηριστικά των αναδυόμενων μεθόδων. Δεν υπάρχει αμφιβολία ότι υπήρξε μια αλλαγή στη στάση της κοινωνίας απέναντι στα βιομετρικά στοιχεία για να γίνει αποδεκτή η τεχνολογία. Αυτό οφείλεται στην αυξημένη ευαισθητοποίηση και αναγνώριση της ανάγκης για υψηλή ασφάλεια και καλύτερη κατανόηση του σκοπού αυτής της τεχνολογίας.

Ωστόσο, χρειάζεται περισσότερη δουλειά για να επιτευχθεί ακόμα μεγαλύτερη αποδοχή. Αυτό θα απαιτούσε την αντιμετώπιση ζητημάτων ασφάλειας και απορρήτου που είναι εγγενή στις βιομετρικές τεχνολογίες.

Επιπλέον, υπάρχουν πολλά σύγχρονα ζητήματα που πρέπει να αντιμετωπιστούν. Αυτά περιλαμβάνουν ζητήματα που σχετίζονται με αξιολογήσεις βιομετρικών συστημάτων, όπως η καλύτερη κατανόηση των επιπτώσεων της γήρανσης, η εκτίμηση των διαστημάτων εμπιστοσύνης, οι επιπτώσεις στο περιβάλλον, η μοντελοποίηση και η πρόβλεψη απόδοσης, το πρωτόκολλο και η συγκριτική αξιολόγηση, οι κοινωνικές επιπτώσεις και οι μελέτες χρηστικότητας. Ένας τομέας που παίζει σημαντικό ρόλο σε αυτό είναι η τεχνητή νοημοσύνη, και με αυτό το έναυσμα, αναλύεται η τεχνητή νοημοσύνη στο επόμενο κεφάλαιο.

4. ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Σήμερα, διάφορες νέες τεχνολογίες δικτύωσης και υπολογιστών, όπως η δικτύωση με βάση το λογισμικό (Software Defined Networking - SDN), τα μεγάλα δεδομένα (Big Data) και η υπολογιστική ομίχλη (fog computing), έχουν προωθήσει την ταχεία ανάπτυξη του κυβερνοχώρου. Σε αυτό το πλαίσιο η ασφάλεια στον κυβερνοχώρο έχει γίνει ένα από τα πιο σημαντικά ζητήματα. Η ασφάλεια του κυβερνοχώρου έχει επιβάλει τεράστιες επιπτώσεις σε διάφορες υποδομές ζωτικής σημασίας. Η παραδοσιακή ασφάλεια βασίζεται στον στατικό έλεγχο συσκευών ασφαλείας που αναπτύσσονται στα άκρα ή σε ειδικούς κόμβους, όπως με τείχη προστασίας, συστήματα ανίχνευσης εισβολών (IDS) και συστήματα πρόληψης εισβολής (IPS), για την παρακολούθηση της ασφάλειας του δικτύου σύμφωνα με τους προκαθορισμένους κανόνες. Ωστόσο, αυτή η μεθοδολογία παθητικής άμυνας δεν είναι πλέον χρήσιμη για την προστασία συστημάτων από νέες απειλές για την ασφάλεια στον κυβερνοχώρο, όπως οι προηγμένες επίμονες απειλές (Advanced Persistent Threats - APT) και οι επιθέσεις της "ημέρας μηδέν". Επιπλέον, καθώς οι απειλές στον κυβερνοχώρο βρίσκονται παντού και είναι βιώσιμες, τα ποικίλα σημεία εισόδου επιθέσεων, η εισβολή σε υψηλό επίπεδο και τα εργαλεία συστηματικής επίθεσης μειώνουν το κόστος της ανάπτυξης απειλών στον κυβερνοχώρο. Για να μεγιστοποιηθεί το επίπεδο ασφάλειας των βασικών πόρων του συστήματος, είναι κρίσιμης σημασίας να αναπτυχθούν καινοτόμες και έξυπνες μεθοδολογίες άμυνας ασφάλειας που να μπορούν να αντιμετωπίσουν διαφοροποιημένες και βιώσιμες απειλές. Για την εφαρμογή νέων λύσεων και προστασίας της ασφάλειας στον κυβερνοχώρο, το σύστημα θα πρέπει να λαμβάνει το ιστορικό και τα τρέχοντα δεδομένα κατάστασης ασφάλειας και να λαμβάνει έξυπνες αποφάσεις που μπορούν να παρέχουν προσαρμοστική διαχείριση και έλεγχο ασφάλειας.

Η τεχνητή νοημοσύνη (Artificial Intelligence - AI) είναι ένας ταχέως αναπτυσσόμενος κλάδος της επιστήμης των υπολογιστών που ερευνά και αναπτύσσει θεωρίες, μεθόδους, τεχνικές και συστήματα εφαρμογής για την προσομοίωση, και επέκταση της ανθρώπινης νοημοσύνης. Χάρη στην ανάπτυξη της τεχνολογίας υπολογιστών μεγαλύτερης απόδοσης και την εμφάνιση της βαθιάς μάθησης (Deep Learning - DL), η τεχνολογία AI έχει σημειώσει μεγάλη πρόοδο τα τελευταία χρόνια, [9].

4.1 ΝΕΑ ΤΑΣΗ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ - ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Υπάρχουν πολλές προσεγγίσεις για την εφαρμογή της τεχνητής νοημοσύνης. Σε πολύ πρώιμο στάδιο, οι άνθρωποι χρησιμοποίησαν μια βάση γνώσεων για να την τυποποιήσουν. Ωστόσο, αυτή η προσέγγιση χρειάζεται πάρα πολλές χειροκίνητες λειτουργίες για να περιγράψει ακριβώς τον κόσμο με πολύπλοκους κανόνες. Για αυτό το λόγο, οι επιστήμονες σχεδίασαν ένα μοτίβο στο οποίο το σύστημα AI μπορεί να εξάγει ένα μοντέλο από ακατέργαστα δεδομένα, και αυτή η ικανότητα ονομάζεται "μηχανική μάθηση" (Machine Learning – ML). Οι αλγόριθμοι ML περιλαμβάνουν στατιστικούς μηχανισμούς, όπως τον αλγόριθμο Bayes, την προσέγγιση συναρτήσεων (linear ή logistics regression) και δέντρα αποφάσεων. Όλοι αυτοί οι αλγόριθμοι είναι ισχυροί και μπορούν να χρησιμοποιηθούν σε πολλές περιπτώσεις όπου απαιτείται μια απλή ταξινόμηση. Ωστόσο, αυτές οι μέθοδοι έχουν περιορισμένη ακρίβεια, γεγονός που μπορεί να οδηγήσει σε κακή απόδοση στη μαζική και πολύπλοκη αναπαράσταση δεδομένων. Η DL προτάθηκε για την επίλυση των παραπάνω ελλείψεων. Η DL μιμείται τη διαδικασία των ανθρώπινων νευρώνων και χτίζει τη νευρωνική αρχιτεκτονική με πολύπλοκες διασυνδέσεις. Σήμερα, η DL αποτελεί πόλο έλξης για έρευνα στον ακαδημαϊκό χώρο και έχει χρησιμοποιηθεί ευρέως σε διάφορα βιομηχανικά σενάρια. Για αυτό το λόγο, ακολουθεί η κατηγοριοποίηση και οι εφαρμογές προηγμένων μοντέλων σε DL σε διάφορους τομείς.

4.1.1 Κατηγοριοποίηση βαθιάς μάθησης (Deep Learning)

Σύμφωνα με τους συγγραφείς [38], [39], η κατηγοριοποίηση της DL βασίζεται στον μαθησιακό μηχανισμό του και αποτελείται από τα εξής τέσσερα μέρη:

- Εποπτευόμενη μάθηση: Στη διαδικασία της μηχανικής μάθησης, η εποπτευόμενη μάθηση ανήκει σε μια σχετικά βασική μέθοδο εκμάθησης. Αυτή η μέθοδος μάθησης αναφέρεται στην καθιέρωση αντίστοιχων μαθησιακών στόχων από τους ανθρώπους πριν από τη διαδικασία της μάθησης. Κατά την αρχική εκπαίδευση του μηχανήματος, το μηχάνημα βασίζεται στην τεχνολογία πληροφοριών για να μάθει τις ανάγκες της μάθησης. Προκειμένου να συλλεχθούν βασικές πληροφορίες δεδομένων, θα πρέπει να ολοκληρωθεί σταδιακά το απαιτούμενο μαθησιακό περιεχόμενο σε εποπτευόμενο περιβάλλον. Σε σύγκριση με άλλες μεθόδους μάθησης, η εποπτευόμενη μάθηση μπορεί να τονώσει πλήρως το γενικευμένο δυναμικό μάθησης του ίδιου του μηχανήματος. Μετά την ολοκλήρωση της

μάθησης του συστήματος, μπορεί να βοηθήσει τους ανθρώπους να επιλύσουν ορισμένα προβλήματα ταξινόμησης ή παλινδρόμησης. Για την ταξινόμηση γίνεται διανομή των δεδομένων στις κατηγορίες που ορίζονται στο σύνολο δεδομένων σύμφωνα με τα συγκεκριμένα χαρακτηριστικά τους. Για την παλινδρόμηση γίνεται πρόβλεψη ή συμπέρασμα των άλλων χαρακτηριστικών των δεδομένων με βάση τις διαθέσιμα χαρακτηριστικά τους. Επί του παρόντος, οι κλασικές μέθοδοι μάθησης που χρησιμοποιούνται συνήθως περιλαμβάνουν δίκτυα Bayes (Bayesian Networks – BN), μηχανές διανυσμάτων υποστήριξης (Support Vector Machines - SVM), K- κοντινότεροι γείτονες (K-Nearest Neighbours – KNN), κλπ.

- Μη εποπτευόμενη μάθηση: Η αντίθετη της εποπτευόμενης μάθησης είναι η μη εποπτευόμενη μάθηση. Η αποκαλούμενη μάθηση χωρίς επίβλεψη σημαίνει ότι το μηχάνημα δεν μαρκάρει το περιεχόμενο προς μια συγκεκριμένη κατεύθυνση καθόλη τη διαδικασία μάθησης, αλλά βασίζεται στο ίδιο το μηχάνημα για να ολοκληρώσει την ανάλυση των πληροφοριών των δεδομένων. Στην πράξη, η διαδικασία είναι το μηχάνημα να έχει την ελευθερία να μάθει τις βασικές έννοιες και το περιεχόμενο και στη συνέχεια να ολοκληρώσει μια σειρά εκμάθησης περιεχομένου, συμπεριλαμβανομένων εννοιών και περιεχομένου παρόμοιων με τις βασικές αρχές. Γενικά, η συνεχής βελτίωση της μάθησης σταδιακά έχει αυξήσει το εύρος του περιεχομένου της μηχανικής μάθησης. Προς το παρόν, η μη εποπτευόμενη μάθηση περιλαμβάνει αλγόριθμους όπως τα δίκτυα deep belief και αυτοκωδικοποιητές (autoencoders). Τέτοιες καταστάσεις ευνοούν τη λύση των προβλημάτων ομαδοποίησης (clustering) και συσχέτισης (association) και έχουν εφαρμογή στην ανάπτυξη πολλών βιομηχανιών. Η ομαδοποίηση περιλαμβάνει την εύρεση των ομάδων δεδομένων που είναι παρόμοιες μεταξύ τους όταν οι εγγενείς ομαδοποιήσεις στα δεδομένα δεν είναι γνωστές. Η συσχέτιση περιλαμβάνει τον καθορισμό των συσχετίσεων και των συνδέσεων μεταξύ των δεδομένων στο ίδιο σύνολο δεδομένων. Τέλος, παρατηρείται και η αφαίρεση των χαρακτηριστικών (Deduction of Features) όταν τα χαρακτηριστικά που σχετίζονται με την ομάδα και την κατηγορία των δεδομένων δεν μπορούν να προσδιοριστούν. Σε τέτοιες περιπτώσεις, η επιλογή μιας υποομάδας χαρακτηριστικών ή η απόκτηση νέων χαρακτηριστικών που συνδυάζουν τα χαρακτηριστικά ονομάζεται αφαίρεση χαρακτηριστικών.

- Ημι-εποπτευόμενη μάθηση: Η εποπτευόμενη και η μη εποπτευόμενη μάθηση είναι ανεπαρκείς όταν τα δεδομένα με ετικέτα είναι λιγότερα από τα δεδομένα χωρίς ετικέτα. Σε τέτοιες περιπτώσεις, τα μη επισημασμένα δεδομένα, τα οποία είναι ανεπαρκή, χρησιμοποιούνται για την εξαγωγή πληροφοριών σχετικά με αυτά. Και, αυτή η μέθοδος ονομάζεται ημι-εποπτευόμενη μάθηση. Η διαφορά μεταξύ της ημι-εποπτευόμενης μάθησης και της εποπτευόμενης μάθησης είναι το σύνολο δεδομένων με ετικέτα. Στην εποπτευόμενη μάθηση, τα επισημασμένα δεδομένα είναι περισσότερα από τα δεδομένα που πρέπει να προβλεφθούν. Αντίθετα, στην ημι-εποπτευόμενη μάθηση, τα επισημασμένα δεδομένα είναι λιγότερα από τα δεδομένα που θα πρέπει να προβλεφθούν.
- Ενίσχυση της μάθησης: Εκτός από την εποπτευόμενη μάθηση και τη μη εποπτευόμενη μάθηση, υπάρχουν επίσης μέθοδοι εφαρμογής ενισχυμένης μάθησης στη μηχανική μάθηση. Η ενισχυμένη μάθηση είναι η συστηματική εκμάθηση ενός συγκεκριμένου περιεχομένου. Στη συγκεκριμένη διαδικασία εφαρμογής, χρησιμοποιούνται τα δεδομένα που συλλέχθηκαν την προηγούμενη περίοδο. Οργανώνει και επεξεργάζεται τις πληροφορίες ανατροφοδότησης ενός συγκεκριμένου τμήματος για να σχηματίσει έναν κλειστό βρόχο επεξεργασίας δεδομένων. Συνολικά, η ενισχυτική μάθηση είναι ένας τύπος μαθησιακής μεθόδου που επεκτείνει τη συλλογή δεδομένων με βάση στατιστικά και δυναμική μάθηση. Τέτοιες μέθοδοι χρησιμοποιούνται κυρίως για την επίλυση του προβλήματος ελέγχου των ρομπότ. Οι αντιπροσωπευτικές μέθοδοι μάθησης περιλαμβάνουν τον αλγόριθμο Q-learning και τον αλγόριθμο εκμάθησης χρονικής διαφοράς.

4.1.2 Εφαρμογές βαθιάς μάθησης

Σε αυτό την ενότητα, εξετάζονται οι εφαρμογές της DL. Η DL χρησιμοποιείται ευρέως σε αυτόνομα συστήματα λόγω των σημαντικών πλεονεκτημάτων στη βελτιστοποίηση, τη διάκριση και την πρόβλεψη. Λόγω των τεράστιων κατηγοριών περιοχών εφαρμογών, αναφέρονται μόνο μερικοί αντιπροσωπευτικοί τομείς εφαρμογών.

4.1.2.1 Αναγνώριση εικόνας και βίντεο

Η αναγνώριση εικόνας και βίντεο είναι ο πιο σημαντικός τομέας της έρευνας της DL. Η τυπική δομή της DL σε αυτό τον τομέα είναι το βαθύ συνελικτικό νευρωνικό δίκτυο (Convolutional Neural Network - CNN). Αυτή η δομή μπορεί να μειώσει το μέγεθος της εικόνας

συγκεντρώνοντας και ομαδοποιώντας την εικόνα πριν τοποθετηθούν τα δεδομένα στο πλήρως συνδεδεμένο νευρωνικό δίκτυο. Σε αυτόν τον τομέα, υπάρχει μεγάλο ερευνητικό ενδιαφέρον και πολλές σχετικές εφαρμογές βασίζονται σε αυτή την έρευνα. Για παράδειγμα, ο Ren [40], πρότεινε ένα ταχύτερο CNN για ανίχνευση αντικειμένων σε πραγματικό χρόνο για να μειώσει σημαντικά τον χρόνο λειτουργίας του δικτύου ανίχνευσης.

4.1.2.2 Ανάλυση κειμένου και επεξεργασία φυσικής γλώσσας

Με την ανάπτυξη της κοινωνικής δικτύωσης και του κινητού διαδικτύου, δημιουργούνται τεράστια δεδομένα από την ανθρώπινη αλληλεπίδραση. Η απαίτηση της ανάλυσης κειμένου και της επεξεργασίας της φυσικής γλώσσας είναι η βασική προϋπόθεση της συνεχούς (on-the-fly) μετάφρασης και της αλληλεπίδρασης ανθρώπου-μηχανής με φυσική ομιλία. Πολλές σχετικές εφαρμογές DL έχουν προταθεί, π.χ. μια εργαλειοθήκη, με το όνομα "Stanford CoreNLP", η οποία είναι μια επεκτάσιμη γραμμή διοχέτευσης που παρέχει ανάλυση βασικής φυσικής γλώσσας, [9].

4.1.2.3 Οικονομία και ανάλυση αγοράς

Οι συναλλαγές μετοχών και άλλα μοντέλα αγοράς απαιτούν πολύ ακριβείς προβλέψεις αγοράς. Η DL έχει αξιοποιηθεί σε μεγάλο βαθμό ως ένα ισχυρό εργαλείο πρόβλεψης της αγοράς. Για παράδειγμα, ο Korczak [41], πρότεινε έναν αλγόριθμο πρόβλεψης οικονομικών χρονοσειρών με βάση την αρχιτεκτονική του CNN. Το ποσοστό σφάλματος πρόβλεψης μειώθηκε σημαντικά μέσω δοκιμών με χρήση δεδομένων αγοράς συναλλάγματος.

4.2 Κυβερνοασφάλεια βασισμένη στην τεχνητή νοημοσύνη

Σε αυτήν την ενότητα, εξετάζονται τα παραδοσιακά σχήματα ML κατά των επιθέσεων στον κυβερνοχώρο και διάφορα σχήματα DL. Συζητούνται η διαδικασία υλοποίησης, τα πειραματικά αποτελέσματα με βάση τα πειράματα που έχουν εκπονηθεί και η αποτελεσματικότητα διαφορετικών προγραμμάτων για την καταπολέμηση των επιθέσεων στον κυβερνοχώρο.

4.2.1 Παραδοσιακά σχήματα μηχανικής μάθησης ενάντια στις κυβερνοεπιθέσεις

Μια λύση μηχανικής μάθησης αποτελείται από τέσσερα κύρια βήματα:

- εξαγωγή χαρακτηριστικών,
- επιλογή κατάλληλου αλγορίθμου ML,

- εκπαίδευση μοντέλου και στη συνέχεια επιλογή του μοντέλου με την καλύτερη απόδοση αξιολογώντας διαφορετικούς αλγόριθμους και προσαρμόζοντας τις παραμέτρους.
- ταξινόμηση ή πρόβλεψη άγνωστων δεδομένων χρησιμοποιώντας το εκπαιδευμένο μοντέλο.

Οι κοινές λύσεις ML περιλαμβάνουν τον αλγόριθμο k-πλησιέστερο γείτονα (k-nearest-neighbor - k-NN), τη μηχανή διανυσμάτων υποστήριξης (Support Vector Machine - SVM), το δέντρο αποφάσεων, το νευρωνικό δίκτυο, κ.λπ. Διαφορετικά είδη αλγορίθμων επιλύουν διαφορετικούς τύπους προβλημάτων. Είναι απαραίτητο να επιλεγεί ένας κατάλληλος αλγόριθμος σύμφωνα με συγκεκριμένα σενάρια βιομηχανικών εφαρμογών.

4.2.1.1 Ασφάλεια βασισμένη στον k-NN

Η βασική προϋπόθεση της εκτέλεσης του k-NN είναι ότι τα δεδομένα και οι ετικέτες του συνόλου δεδομένων εκπαίδευσης πρέπει να είναι γνωστά. Εισάγονται τα δεδομένα δοκιμής και, στη συνέχεια, συγκρίνονται τα χαρακτηριστικά των δεδομένων δοκιμής με τα αντίστοιχα χαρακτηριστικά στο σετ εκπαίδευσης για την εύρεση των κορυφαίων k μεταδεδομένα που είναι πιο παρόμοια με το σύνολο εκπαίδευσης. Τέλος, επιλέγεται αυτό με τις περισσότερες εμφανίσεις μεταξύ των k μεταδεδομένων ως η κλάση που αντιστοιχεί στα δεδομένα δοκιμής.

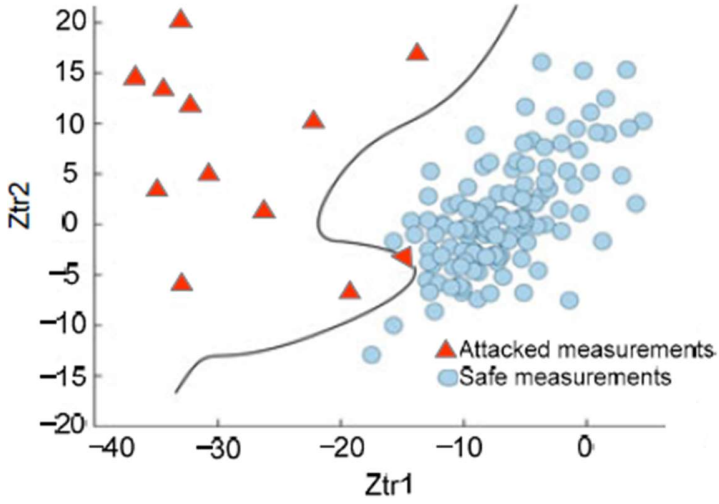
Σύμφωνα με τον Syarif [42], πρότεινε ένα σχήμα ανίχνευσης εισβολής χρησιμοποιώντας αλγόριθμους δυαδικής βελτιστοποίησης σμήνους σωματιδίων (Particle Swarm Optimization - PSO) και τον k-NN. Επιλέχτηκε το σύνολο δεδομένων KDD CUP 1999, το οποίο είναι ένα ευρέως χρησιμοποιούμενο πρότυπο σύνολο δεδομένων για προσομοίωση από ερευνητές σε IDS. Τα συνολικά πειραματικά αποτελέσματα δείχνουν αύξηση ακρίβειας 2% σε σύγκριση με εκείνα που έγιναν χρησιμοποιώντας μόνο τον αλγόριθμο k-NN.

Οι υβριδικοί ταξινομητές συνήθως αποδίδουν καλύτερα από τους μεμονωμένους. Οι k-NN, SVM και pdAPSO συνδυάζονται για ανίχνευση εισβολής. Ο Dada [43], σύγκρινε τις επιδόσεις αυτών των τριών ταξινομητών χρησιμοποιώντας σύνολα δεδομένων KDD99 και τα πειραματικά αποτελέσματα έδειξαν ότι η συγχώνευση των τριών ταξινομητών μπορεί να οδηγήσει σε ακρίβεια ταξινόμησης 98,55%. Ωστόσο, η συγκεκριμένη μελέτη εστίασε μόνο στην ακρίβεια ταξινόμησης και όχι στην πολυπλοκότητα και την αποτελεσματικότητα του μοντέλου.

Με βάση έναν ταξινομητή πολλαπλών κλάσεων k-NN, ο Meng [44], ανέπτυξε μια μέθοδο επαλήθευσης ειδοποιήσεων βασισμένη στη γνώση για τον εντοπισμό ψευδών συναγερμών και μη κρίσιμων συναγερμών. Στη συνέχεια, για να φιλτράρουν αυτούς τους ανεπιθύμητους συναγερμούς, σχεδίασαν ένα έξυπνο φίλτρο συναγερμού που αποτελείται από τρία κύρια στοιχεία: μια βάση δεδομένων συναγερμών, μια μέτρηση βαθμολογίας και ένα φίλτρο συναγερμού. Διεξήγαγαν πειράματα από διαφορετικές διαστάσεις και τα πειραματικά αποτελέσματα έδειξαν ότι το σχεδιασμένο φίλτρο συναγερμού μπορεί να επιτύχει καλή απόδοση φιλτραρίσματος ακόμη και με περιορισμένη χρήση CPU.

4.2.1.2 Ασφάλεια βασισμένη στον SVM

Η μηχανή διανυσμάτων υποστήριξης (SVM) είναι ένας εποπτευόμενος αλγόριθμος μάθησης που έχει ανώτερη απόδοση, συμπεριλαμβανομένης της ταξινόμησης διανυσμάτων υποστήριξης και της παλινδρόμησης διανυσμάτων υποστήριξης. Η βασική ιδέα του SVM είναι να διαχωρίσει τα δεδομένα κατασκευάζοντας ένα κατάλληλο επίπεδο διαχωρισμού. Το Σχήμα 16 δείχνει μια τυπική υλοποίηση SVM. Το βέλτιστο επίπεδο διαχωρισμού καθορίζεται για την ταξινόμηση των μετρήσεων που έχουν υποστεί επίθεση/ είναι ασφαλείς



Σχήμα 16: Εφαρμογή ταξινόμησης SVM.

Σύμφωνα με τον Olalere [45], κατασκεύασε έναν ταξινομητή κακόβουλου λογισμικού ομοιόμορφου εντοπισμού πόρων (Uniform Resource Locator - URL) σε πραγματικό χρόνο εντοπίζοντας και αξιολογώντας διακριτικά λεξικά χαρακτηριστικά διευθύνσεων URL κακόβουλου λογισμικού. Εξετάστηκαν με χειροκίνητο τρόπο διευθύνσεις URL κακόβουλου

λογισμικού από τη μαύρη λίστα, γεγονός που οδήγησε στον εντοπισμό 12 διακριτικών λεξιλογικών χαρακτηριστικών. Στη συνέχεια, διεξήχθη εμπειρική ανάλυση σχετικά με τα αναγνωρισμένα χαρακτηριστικά των υπαρχόντων διευθύνσεων URL κακόβουλου λογισμικού στη μαύρη λίστα και των διευθύνσεων URL που συλλέχθηκαν πρόσφατα, αποκαλύπτοντας ότι οι εισβολείς ακολούθησαν το ίδιο μοτίβο στη δημιουργία διευθύνσεων URL κακόβουλου λογισμικού. Τέλος, χρησιμοποιήθηκε ένα SVM για να αξιολογήσουν την απόδοση και την αποτελεσματικότητα των εξαγόμενων χαρακτηριστικών και πέτυχαν ακρίβεια 96,95% με χαμηλό ψευδώς αρνητικό ποσοστό (False Negative Rate - FNR) 0,018.

Το SVM έχει επίσης χρησιμοποιηθεί στην ανίχνευση και ανάλυση εισβολών σε ορισμένα καινούρια δίκτυα. Για παράδειγμα, στο SDN, ο ελεγκτής είναι ευάλωτος σε επιθέσεις DDoS, γεγονός που οδηγεί σε εξάντληση πόρων. Ο Kokila [46], χρησιμοποίησε έναν ταξινομητή SVM για να ανιχνεύσει επιθέσεις DDoS στο δίκτυο SDN. Πραγματοποιήθηκαν επίσης κάποια πειράματα στο υπάρχον σύνολο δεδομένων DARPA και συγκρίθηκαν οι επιδόσεις μεταξύ του ταξινομητή SVM και άλλων τεχνικών, δείχνοντας ότι το σχεδιασμένο σχήμα SVM παρήγαγε χαμηλότερο ψευδώς θετικό ποσοστό (False Positive Rate - FPR) και υψηλότερη ακρίβεια ταξινόμησης. Ωστόσο, η εκπαίδευση SVM απαιτεί περισσότερο χρόνο, κάτι που αποτελεί φανερό μειονέκτημα.

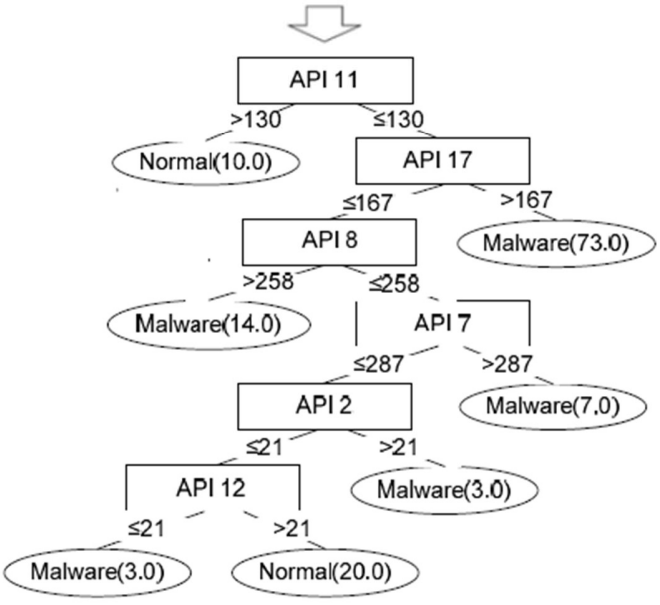
Ο κυβερνοχώρος των διαφορετικών βιομηχανικών εφαρμογών παρουσιάζει διαφορετικά χαρακτηριστικά δικτύου, και ως εκ τούτου τα μοτίβα επιθέσεων που έχουν εμφανιστεί είναι επίσης συγκεκριμένα. Για παράδειγμα, η αμφίδρομη επικοινωνία και το κατανεμημένο ενεργειακό δίκτυο που κάνει το δίκτυο έξυπνο είναι τα κύρια χαρακτηριστικά ενός έξυπνου δικτύου. Στο έξυπνο δίκτυο, η κακόβουλη έγχυση λανθασμένων δεδομένων θα έχει καταστροφικό αντίκτυπο στις αποφάσεις σε διάφορα στάδια. Προτάθηκαν δύο τεχνικές για τον εντοπισμό και την ταξινόμηση σφαλμάτων σε γραμμές μεταφοράς ηλεκτρικής ενέργειας: Και οι δύο προσεγγίσεις βασίζονται στις μηχανές διανυσμάτων υποστήριξης τετάρτου-σφαίρας μιας κατηγορίας (Quarter-Sphere Support Vector Machines - QSSVMs). Η πρώτη προσέγγιση, που ονομάζεται "QSSVM χρονικού χαρακτηριστικού (Temporal-Attribute – TA)-QSSVM", προσπαθεί να προσδιορίσει τις συσχετίσεις χαρακτηριστικών των δεδομένων που μετρώνται σε μεταφορά γραμμής για ανίχνευση σφαλμάτων και η δεύτερη προσέγγιση εκμεταλλεύεται συσχετίσεις χαρακτηριστικών μόνο για ταξινόμηση σφαλμάτων. Τα πειράματα έδειξαν ότι το TA-QSSVM μπορεί να αποκτήσει σχεδόν

100% ακρίβεια ανίχνευσης σφαλμάτων και το A-QSSVM μπορεί να επιτύχει 99% ακρίβεια ταξινόμησης σφαλμάτων, τα οποία είναι αξιοσημείωτα αποτελέσματα. Εκτός από την ακρίβεια, αυτές οι προσεγγίσεις είχαν μικρότερη υπολογιστική πολυπλοκότητα από το SVM πολλαπλών κλάσεων (από $O(n^4)$ έως $O(n^2)$), καθιστώντας τις εφαρμόσιμες στον διαδικτυακό εντοπισμό και ταξινόμηση, [9], [47].

4.2.1.3 Ασφάλεια βασισμένη στα δέντρα απόφασης

Ο αλγόριθμος του δέντρου απόφασης είναι μια μέθοδος για την προσέγγιση της τιμής μιας διακριτής συνάρτησης. Στην ουσία, ο μηχανισμός δέντρου απόφασης είναι μια διαδικασία ταξινόμησης δεδομένων μέσω μιας σειράς κανόνων. Το Σχήμα 17 δείχνει τη διαδικασία κατασκευής του δέντρου απόφασης για τον εντοπισμό κακόβουλου λογισμικού. Το κακόβουλο λογισμικό μπορεί να ταξινομηθεί με βάση ένα δέντρο απόφασης και το αποτέλεσμα της απόφασης προέρχεται από συγκεκριμένα χαρακτηριστικά μέσω προκαθορισμένων κανόνων απόφασης.

API 11	API 17	API 8	API 7	API 2	API 12	Result
158	190	210	231	55	87	Normal(10.0)
125	201	166	105	8	112	Malware(73.0)
97	130	290	303	72	21	Malware(14.0)
130	78	194	316	21	4	Malware(7.0)
21	96	203	255	43	53	Malware(3.0)
58	166	189	178	19	22	Normal(20.0)
85	167	158	214	6	20	Malware(3.0)



Σχήμα 17: Κατασκευή δέντρου απόφασης για ανίχνευση κακόβουλου λογισμικού.

Ο Vuong [48], χρησιμοποίησε ένα δέντρο απόφασης για να δημιουργήσει απλούς κανόνες ανίχνευσης που χρησιμοποιήθηκαν για την άμυνα έναντι επιθέσεων άρνησης υπηρεσίας και εντολής έγχυσης σε ρομποτικά οχήματα. Εξετάστηκαν χαρακτηριστικά εισόδου από τον κυβερνοχώρο, όπως η κίνηση δικτύου και τα δεδομένα δίσκου, και τα φυσικά χαρακτηριστικά εισόδου, όπως η ταχύτητα, η κατανάλωση ενέργειας και το jittering. Τα πειραματικά τους αποτελέσματα έδειξαν ότι διαφορετικές επιθέσεις έχουν διαφορετικό αντίκτυπο στις συμπεριφορές των ρομπότ, συμπεριλαμβανομένων των διαδικασιών στον κυβερνοχώρο και των φυσικών λειτουργιών, και η προσθήκη χαρακτηριστικών φυσικής εισόδου θα μπορούσε να βοηθήσει το δέντρο αποφάσεων να αυξήσει τη συνολική ακρίβεια ανίχνευσης και να μειώσει το ποσοστό ψευδώς θετικών.

Οι επιθέσεις APT χρησιμοποιούν μεθόδους κοινωνικής μηχανικής για να εισβάλουν σε διάφορα συστήματα, κάτι που φέρνει μεγάλα κοινωνικά ζητήματα. Στο Σχήμα 17 σχεδιάστηκε ένα σύστημα ανίχνευσης εισβολής με βάση το δέντρο αποφάσεων που ανιχνεύει επιθέσεις APT που ενδέχεται να αλλάξουν λογικά μετά την εισβολή σε ένα σύστημα. Η ιδέα ήταν να αναλυθούν οι πληροφορίες συμπεριφοράς μέσω ενός δέντρου αποφάσεων. Αυτό το σύστημα θα μπορούσε επίσης να ανιχνεύσει την πιθανότητα της αρχικής εισβολής και να μειώσει τον κίνδυνο στο ελάχιστο, απαντώντας σε επιθέσεις APT το συντομότερο δυνατό. Η ακρίβεια ανίχνευσης ήταν 84,7% στα πειράματά τους και θεωρείται υψηλή, λαμβάνοντας υπόψη τη δυσκολία στον εντοπισμό επιθέσεων APT που σχετίζονται με κακόβουλο λογισμικό, [49].

4.2.1.4 Ασφάλεια βασισμένη στα CNN

Στο παρελθόν αναπτύχθηκε ένα σύστημα ανίχνευσης εισβολής βασισμένο σε ένα νευρωνικό δίκτυο για την ανίχνευση επιπτώσεων επιθέσεων έγχυσης εντολών και απόκρισης παρακολουθώντας τις φυσικές συμπεριφορές των συστημάτων ελέγχου και απόκτησης δεδομένων. Τα πειραματικά αποτελέσματα έδειξαν ότι το IDS που βασίζεται στο νευρωνικό δίκτυο έχει εξαιρετική απόδοση στην ανίχνευση απόκρισης έγχυσης της επίθεσης Man in the Middle και DoS, αλλά δεν μπόρεσε να ανιχνεύσει επιθέσεις έγχυσης απόκρισης με επανάληψη (replay attack).

Επιπλέον προτάθηκε ένας υπολογιστικά αποδοτικός αλγόριθμος νευρωνικών δικτύων για την παροχή ενός σχήματος ειδοποίησης ανίχνευσης εισβολής για την επίγνωση της κατάστασης

ασφάλειας στον κυβερνοχώρο. Τα πειραματικά αποτελέσματα έδειξαν ότι αυτή η βελτιωμένη έκδοση του αλγορίθμου νευρωνικών δικτύων μείωσε τις απαιτήσεις μνήμης κατά 70% και μείωσε το χρόνο εκτέλεσης από 37 δευτερόλεπτα σε 1 δευτερόλεπτο, [9].

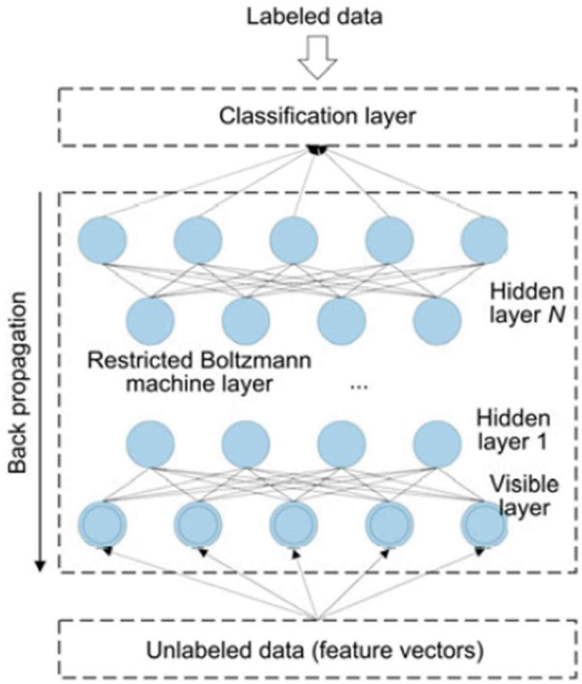
4.2.2 Λύσεις βαθιάς μάθησης για άμυνα απέναντι σε επιθέσεις στο κυβερνοχώρο

Η μέθοδος DL είναι πολύ παρόμοια με τη μέθοδο ML. Όπως αναφέρθηκε προηγουμένως, η επιλογή χαρακτηριστικών στη DL είναι αυτόματη και όχι χειροκίνητη και η DL προσπαθεί να αποκτήσει βαθύτερα χαρακτηριστικά από τα δοσμένα δεδομένα. Τα τρέχοντα προγράμματα DL περιλαμβάνουν το δίκτυα Deep Belief (Deep Belief Network - DBN), το επαναλαμβανόμενο νευρωνικό δίκτυο (Recurrent Neural Network - RNN) και το CNN. Σε αυτή την ενότητα περιγράφεται η χρήση διαφορετικών τύπων βαθιά νευρωνικών δικτύων για την άμυνα έναντι πολλών επιθέσεων δικτύου σε διαφορετικά σενάρια.

4.2.2.1 Άμυνα με βάση το δίκτυο Deep Belief

Το DBN είναι ένα μοντέλο παραγωγής πιθανοτήτων που αποτελείται από πολλαπλά περιορισμένα επίπεδα Boltzmann. Ο Li [9], αναφέρει μελέτες των DBN:

- Προτάθηκε μια προσέγγιση που βασίζεται σε DL και ονομάζεται "DeepFlow" για να εντοπίζει άμεσα κακόβουλο λογισμικό από τις ροές δεδομένων σε εφαρμογές Android. Αυτό το σχήμα υλοποιήθηκε με βάση το DBN (Σχήμα 18). Με βάση την αρχιτεκτονική DeepFlow, μπορούν να αναλυθούν δεδομένα σύνθετων χαρακτηριστικών επίθεσης. Η αρχιτεκτονική DeepFlow αποτελείται από τρία στοιχεία: το FlowDroid για εξαγωγή χαρακτηριστικών, το SUSI για κανονικοποίηση χαρακτηριστικών και το μοντέλο DBN DL για ταξινόμηση. Τα πειραματικά αποτελέσματα έδειξαν ότι το DeepFlow ξεπερνά τους παραδοσιακούς αλγόριθμους ML, όπως οι Naïve Bayes, PART, λογιστική παλινδρόμηση, SVM και Multi-Layer Perceptron (MLP).



Σχήμα 18: Δίκτυο Deep Belief.

- Εστιάζοντας στα προβλήματα στην ανίχνευση εισβολών, όπως περιττές πληροφορίες, μεγάλος χρόνος εκπαίδευσης κλπ., προτάθηκε ένα άλλο σχήμα ανίχνευσης εισβολής συνδυάζοντας το DBN και ένα πιθανοτικό νευρωνικό δίκτυο. Σε αυτή τη μέθοδο, τα ακατέργαστα δεδομένα μετατράπηκαν σε δεδομένα χαμηλής διάστασης και το DBN (με μη γραμμική ικανότητα μάθησης) εξήγαγε τα βασικά χαρακτηριστικά από τα αρχικά δεδομένα. Χρησιμοποιήθηκε ένας αλγόριθμος PSO για να βελτιστοποιηθεί ο αριθμός κόμβων κρυφού επίπεδου ανά επίπεδο. Στη συνέχεια χρησιμοποιήθηκε ένα πιθανοτικό νευρωνικό δίκτυο για να ταξινομηθούν τα δεδομένα χαμηλής διάστασης. Η αξιολόγηση απόδοσης έγινε χρησιμοποιώντας το σύνολο δεδομένων KDD CUP 1999 και έδειξε ότι αυτή η μέθοδος αποδίδει καλύτερα από τα παραδοσιακά πιθανοτικά νευρωνικά δίκτυα, PCA- πιθανοτικά νευρωνικά δίκτυα και ακατέργαστα DBN- πιθανοτικά νευρωνικά δίκτυα χωρίς βελτιστοποίηση.

4.2.2.2 Ανίχνευση επιθέσεων με βάση αναδρομικό νευρωνικό δίκτυο

Σε αντίθεση με τα παραδοσιακά νευρωνικά δίκτυα τροφοδοσίας (Feed-Forward Neural Networks - FNN), τα αναδρομικά νευρωνικά δίκτυα (Recurrent Neural Networks – RNN)

εισάγουν κατευθυντικούς βρόχους που μπορούν να χειριστούν τη συσχέτιση συμφραζομένων μεταξύ των εισόδων για την επεξεργασία δεδομένων ακολουθίας. Σύμφωνα με τον Li [9], αναφέρθηκε σε δύο μελέτες:

- Προτάθηκε σύστημα για την ταξινόμηση κακόβουλου λογισμικού Android, χρησιμοποιήθηκε ένα αναδρομικό νευρωνικό δίκτυο βραχυπρόθεσμης μνήμης. Όλα τα δίκτυα πέτυχαν την υψηλότερη ακρίβεια 89,7% στο πραγματικό σύνολο δεδομένων δοκιμής κακόβουλου λογισμικού Android.
- Προτάθηκε ένα σύστημα ανίχνευσης εισβολής βασισμένο σε σύννεφο για το Διαδίκτυο Οχημάτων (Internet of Vehicles - IoV) χρησιμοποιώντας ένα βαθύ MLP και ένα RNN. Το RNN, με ένα κρυφό επίπεδο βραχυπρόθεσμης μνήμης, αποδείχθηκε πολλά υποσχόμενο στην εκμάθηση του χρονικού πλαισίου διαφόρων επιθέσεων, όπως DoS, έγχυση εντολών και κακόβουλο λογισμικό. Πραγματοποιήθηκαν επίσης ορισμένα πειράματα σε πραγματικό περιβάλλον στον κυβερνοχώρο για να επαληθεύσουν την προσέγγισή τους.

4.2.2.3 Ανίχνευση επίθεσης με βάση συνελικτικό νευρωνικό δίκτυο

Το CNN είναι ένα είδος νευρωνικού δικτύου τροφοδοσίας που περιλαμβάνει ένα συνελικτικό επίπεδο και ένα επίπεδο συγκέντρωσης. Οι τεχνητοί νευρώνες μπορούν να ανταποκριθούν στα γύρω στοιχεία.

Ο Meng [44], πρότεινε ένα νέο μοντέλο, που ονομάζεται "ταξινόμηση κακόβουλου λογισμικού με βάση στατικές αλληλουχίες γονιδίων κακόβουλου λογισμικού" για ταξινόμηση κακόβουλου λογισμικού. Πρώτον, το σχήμα εξήγαγε τις αλληλουχίες γονιδίων κακόβουλου λογισμικού τόσο πληροφοριακών όσο και υλικών χαρακτηριστικών. Δεύτερον, προσπάθησε να προσδιορίσει την αναπαράσταση της συσχέτισης και της ομοιότητας κάθε κακόβουλου λογισμικού. Τέλος, για να επιτευχθεί ακριβής ταξινόμηση κακόβουλου λογισμικού, χρησιμοποιήθηκε το νευρωνικό δίκτυο για την ανάλυση των εξαγόμενων γονιδιακών ακολουθιών κακόβουλου λογισμικού. Η ακρίβεια ταξινόμησης ήταν έως και 98% με το προτεινόμενο σχήμα και ήταν πιο αποτελεσματικό και από το μοντέλο SVM.

4.2.2.4 Λύσεις που βασίζονται σε αυτόματο κωδικοποιητή για ανίχνευση απειλών

Ορισμένοι ερευνητές προσπάθησαν να χρησιμοποιήσουν τη DL για τη κατανομή ανίχνευσης επίθεσης σε ένα περιβάλλον υπολογιστικής ομίχλης. Προτάθηκε μια κατανεμημένη προσέγγιση

DL για την ανίχνευση επιθέσεων στον κυβερνοχώρο σε περιβάλλον υπολογιστικής ομίχλης. Το μοντέλο που υιοθετήθηκε ήταν ένας αυτόματος κωδικοποιητής για μη εποπτευόμενη DL. Τα πειραματικά αποτελέσματα έδειξαν ότι το προτεινόμενο βαθύ μοντέλο αποδίδει καλύτερα από τα απλά μοντέλα όσον αφορά το ποσοστό ψευδών ειδοποιήσεων, την ακρίβεια και την επεκτασιμότητα, [9].

Τέλος, άλλοι ερευνητές εστίασαν σε μοντέλα ανίχνευσης ανωμαλιών και άλλοι για ανίχνευση επιθέσεων DoS με αντίστοιχα καλά αποτελέσματα ακόμα και από υβριδικά μοντέλα.

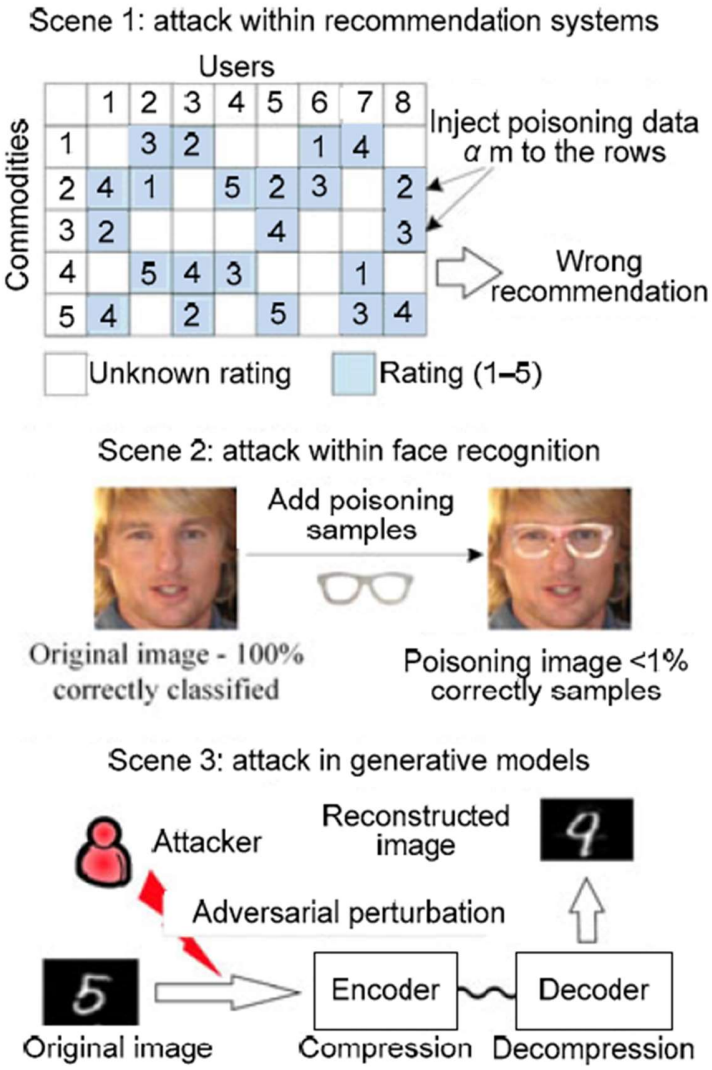
4.3 ΕΠΙΘΕΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΜΥΝΤΙΚΕΣ ΤΕΧΝΙΚΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

Στην πραγματικότητα, η τεχνητή νοημοσύνη αντιμετωπίζει επίσης απειλές για την ασφάλεια στον κυβερνοχώρο. Για παράδειγμα, η ML απαιτεί προστασία των δειγμάτων, των μοντέλων μάθησης και των διαδικασιών διαλειτουργικότητας.

4.3.1 Ανταγωνιστικές επιθέσεις στην τεχνητή νοημοσύνη

Οι παραδοσιακές προσεγγίσεις ML υποθέτουν ότι η κατανομή των δεδομένων εκπαίδευσης είναι σχεδόν ίδια με αυτή των δεδομένων δοκιμής. Σε ένα ανταγωνιστικό περιβάλλον, ωστόσο, τα σύγχρονα βαθιά δίκτυα είναι επιρρεπή σε επιθέσεις από αντίθετα δείγματα. Αυτά τα αντίθετα δείγματα επιβάλλουν μόνο μια μικρή διαταραχή στα αρχικά δείγματα, και έτσι ένα ανθρώπινο εικονικό σύστημα δεν θα μπορούσε να ανιχνεύσει τη διαταραχή. Μια τέτοια επίθεση μπορεί να οδηγήσει σε λανθασμένη ταξινόμηση του βαθιού νευρωνικού δικτύου. Η σημασία τέτοιων φαινομένων έχει προσελκύσει πολλούς ερευνητές να μελετήσουν τις ανταγωνιστικές επιθέσεις και την ασφάλεια της DL.

Το Σχήμα 19 δείχνει τρεις τυπικές ανταγωνιστικές επιθέσεις σε διαφορετικά σενάρια εφαρμογών. Στα συστήματα συστάσεων, η έγχυση λανθασμένων δεδομένων μπορεί να οδηγήσει σε εσφαλμένες συστάσεις. Στην αναγνώριση προσώπου, η προσθήκη έστω και μικρού αριθμού τροποποιημένων εικόνων μπορεί να προκαλέσει την εφαρμογή να κάνει μια σχεδόν εντελώς λανθασμένη ταξινόμηση. Η επιβολή μόνο μιας μικρής αντίθετης διαταραχής σε ένα παραγωγικό μοντέλο μπορεί να παράγει εντελώς εσφαλμένα ανακατασκευασμένα δείγματα.



Σχήμα 19: Ανταγωνιστικές επιθέσεις σε διαφορετικά σενάρια.

Προτάθηκε μια κατηγορία αλγορίθμων για εισάγουν διαταραχές στους ταξινομητές τροποποιώντας μόνο μερικά pixel μιας εικόνας αντί για να εισάγει διαταραχή σε ολόκληρη την εικόνα. Η λογική τους βασίστηκε σε μια ακριβή κατανόηση της χαρτογράφησης μεταξύ των εισόδων και των εξόδων του βαθιού νευρωνικού δικτύου. Τα αποτελέσματα έδειξαν ότι ο προτεινόμενος αλγόριθμος θα μπορούσε να παράγει δείγματα ταξινομημένα από ανθρώπους αλλά εσφαλμένα ταξινομημένα από ένα βαθύ δίκτυο με ποσοστό 97% όταν μόνο το 4,02% των χαρακτηριστικών εισόδου ανά δείγμα τροποποιήθηκαν. Άλλοι αντίστοιχοι αλγόριθμοι που εισήγαγαν διαταραχές σε εικόνες προτάθηκαν και εξήχθη το συμπέρασμα ότι η καταπολέμηση

της εκάστοτε επίθεσης επιτυγχάνεται με τη δημιουργία ενός αντίθετου δείγματος που είναι ειδικό για τη συνάρτηση απώλειας, χρησιμοποιώντας τις πληροφορίες κλίσης της συνάρτησης μικροαπωλειών του δικτύου για τη δημιουργία αντι-διαταραχής, [9].

4.3.2 Μέθοδοι άμυνας ενάντια σε ανταγωνιστικές επιθέσεις

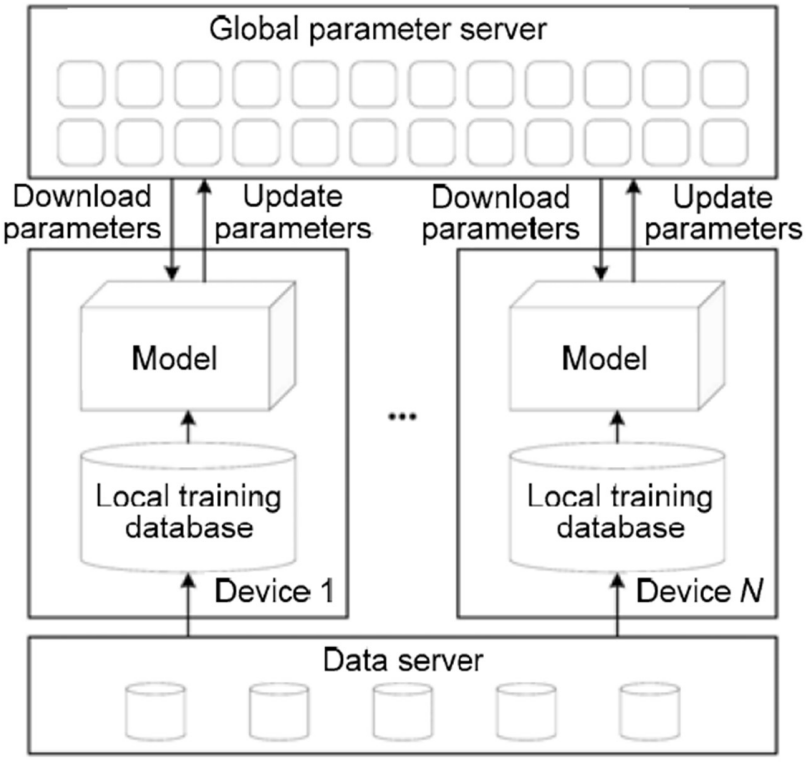
Ακολουθεί μια σύντομη περιγραφή μεθόδων άμυνας σε ανταγωνιστικές επιθέσεις:

- Τροποποίηση της εκπαιδευτικής διαδικασίας και δεδομένων εισόδου: Η ευρωστία ενός δικτύου σε βάθος βελτιώνεται με τη συνεχή εισαγωγή νέων τύπων αντίθετων δειγμάτων και την εκτέλεση εκπαίδευσης αντίπαλων δεδομένων. Για να διασφαλιστεί η αποτελεσματικότητα, αυτή η μέθοδος απαιτεί υψηλής έντασης αντίθετα δείγματα και η αρχιτεκτονική του δικτύου πρέπει να είναι εξοπλισμένη με επαρκή εκφραστική ισχύ. Αυτή η μέθοδος ονομάζεται "brute-force adversarial training", επειδή απαιτεί μεγάλο όγκο δεδομένων εκπαίδευσης.
- Τροποποίηση δικτύου: Έχει παρατηρηθεί ότι η απλή συγκέντωση των αυτόματων κωδικοποιητών απενεργοποίησης θορύβου στο αρχικό δίκτυο τους κάνει πιο ευάλωτους. Αποδείχτηκε ότι χρησιμοποιώντας την κανονικοποίηση της κλίσης εισόδου για τη βελτίωση της ευρωστίας έναντι της επίθεσης έχει καλό αποτέλεσμα σε συνδυασμό με το "brute-force adversarial training", αλλά η υπολογιστική πολυπλοκότητα είναι πολύ υψηλή. Μερικοί ερευνητές προσπάθησαν να χρησιμοποιήσουν βιολογικά εμπνευσμένες λύσεις.
- Χρήση επιπλέον δικτύου: Αποδείχθηκε ότι σε ένα σχήμα αν προστεθεί ένα ξεχωριστό εκπαιδευμένο δίκτυο στο αρχικό μοντέλο, μπορεί να επιτευχθεί μια μέθοδος που δεν απαιτεί παράγοντες προσαρμογής και δεν επηρεάζεται από το αλλοιωμένο δείγμα. Μελετήθηκαν επίσης μέθοδοι συμπίεσης χαρακτηριστικών, εάν το δείγμα είναι αντίθετο ή όχι χρησιμοποιώντας δύο μοντέλα. Σε άλλες μελέτες εκπαιδεύτηκε ένα μοντέλο ώστε να αντιμετωπίζει όλες τις εισερχόμενες εικόνες ως θόρυβο, μαθαίνοντας πρώτα πώς να εξομαλύνουν την εικόνα και μετά ταξινομώντας την.

4.3.3 Κατασκευή ασφαλών συστημάτων τεχνητής νοημοσύνης

Το 2015 προτάθηκε για πρώτη φορά η κατασκευή συστήματος (από τους Shokri και Shmatikov) DL για διατήρηση της ιδιωτικότητας κάτω από ένα κατανεμημένο σύστημα εκπαίδευσης (Σχήμα

20) που επιτρέπει σε πολλά μέρη να μάθουν συνεργατικά ένα ακριβές μοντέλο νευρωνικού δικτύου χωρίς να διαρρεύσουν τα σύνολα δεδομένων εισόδου τους. Η βασική καινοτομία είναι η επιλεκτική κοινή χρήση παραμέτρων βαθιού νευρωνικού δικτύου κατά τη διάρκεια της εκπαίδευσης των μοντέλων, γεγονός που καθιστά το σχήμα αποτελεσματικό και ισχυρό επειδή η εκπαίδευση μπορεί να εκτελεστεί ασύγχρονα. Στα πειράματα όπου χρησιμοποιήθηκαν δύο σύνολα δεδομένων: το MNIST και το SVHN, αξιολογήθηκε το σύστημα αυτό. Τα αποτελέσματα έδειξαν υψηλή ακρίβεια ταξινόμησης και στα δύο σύνολα δεδομένων, ακόμη και όταν οι συμμετέχοντες μοιράστηκαν το 10% των παραμέτρων τους. Αργότερα, το 2018, αποδείχτηκε ότι στο σύστημα των Shokri και Shmatikov, οι διαβαθμίσεις που μοιράζονται στον διακομιστή σύννεφο ενδέχεται να παραβιάζονται, οδηγώντας σε τοπικές διαρροές δεδομένων. Για την αποφυγή αυτού του φαινομένου χρησιμοποιήθηκε προσθετική ομομορφική κρυπτογράφηση για να επιτρέψει τον υπολογισμό της κρυπτογράφησης σε όλες τις διαβαθμίσεις. Το tradeoff αυτού του σχήματος είναι το κόστος της αυξημένης επιβάρυνσης επικοινωνίας μεταξύ του διακομιστή σύννεφου και των συμμετεχόντων στη DL.



Σχήμα 20: Συστήματα ασφαλούς κατανεμημένης μηχανικής/ βαθιάς μάθησης.

Σε ένα συνεργατικό περιβάλλον μάθησης, οι κινητές συσκευές μπορούν να συμμετέχουν στη διαδικασία μάθησης και οι χρήστες τερματικών επωφελούνται από το κοινό μοντέλο που εκπαιδεύεται σε κατανεμημένα δεδομένα. Το 2017 σχεδιάστηκε ένα πρακτικό ασφαλές συγκεντρωτικό πρωτόκολλο για δεδομένα υψηλών διαστάσεων σε ML που διατηρούν το απόρρητο. Αυτό το συγκεντρωτικό πρωτόκολλο επιτρέπει στον διακομιστή να υπολογίζει με ασφάλεια το άθροισμα των παραμέτρων που συλλέγονται από πολλές κινητές συσκευές με κατανεμημένο τρόπο. Τα πειραματικά αποτελέσματα έδειξαν ότι το προτεινόμενο πρωτόκολλο παράγει χαμηλότερη επιβάρυνση και έχει καλύτερη ανοχή σε σφάλματα και μεγαλύτερη ευρωστία, [9], [14].

4.4 ΣΥΝΟΨΗ

Στο παρόν κεφάλαιο μελετήθηκε η ενοποίηση της τεχνητής νοημοσύνης και της ασφάλειας του κυβερνοχώρου από δύο πτυχές: Από τη μία πλευρά, αναλύθηκε η χρήση τεχνολογιών που σχετίζονται με την τεχνητή νοημοσύνη (ML και DL) για τον εντοπισμό και την αντιμετώπιση διαφόρων τύπων επιθέσεων στον κυβερνοχώρο. Από την άλλη πλευρά, ενόψει των επιθέσεων που μπορεί να αντιμετωπίσει η ίδια η τεχνητή νοημοσύνη και των απαιτήσεων προστασίας ασφάλειας, εξετάστηκαν πρώτα διάφορες επιθέσεις τις οποίες μπορεί να υποστούν συστήματα τεχνητής νοημοσύνης σε ένα ανταγωνιστικό περιβάλλον. Εντέλει περιγράφηκαν αμυντικές στρατηγικές για διάφορα είδη επιθέσεων και πώς μπορεί να δημιουργηθεί ένα ασφαλές σύστημα AI σε ένα κατανεμημένο περιβάλλον ML/ DL.

Με την ταχεία ανάπτυξη της τεχνητής νοημοσύνης και της ασφάλειας του κυβερνοχώρου, η ενοποίηση αυτών των δύο κλάδων θα παρουσιάζει όλο και περισσότερα σενάρια εφαρμογών. Παρόλο που οι νέες τεχνολογίες τεχνητής νοημοσύνης, όπως η DL, διαδραματίζουν σημαντικό ρόλο στην άμυνα του κυβερνοχώρου, το ίδιο το σύστημα AI μπορεί επίσης να δεχθεί επίθεση ή να εξαπατηθεί, και να οδηγήσει σε εσφαλμένα αποτελέσματα ταξινόμησης ή πρόβλεψης. Για παράδειγμα, σε ανταγωνιστικά περιβάλλοντα, η εκμετάλλευση των δειγμάτων εκπαίδευσης θα έχει ως αποτέλεσμα τοξικές επιθέσεις και η εκμετάλλευση των δειγμάτων δοκιμής θα έχει ως αποτέλεσμα επιθέσεις αποφυγής. Οι επιθέσεις σε ανταγωνιστικά περιβάλλοντα έχουν σκοπό να υπονομεύσουν την ακεραιότητα και τη χρηστικότητα διαφόρων εφαρμογών τεχνητής νοημοσύνης και να παραπλανήσουν τα νευρωνικά δίκτυα χρησιμοποιώντας αντίθετα δείγματα, με αποτέλεσμα

οι ταξινομητές να εξάγουν λανθασμένη ταξινόμηση. Βεβαίως υπάρχουν και αντίστοιχα αμυντικά μέτρα έναντι των επιθέσεων. Αυτά τα αμυντικά μέτρα επικεντρώνονται κυρίως σε τρεις πτυχές: (1) τροποποίηση της εκπαιδευτικής διαδικασίας ή των δειγμάτων εισόδου, (2) τροποποίηση του ίδιου του δικτύου, όπως προσθήκη περισσότερων επιπέδων/ υποδικτύων και αλλαγή της συνάρτησης απώλειας/ ενεργοποίησης, (3) χρήση ορισμένων εξωτερικών μοντέλων ως προσθήκες κατά την ταξινόμηση δειγμάτων που δεν έχουν εμφανιστεί. Καθώς τα μοντέλα DL γίνονται πιο περίπλοκα και τα σύνολα δεδομένων γίνονται μεγαλύτερα, οι κεντρικοποιημένες μέθοδοι εκπαίδευσης δεν μπορούν να προσαρμοστούν σε αυτές τις νέες απαιτήσεις. Έχουν εμφανιστεί κατανεμημένοι τρόποι μάθησης, όπως η συνεργατική μάθηση που κυκλοφόρησε η Google, επιτρέποντας σε πολλά έξυπνα τερματικά να μάθουν ένα κοινό μοντέλο με συνεργατικό τρόπο. Ωστόσο, όλα τα δεδομένα εκπαίδευσης αποθηκεύονται σε τερματικές συσκευές, γεγονός που φέρνει πολλές προκλήσεις ασφαλείας: Πώς να εξασφαλιστεί ότι το μοντέλο δεν έχει κλαπεί με κακόβουλο τρόπο και ότι μπορεί να δημιουργήσει ένα κατανεμημένο σύστημα μηχανικής μάθησης με προστασία απορρήτου; Αυτά αποτελούν ακόμα ερευνητικές προκλήσεις.

5. ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΕ ΣΥΝΔΥΑΣΜΟ ΜΕ ΒΙΟΜΕΤΡΙΚΗ ΤΕΧΝΟΛΟΓΙΑ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Οι βιομετρικές λύσεις χρησιμοποιούνται συνήθως για ασφάλεια και έλεγχο πρόσβασης σε επιχειρήσεις και κυβερνητικούς οργανισμούς. Η κυβέρνηση των ΗΠΑ έχει δείξει έντονο ενδιαφέρον για τις βιομετρικές εφαρμογές και έχει αφιερώσει μεγάλα χρηματικά ποσά σε προηγμένα ερευνητικά προγράμματα επιχειρήσεων που προσφέρουν βιομετρικές λύσεις.

Η Intelligence Advanced Research Projects Activity (IARPA), ένας κυβερνητικός οργανισμός των ΗΠΑ που χρηματοδοτεί την ακαδημαϊκή και βιομηχανική έρευνα, ανακοίνωσε την έναρξη του προγράμματος Odin τον Οκτώβριο του 2017. Το Odin στοχεύει να αναπτύξει τεχνολογίες ανίχνευσης επιθέσεων με βάση τα βιομετρικά χαρακτηριστικά, για τον καλύτερο εντοπισμό μη εξουσιοδοτημένων χρηστών και απατεώνων. Τα άλλα προγράμματα του IARPA, όπως το Biometrics Exploitation Science & Technology και το Janus στοχεύουν επίσης στο να "προωθήσουν σημαντικά τις βιομετρικές τεχνολογίες".

Τον Απρίλιο του 2017, η IARPA ανέθεσε στον πάροχο βιομετρικών λύσεων τεχνητής νοημοσύνης Crossmatch ένα συμβόλαιο 5,8 εκατομμυρίων δολαρίων για την "ανάπτυξη τεχνολογιών επόμενης γενιάς για ανίχνευση επιθέσεων με βάση τα βιομετρικά χαρακτηριστικά". Τον Ιούνιο του 2017, χρηματοδότησε ένα τετραετές συμβόλαιο 12,5 εκατομμυρίων δολαρίων με το SRI International, ένα ανεξάρτητο, μη κερδοσκοπικό ερευνητικό κέντρο για την "αντιμετώπιση των ευάλωτων σημείων στα τρέχοντα βιομετρικά συστήματα ασφαλείας", και πιο συγκεκριμένα, σε σαρωτές δακτυλικών αποτυπωμάτων, ίριδας και προσώπου.

Η βιομετρική τεχνολογία έχει προσελκύσει το ενδιαφέρον πολλών επενδυτών και εκτός του χώρου της IARPA. Η SenseTime, μια κινεζική εταιρεία τεχνητής νοημοσύνης που προσφέρει μια σειρά επιχειρηματικών λύσεων τεχνητής νοημοσύνης, συμπεριλαμβανομένων των βιομετρικών χαρακτηριστικών, λέει ότι σημείωσε ρεκόρ συγκεντρώνοντας 410 εκατομμύρια δολάρια τον Ιούλιο του 2017, [6].

Σε αυτή την ενότητα θα παρουσιαστούν βασικές τεχνολογίες τεχνητής νοημοσύνης για λύσεις ασφαλείας βιομετρικών χαρακτηριστικών, όπως αναγνώριση προσώπου, αναγνώριση φωνής και δακτυλικού αποτυπώματος. Επίσης, θα αναφερθούν και οργανισμοί – πλατφόρμες που παρέχουν βιομετρικές λύσεις.

5.1 ΑΝΑΓΝΩΡΙΣΗ ΠΡΟΣΩΠΟΥ

Όπως έχει αναφερθεί, ένα βιομετρικό σύστημα αναγνώρισης προσώπου αναγνωρίζει και επαληθεύει την ταυτότητα ενός ατόμου εξάγοντας και συγκρίνοντας επιλεγμένα χαρακτηριστικά του προσώπου από μια ψηφιακή εικόνα ή ένα καρέ βίντεο σε μια βάση δεδομένων προσώπων. Για παράδειγμα, ένας αλγόριθμος μπορεί να αναλύσει την απόσταση μεταξύ των ματιών, το πλάτος της μύτης, το βάθος των κογχών των ματιών, το σχήμα των ζυγωματικών, το μήκος της γραμμής της γνάθου κ.λπ., και να κωδικοποιήσει τα αντίστοιχα δεδομένα ως "αποτυπώματα προσώπου", τα οποία μπορεί στη συνέχεια να χρησιμοποιηθούν για την εύρεση κατάλληλων αντιστοιχίσεων σε μια βάση δεδομένων, [8].

5.1.1 Επιρροή της κάλυψης προσώπου στη βιομετρική αναγνώριση προσώπου στην εποχή της πανδημίας

Η χρήση καλυμμάτων προσώπου, όπως μάσκες, κρύβουν σημαντικό μέρος του κάτω μέρους του προσώπου. Τέτοια εμπόδια αλλάζουν δραματικά τις συνθήκες λειτουργίας για πολλές τεχνολογίες βιομετρικής αναγνώρισης. Τέτοιες αλλαγές μπορούν να κάνουν τη βιομετρική αναγνώριση ιδιαίτερα δύσκολη.

Οι φυσικές διαφορές μεταξύ των ατόμων αποδίδουν έναν καλό διαχωρισμό στην κατηγοριοποίηση των κλάσεων και έτσι κάνει τη χρήση των χαρακτηριστικών του προσώπου για βιομετρική αναγνώριση ιδιαίτερα ελκυστική. Οι παραδοσιακές λύσεις βασίζονται σε χαρακτηριστικά που βασίζονται στην υφή, σε σημαντικά σημεία προσώπου και άλλους περιγραφικούς παράγοντες για την αναγνώριση του προσώπου. Πιο πρόσφατα, η χρήση της βαθιάς μάθησης και των μαζικής εκπαίδευσης συνόλων δεδομένων έχει οδηγήσει σε σημαντική πρόοδο. Τα καλύτερα συστήματα αποδίδουν αξιόπιστα ακόμη και με εξαιρετικά χαμηλής ποιότητας δείγματα δεδομένων (και χωρίς περιορισμούς). Οι περισσότερες εργασίες πριν από την πανδημία του COVID-19 αναφέρονται σε εμπόδια από, π.χ., γυαλιά ηλίου, κομμένες λήψεις ή σκιές. Η χρήση μάσκας προσώπου επομένως παρουσιάζει μια νέα και σημαντική πρόκληση για τα συστήματα αναγνώρισης προσώπου, ειδικά λαμβάνοντας υπόψη τις αυστηρές απαιτήσεις λειτουργίας για σενάρια εφαρμογών στα οποία χρησιμοποιείται συχνά η τεχνολογία αναγνώρισης προσώπου, π.χ. αυτοματοποιημένος έλεγχος των συνόρων. Η απαίτηση για εξαιρετικά χαμηλά ποσοστά σφάλματος εξαρτάται συνήθως από τη λήψη "καθαρών" εικόνων καλής ποιότητας.

Η πιο σημαντική αξιολόγηση της επίδρασης των μασκών στις λύσεις αναγνώρισης προσώπου διενεργήθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST). Η αξιολόγηση πραγματοποιήθηκε χρησιμοποιώντας ένα μεγάλο σύνολο δεδομένων εικόνων προσώπων με ψηφιακά δημιουργημένες μάσκες διαφορετικού μεγέθους, σχήματος και χρώματος. Η μελέτη εξέτασε την απόδοση αναγνώρισης προσώπου των αλγορίθμων που υποβλήθηκαν στη δοκιμή Face Recognition Vendor Test (FRVT) όσον αφορά την απόδοση βιομετρικής επαλήθευσης (δηλαδή, συγκρίσεις ένας προς έναν). Τα ποσοστά ψευδώς αρνητικών σφαλμάτων (δηλαδή, ποσοστό ψευδούς μη αντιστοίχισης) για αλγόριθμους που υποβλήθηκαν πριν από την πανδημία, παρατηρήθηκαν ότι αυξάνονται κατά μία τάξη μεγέθους, ακόμη και για τους πιο αξιόπιστους αλγόριθμους. Ακόμη και ορισμένοι από τους αλγόριθμους με την καλύτερη απόδοση (όπως κρίθηκε από την αξιολόγηση με μη καλυμμένα πρόσωπα) απέτυχαν σχεδόν ολοκληρωτικά, με ποσοστά ψευδώς αρνητικών σφαλμάτων έως και 50%.

Φυσικά, αυτά τα αποτελέσματα είναι αναμενόμενα, δεδομένου ότι τα συστήματα που σχεδιάστηκαν πριν από την πανδημία ήταν απίθανο να έχουν βελτιστοποιηθεί για δεδομένα καλυμμένων προσώπων. Η ίδια η μελέτη είχε και κάποιους περιορισμούς, π.χ. Αντί να χρησιμοποιεί γνήσιες εικόνες που συλλέγονται από άτομα που φορούσαν μάσκες, χρησιμοποίησε συνθετικά δημιουργημένες εικόνες όπου οι μάσκες τοποθετούνταν από πάνω, χρησιμοποιώντας τα βασικά σημεία προσώπου που προέκυπταν αυτόματα. Παρά τις ελλείψεις, η μελέτη υπογραμμίζει ωστόσο τις γενικές προκλήσεις για τη βιομετρική αναγνώριση προσώπου από καλύμματα προσώπου και μάσκες. Οι γενικές παρατηρήσεις είναι ότι: 1) η μείωση της αξιοπιστίας πιστοποίησης αυξάνεται όταν η μάσκα καλύπτει μεγαλύτερο ποσοστό του προσώπου συμπεριλαμβανομένης της μύτης, 2) η αξιοπιστία μειώνεται περισσότερο για τις ζευγαρωμένες βιομετρικές συγκρίσεις παρά για τις μη ζευγαρωμένες συγκρίσεις, δηλαδή οι μάσκες αυξάνουν το ποσοστό ψευδούς μη αντιστοίχισης περισσότερο από το ποσοστό ψευδούς αντιστοίχισης, 3) διαφορετικά σχήματα και χρώματα μάσκας οδηγούν σε διαφορές στην αξιοπιστία της πιστοποίησης, εύρημα που υπογραμμίζει την ανάγκη αξιολόγησης με χρήση γνήσιων δεδομένων καλυμμένων προσώπων, 4) σε πολλές περιπτώσεις, τα καλυμμένα πρόσωπα δεν εντοπίζονται καν.

Η χρήση διαφανών μασκών ή ασπίδων μπορεί να καταπολεμήσει σε κάποιο βαθμό τον αντίκτυπο των αδιαφανών μασκών στα συστήματα αναγνώρισης προσώπου. Οι διαφανείς μάσκες, όπως αυτές που φαίνονται στο Σχήμα 21, επιτρέπουν σε κάποιο τμήμα του καλυμμένου προσώπου

να παραμένει ορατό, αλλά ακόμη και η επίδρασή τους είναι πιθανότατα ασαφής. Οι διαφανείς μάσκες μπορεί να προκαλέσουν αντανακλάσεις φωτός, οπτικές παραμορφώσεις ή/ και θόλωση. Τόσο οι αδιαφανείς όσο και οι διαφανείς μάσκες, καθώς και οι στρατηγικές για την αντιμετώπιση των επιπτώσεών τους, ενδέχεται να αυξήσουν τον κίνδυνο επιθέσεων παρουσίασης. Για παράδειγμα, είναι κατανοητό ότι μάσκες με συγκεκριμένα μοτίβα θα μπορούσαν να χρησιμοποιηθούν για να εξαπολύσουν επιθέσεις απόκρυψης ή πλαστοπροσωπίας.

Σχήμα 21: Παραδείγματα εναλλακτικών προστατευτικών μασκών: Η πρώτη είναι η διαφανής μάσκα και η δεύτερη είναι η ασπίδα προσώπου.

Ανεξάρτητα από τον ακριβή τύπο μάσκας προσώπου, η χρήση μιας μάσκας μπορεί να έχει επίδραση στην ποιότητα της εικόνας του προσώπου. Τα περισσότερα βιομετρικά συστήματα εκτιμούν την ποιότητα μιας ανιχνευμένης εικόνας προσώπου πριν από την εξαγωγή χαρακτηριστικών. Αυτή η εκτίμηση ποιότητας υποδεικνύει την καταλληλότητα της εικόνας για σκοπούς αναγνώρισης. Για τα υπάρχοντα συστήματα, οι διαμορφώσεις χαμηλής ποιότητας ενδέχεται να οδηγήσουν σε παράβλεψη δειγμάτων με μάσκες προσώπου και, συνεπώς, να αυξήσουν το ποσοστό αποτυχίας.

Οι μελέτες που έχουν πραγματοποιηθεί μέχρι στιγμής υπογραμμίζουν τις προκλήσεις που αντιμετωπίζουν τα συστήματα αναγνώρισης στην εποχή του COVID-19 και εγείρουν πολλά ανοιχτά ερωτήματα. Αυτά περιλαμβάνουν, αλλά δεν περιορίζονται σε δοκιμές μεγάλης κλίμακας που χρησιμοποιούν εικόνες με πραγματικές και όχι ψηφιακά δημιουργημένες μάσκες, ταυτοποίηση (δηλαδή αναζήτηση ένα προς πολλά), δημογραφικές διαφοροποιήσεις, παρουσία πρόσθετων εμποδίων όπως γυαλιά, επίδραση στην ποιότητα εικόνας προσώπου, απόκτηση δεδομένων χωρίς γενικούς περιορισμούς, καθώς και επιπτώσεις στην ακρίβεια των συστημάτων αναγνώρισης, [10].

5.1.2 Περίπτωση της Trueface.AI – για ανίχνευση απάτης

Ορισμένες φορές, η τεχνολογία αναγνώρισης προσώπου μπορεί να μην είναι σε θέση να διακρίνει τη διαφορά μεταξύ ενός ανθρώπινου προσώπου και μιας φωτογραφίας. Ως αποτέλεσμα, αυτή η ευπάθεια μπορεί να υπονομεύσει σε μεγάλο βαθμό την ασφάλεια ενός συστήματος. Σε μια προσπάθεια για να αντιμετωπιστεί αυτή η πρόκληση, στο Trueface.AI, οι προγραμματιστές ενός κουδουνιού αναγνώρισης προσώπου που ονομάζεται Chui, χρησιμοποιούν τεχνολογία βαθιάς μάθησης και αναγνώρισης προσώπου για να διακρίνουν ένα ανθρώπινο πρόσωπο από μια φωτογραφία, όπως απεικονίζεται στο Σχήμα 22.

Σχήμα 22: Παράδειγμα προσπάθειας παραβίασης συστήματος αναγνώρισης προσώπου.

Ο αλγόριθμος βαθιάς μάθησης του Trueface.AI εκπαιδεύτηκε σε χιλιάδες παραδείγματα "επιθέσεων" που συνέλεξε η ομάδα προγραμματιστών όλα αυτά τα χρόνια. Έχει αναφερθεί ότι η τεχνολογία του Trueface.AI εφαρμόζεται από εταιρείες σε διάφορους κλάδους, συμπεριλαμβανομένης της υγειονομικής περίθαλψης και των τραπεζών, [6], [7].

5.1.3 Περίπτωση της Kairos – για ανίχνευση απάτης

Αναμφισβήτητα μία από τις μεγαλύτερες εταιρείες στον χώρο της αναγνώρισης προσώπου με χρήση τεχνητής νοημοσύνης, η Kairos χρησιμοποιεί τη μηχανική μάθηση και την υπολογιστική όραση για να τρέξει τα εργαλεία της, που αφορούν τυπικά χαρακτηριστικά αναγνώρισης προσώπου και άλλες επιλογές όπως την ανίχνευση φύλου, ηλικίας και εθνότητας.

Από την ίδρυση της εταιρείας το 2012, η Kairos φέρεται να έχει συγκεντρώσει 4,26 εκατομμύρια δολάρια σε συνολική μετοχική χρηματοδότηση από έναν συνδυασμό επενδυτών venture, angel, seed και Series A και B. Το 2015, η εταιρεία πραγματοποίησε κατά προσέγγιση

2,7 εκατομμύρια δολάρια εξαγορά της IMRSV (μιας εταιρείας λογισμικού) που σύμφωνα με πληροφορίες "μετατρέπει οποιαδήποτε web κάμερα σε έξυπνο αισθητήρα".

Η Kairos έχει δημοσιεύσει ορισμένες περιπτωσιολογικές μελέτες στον ιστότοπό της για να παρέχει παραδείγματα των εφαρμογών της σε πολλούς κλάδους. Για παράδειγμα, για μια εταιρεία το api Kairos εντόπισε πιθανή ετήσια εξοικονόμηση 14,5 εκατομμυρίων δολαρίων, εντοπίζοντας ασυμφωνίες σε μη αυτόματες κάρτες χρόνου εργασίας, [6], [7].

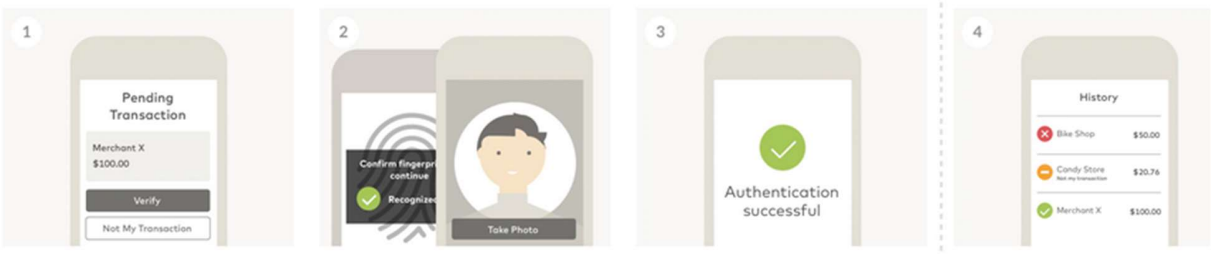
5.1.4 Περίπτωση της Walmart – για αποτροπή κλοπής

Στον τομέα του λιανικού εμπορίου, οι μεγάλοι έμποροι λιανικής φαίνεται να εξερευνούν την τεχνολογία αναγνώρισης προσώπου για λόγους ασφαλείας. Ωστόσο, ορισμένες προσπάθειες αντιμετωπίστηκαν με επιφυλάξεις από πλευράς ιδιωτικότητας των καταναλωτών.

Το 2015, η Walmart φέρεται να άρχισε να δοκιμάζει την αναγνώριση προσώπου σε ορισμένα από τα καταστήματά της σε μια προσπάθεια να εντοπίσει τους κλέφτες, αλλά στη συνέχεια σταμάτησε τη χρήση της. Η ίδια η εταιρεία αργότερα αναγνώρισε δημοσίως τις δοκιμές και ισχυρίστηκε ότι η τεχνολογία δεν παρείχε επαρκή απόδοση επένδυσης (Return of Investment - ROI) για να δικαιολογήσει τη συνέχιση της χρήσης της. Φαίνεται ότι η δυσμενής φήμη που απέκτησε η τεχνολογία, μπορεί να ήταν ένας από τους κύριους λόγους πίσω από αυτή την απόφαση, [6], [7].

5.1.5 Περίπτωση της εφαρμογής της MasterCard για κινητές συσκευές – για ασφάλεια λογαριασμού

Οι κωδικοί πρόσβασης έχουν γίνει ένα πρόσθετο βάρος κατά την πλοήγηση στο περιβάλλον του Διαδικτύου. Η MasterCard είναι ένα από τα χρηματοπιστωτικά ιδρύματα που προσπάθησαν να παρακάμψουν την ανάγκη για κωδικούς πρόσβασης μέσω της αναγνώρισης προσώπου. Η εφαρμογή MasterCard Identity Check Mobile επαληθεύει τις ηλεκτρονικές πληρωμές είτε μέσω δακτυλικών αποτυπωμάτων είτε μέσω αναγνώρισης προσώπου. Όπως φαίνεται στην , οι χρήστες της εφαρμογής μπορούν να επαληθεύσουν τις πληρωμές τους χρησιμοποιώντας την κάμερα του smartphone τους για να τραβήξουν μια φωτογραφία των προσώπων τους.



Σχήμα 23: Στιγμιότυπα από πιστοποίηση προσώπου στην εφαρμογή της MasterCard.

Τα αποτελέσματα από μια έρευνα καταναλωτών από 750 χρήστες της εφαρμογής στην Ολλανδία αποκάλυψαν ότι το 92 τοις εκατό θεώρησαν την εφαρμογή "πιο βολική από τους κωδικούς πρόσβασης". Σε μια δοκιμή στις ΗΠΑ με 200 χρήστες, το 86 τοις εκατό των ερωτηθέντων βρήκαν την εφαρμογή "πιο εύχρηστη από τους κωδικούς πρόσβασης". Γενικότερα, σε έρευνα της MasterCard, αναφέρθηκε ότι η πλειοψηφία των χρηστών είτε πιστεύει περισσότερο στην ασφάλεια των βιομετρικών λύσεων, είτε ξεχνάει το PIN της. Εν κατακλείδι, η MasterCard υπολογίζει ότι η εφαρμογή είναι θα καλύψει μεταφορές χρημάτων από το κινητό με βιομετρικό τρόπο αξίας 2.5 τρισεκατομμυρίων δολαρίων, [6], [7], [50].

5.2 ΑΝΑΓΝΩΡΙΣΗ ΦΩΝΗΣ

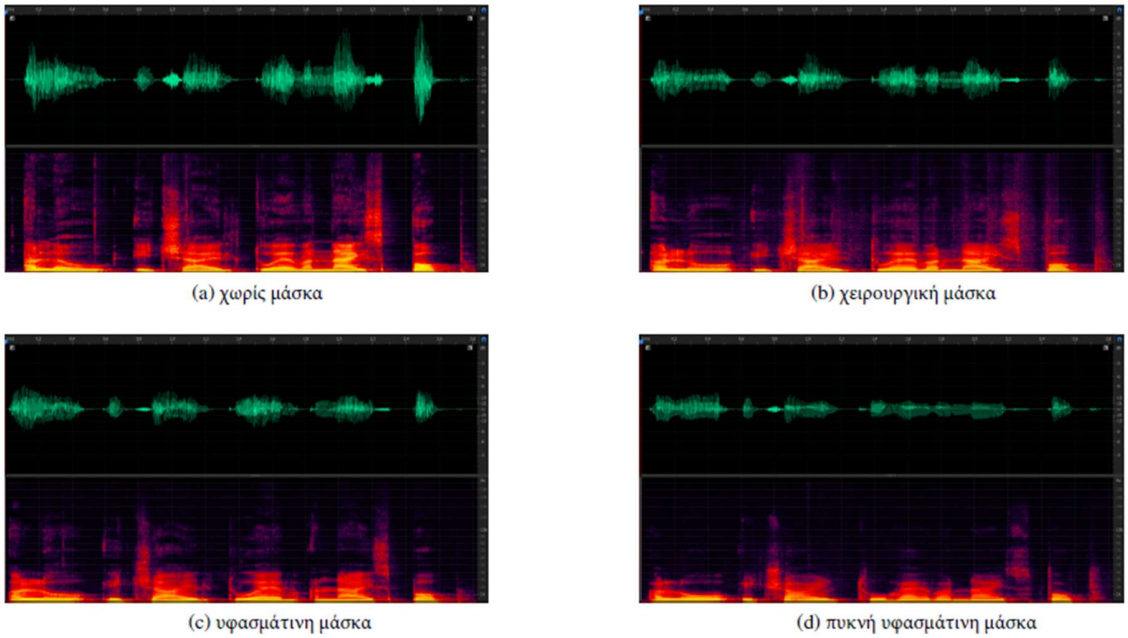
Η αναγνώριση ομιλητή ή φωνής διαφέρει από την αναγνώριση ομιλίας στο ότι η πρώτη αναγνωρίζει και προσδιορίζει έναν ομιλητή χρησιμοποιώντας βιομετρικά στοιχεία φωνής και η δεύτερη αναλύει αυτό που λέγεται. Τα βιομετρικά χαρακτηριστικά της φωνής περιλαμβάνουν τόσο τα φυσικά χαρακτηριστικά, όπως το σχήμα της φωνητικής οδού που είναι υπεύθυνη για την άρθρωση και τον έλεγχο της παραγωγής ομιλίας, όσο και χαρακτηριστικά της συμπεριφοράς όπως το ύψος, ο ρυθμός και ο τόνος κ.λπ.

Οι βιομετρικές λύσεις φωνής ψηφιοποιούν τις λέξεις μειώνοντάς τις σε τμήματα που περιλαμβάνουν κωδικοποιημένες συχνότητες ή μορφοποιητές και παράγουν ένα μοντέλο "φωνητικής αποτύπωσης" μοναδικό για ένα άτομο. Αυτή η φωνητική αποτύπωση χρησιμοποιείται για την αναγνώριση και τον έλεγχο ταυτότητας του ομιλούμενου, [6].

5.2.1 Επιρροή της κάλυψης προσώπου στη βιομετρική αναγνώριση φωνής στην εποχή της πανδημίας

Οι συνέπειες του COVID-19 στα συστήματα αναγνώρισης φωνής εξαρτώνται σε μεγάλο βαθμό από την επίδραση των μασκών προσώπου στην παραγωγή ομιλίας. Οι μάσκες προσώπου

εμποδίζουν τα κάτω μέρη του προσώπου και αποτελούν εμπόδιο στη συνήθη μετάδοση των ήχων της ομιλίας παρεμβαίνοντας στις διακυμάνσεις της πίεσης του αέρα που προέρχονται από το στόμα και τη μύτη. Το αποτέλεσμα είναι παρόμοιο με τα ακουστικά φίλτρα, όπως τα ηχοαπορροφητικά υφάσματα που χρησιμοποιούνται για ηχομόνωση ή τα στόμια εξάτμισης αυτοκινήτων. Δεδομένου ότι οι μάσκες έχουν σχεδιαστεί για να εμποδίζουν τη διάδοση ικών σωματιδίων μικρών μεγεθών, αποτελούνται από ιδιαίτερα πυκνά στρώματα υφάσματος. Το αποτέλεσμα στην ομιλία είναι μια συχνά σημαντική εξασθένηση και αλλοίωση. Οι πυκνότερες δομές υφάσματος τείνουν να απορροφούν ήχο σε συχνότητες πάνω από 2 kHz, ενώ οι παχύτερες δομές απορροφούν ήχο συχνοτήτων κάτω των 500 Hz. Με αυτές τις ζώνες να επικαλύπτουν αυτές της ανθρώπινης ομιλίας, οι μάσκες εξασθενούν και παραμορφώνουν τα σήματα ομιλίας και ως εκ τούτου υποβαθμίζουν την αξιοπιστία των βιομετρικών συστημάτων φωνής που εκπαιδεύονται με κανονική (χωρίς μάσκα) ομιλία. Οι μάσκες μπορούν επίσης να έχουν αρνητικό αντίκτυπο στα συστήματα ανίχνευσης επιθέσεων παρουσίασης (Presentation Attack Detection - PAD), τα οποία παρουσιάζουν αντίμετρα για τη διάκριση της νόμιμης και της πλαστής ομιλίας. Αυτά τα συστήματα βασίζονται σε φασματικά χαρακτηριστικά που λαμβάνονται από τις δύο κατηγορίες. Γίνεται σαφές ότι οποιαδήποτε τροποποίηση/ απόκλιση του χρήσιμου φάσματος έχει ως αποτέλεσμα μεγαλύτερη δυσκολία στην ανίχνευσή του. Επιπλέον, άλλα συστήματα αντιμέτρων βασίζονται στην ανίχνευση του θορύβου POP: ένας καλόπιστος χρήστης εκπέμπει θόρυβο pop που προκαλείται φυσικά όταν μιλάει κοντά στο μικρόφωνο. Αυτός ο θόρυβος μειώνεται από τη μάσκα και, κατά συνέπεια, η απόδοση του PAD μειώνεται. Το Σχήμα 24 δείχνει τις κυματομορφές ομιλίας και τα αντίστοιχα φασματογράμματα που προέρχονται από τον μετασχηματισμό Fourier βραχείας διάρκειας (Short-Time Fourier Transform - STFT) για τέσσερις διαφορετικές εγγραφές αναγνωσμένης ομιλίας. Το περιεχόμενο του κειμένου είναι το ίδιο και για τις τέσσερις ηχογραφήσεις: "allow each child to have an ice pop". Η πρώτη εικόνα είναι για κανονική εγγραφή χωρίς μάσκα, ενώ οι άλλες τρεις είναι για τον ίδιο ομιλητή που φοράει χειρουργική μάσκα, λεπτή ή ελαφριά υφασμάτινη μάσκα και μάσκα από πυκνό ύφασμα. Να σημειωθεί ότι η λέξη pop που προφέρεται στο τέλος της πρότασης γίνεται όλο και λιγότερο αισθητή με την ύπαρξη όλο και πιο βαριών μασκών. Ένα άλλο αξιοσημείωτο αποτέλεσμα αφορά την εξασθένηση των υψηλών συχνοτήτων για βαρύτερες μάσκες, η οποία επηρεάζει όχι μόνο την απόδοση αναγνώρισης αλλά και την ευκρίνεια της ομιλίας.



Σχήμα 24: Παραδείγματα τεσσάρων φασματογραμμάτων για το κείμενο: "allow each child to have an ice pop", που προφέρεται από τον ίδιο ομιλητή φορώντας διαφορετικούς τύπους μάσκας: (a) χωρίς μάσκα, (b) χειρουργική, (c) υφασμάτινη και (d) μάσκα από πυκνό πανί.

Προκειμένου να αντιμετωπιστούν τα τρέχοντα ζητήματα στην κοινότητα βιομετρίας φωνής, τα ευρήματα του 2020 της 12ης Computational Paralinguistics Challenge (COMPARE) εξέτασαν την περίπτωση ανίχνευσης μάσκας. Τα αποτελέσματα της δημιουργίας συστήματος δείχνουν ότι οι στόχοι απέχουν πολύ από το να επιτευχθούν. Τα σήματα ομιλίας, σε αυτό το πλαίσιο, δεν σχετίζονται μόνο με τα βιομετρικά στοιχεία της φωνής, αλλά μπορούν να χρησιμοποιηθούν για την ανίχνευση παραμορφώσεων σήματος.

Η υπάρχουσα εργασία δείχνει ότι οι μάσκες προσώπου επηρεάζουν όντως τις τεχνολογίες που βασίζονται στη φωνή και ότι υπάρχει δυνατότητα αντιστάθμισης αυτών των επιπτώσεων. Έτσι, η συνάφεια της αναγνώρισης ομιλητών αυξάνεται σε αυτό το χρονικό διάστημα, καθώς είναι απρόσβλητη και ανέγγιχτη, δηλαδή μπορεί να γίνει από απόσταση, χωρίς καμία φυσική αλληλεπίδραση (από το τηλέφωνο), [10].

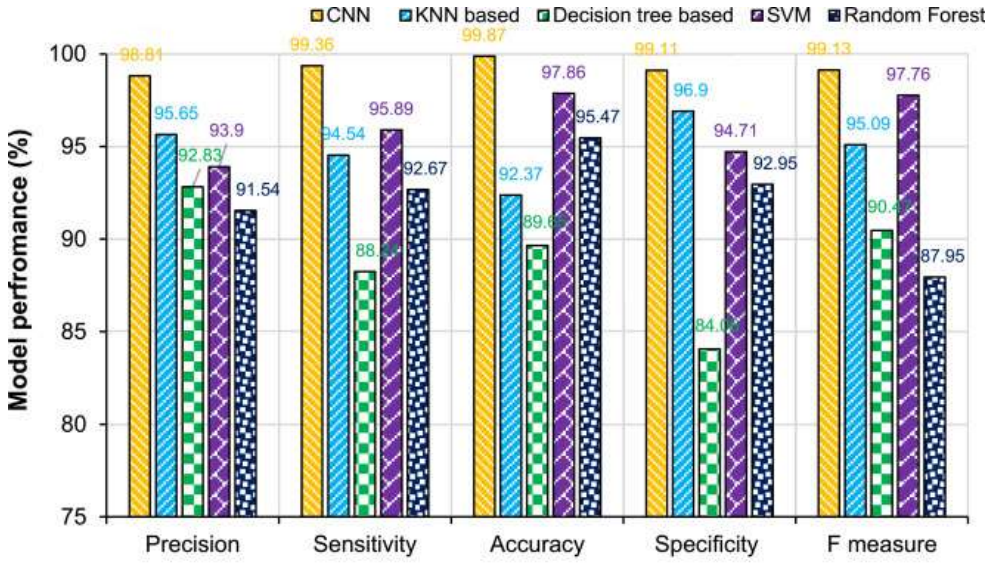
5.3 ΑΝΑΓΝΩΡΙΣΗ ΔΑΚΤΥΛΙΚΟΥ ΑΠΟΤΥΠΩΜΑΤΟΣ

Όπως αναφέρθηκε, οι περισσότερες βιομετρικές λύσεις δακτυλικών αποτυπωμάτων αναζητούν συγκεκριμένα χαρακτηριστικά ενός δακτυλικού αποτυπώματος, όπως τα μοτίβα των γραμμών κορυφογραμμών στο δάχτυλο, τις κοιλάδες μεταξύ των κορυφογραμμών κ.λπ., κοινώς τα γνωστά

ως μικροσκοπικά στοιχεία, τα οποία στη συνέχεια μετατρέπονται σε αποθηκευμένα ψηφιακά δεδομένα. Προκειμένου να ληφθεί μια αντιστοίχιση δακτυλικών αποτυπωμάτων για επαλήθευση ή πιστοποίηση, τα βιομετρικά συστήματα πρέπει να βρουν επαρκή αριθμό μοτίβων μικροσκοπικών στοιχείων. Αυτός ο αριθμός ποικίλλει ανάλογα με τα συστήματα.

Σύμφωνα με τον Alam [51], για την αξιολόγηση της απόδοσης, δοκιμάστηκαν πολλές άλλες τεχνικές ταξινόμησης δακτυλικών αποτυπωμάτων όπως οι k-Nearest Neighbor (KNN), Decision Tree (DT), Support Vector Machine (SVM) και Random Forest (RF). Ο KNN είναι μια προσέγγιση από πάνω προς τα κάτω όπου η ταξινόμηση πραγματοποιήθηκε με τη δημιουργία ενός δέντρου αποφάσεων από το σύνολο εκπαίδευσης. Χρησιμοποιήθηκε η μέθοδος της μέγιστης διαφοράς στην εντροπία για τους κόμβους για τον διαχωρισμό των δεδομένων. Στην προσέγγιση KNN, η ταξινόμηση προσδιορίστηκε από τη μετρική της απόστασης και την τιμή του k και ο αλγόριθμος KNN υπολογίστηκε στο σύνολο δοκιμών για τις πιο συχνές κλάσεις.

Οι μετρικές αξιολόγησης, συμπεριλαμβανομένης της ακρίβειας (precision), της ευαισθησίας (sensitivity), της εξειδίκευσης (specifity), της ακρίβειας (accuracy) και της F μετρικής φαίνονται στην για διαφορετικά συστήματα ταξινόμησης προκειμένου να συγκριθεί η απόδοση μεταξύ τους. Από τη σύγκριση των αποτελεσμάτων ήταν προφανές ότι η μέθοδος CNN ξεπέρασε τις άλλες τεχνικές ταξινόμησης για όλες τις μετρήσεις. Πιο συγκεκριμένα, η ακρίβεια (accuracy) που υπολογίστηκε με το CNN βελτιώθηκε κατά 2,05%, 4,61%, 8,12% και 11,40% σε σύγκριση με τα SVM, RF, KNN και DT αντίστοιχα. Όσον αφορά την ευαισθησία, την ακρίβεια (accuracy) και τη μετρική F, η μέθοδος SVM φάνηκε να είναι η δεύτερη καλύτερη σε σύγκριση με τις άλλες τεχνικές. Ωστόσο, όσον αφορά την ακρίβεια (precision) και την εξειδίκευση, η μέθοδος KNN παρήγαγε τα δεύτερα καλύτερα αποτελέσματα. Το DT παρήγαγε τα χειρότερα αποτελέσματα εκτός από την ακρίβεια (precision), όπου το DT παρήγαγε καλύτερα αποτελέσματα από το RF.



Σχήμα 25: Μετρικές αξιολόγησης για σύγκριση διαφορετικών συστημάτων ταξινόμησης (δακτυλικών αποτυπωμάτων), [51].

Το δακτυλικό αποτύπωμα μικρής περιοχής που περιέχει λιγότερες λεπτομέρειες αποτελεί πρόκληση σε σύγκριση με την παραδοσιακή αναγνώριση δακτυλικών αποτυπωμάτων μεγάλης περιοχής που βασίζεται στην αντιστοίχιση των μικροσκοπικών στοιχείων. Πρόσφατα, χρησιμοποιήθηκε το φίλτρο Gabor για την εξαγωγή του χάρτη χαρακτηριστικών δακτυλικών αποτυπωμάτων ως πολυδιάστατη επέκταση χαρακτηριστικών με το όνομα ROIFE_CNN, η οποία χρησιμοποιήθηκε ως εικόνα εκπαίδευσης. Ο αλγόριθμος ROIFE_CNN χρησιμοποιήθηκε για την ταξινόμηση και την αναγνώριση της εικόνας θεωρώντας το κεντρικό μπλοκ του δακτυλικού αποτυπώματος ως την περιοχή ενδιαφέροντος. Σύμφωνα με τον Alam [51], η εξαγωγή χαρακτηριστικών από το φίλτρο Gabor και η ταξινόμηση CNN θα μπορούσε να βελτιώσει την ακρίβεια της ταξινόμησης των δακτυλικών αποτυπωμάτων.

5.4 ΣΥΜΠΕΡΙΦΟΡΙΚΑ ΒΙΟΜΕΤΡΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Όπως αναφέρθηκε, τα συμπεριφορικά βιομετρικά χαρακτηριστικά προσδιορίζουν και μετρούν τις ανθρώπινες δραστηριότητες, όπως δυναμική πληκτρολόγησης, φωνητικό αποτύπωμα, χρήση συσκευής, ανάλυση υπογραφής, μοτίβα σφαλμάτων (τυχαίο χτύπημα "l" αντί για "K" δύο φορές σε κάθε πέμπτο πάτημα πλήκτρου) κ.λπ. Τέτοια συμπεριφορικά βιομετρικά χαρακτηριστικά χρησιμοποιούνται συνήθως ως πρόσθετο επίπεδο ασφάλειας, μαζί με άλλα διαπιστευτήρια ή βιομετρικές πληροφορίες.

Τα περισσότερα συστήματα φυσικών βιομετρικών λύσεων ελέγχουν την ταυτότητα του χρήστη μόνο μία φορά και συνήθως στην αρχή μιας ενέργειας, όπως η σύνδεση σε μια συσκευή ή στο άνοιγμα μιας πόρτας. Η τεχνολογία συμπεριφορικής βιομετρίας επιχειρεί να καλύψει το κενό του ελέγχου ταυτότητας σε ένα σενάριο κατά τη διάρκεια μιας ενέργειας.

Για παράδειγμα, ο αρχικός χρήστης μπορεί να παράσχει τα διαπιστευτήριά του/της σε άλλο άτομο μετά τον επιτυχή έλεγχο ταυτότητας του χρήστη (παρόμοια με το tailgating). Προκειμένου να ελαχιστοποιηθούν τέτοιες πιθανότητες σε αυτήν την περίπτωση, οι λύσεις συμπεριφορικής βιομετρίας αναλύουν τις αλληλεπιδράσεις των χρηστών με τις συσκευές τους, καταγράφοντας δραστηριότητες που διαφέρουν από τα συνήθη πρότυπα χρήσης.

Ο Piugie [52], μελέτησε μια βασική προσέγγιση για την αναγνώριση των χρηστών που βασίζεται σε διαφορετικά συμπεριφορικά βιομετρικά στοιχεία χρησιμοποιώντας τη μηχανική μάθηση (κλασική και βαθιά μάθηση). Μελετήθηκαν δύο συμπεριφορικά βιομετρικά χαρακτηριστικά: οι ανθρώπινες δραστηριότητες που καταγράφονται από ένα smartphone και η δυναμική πληκτρολόγησης σε ένα φορητό υπολογιστή. Προτάθηκε ένα σύνολο γενικευμένων μεθόδων για την κλασική προσέγγιση (μηχανική μάθηση) χρησιμοποιώντας το λογισμικό εξόρυξης δεδομένων Orange. Χρησιμοποιήθηκαν οι πιο πρόσφατες επιτυχημένες προσεγγίσεις βαθιάς μάθησης για την ταξινόμηση χρονοσειρών, καθώς η αναγνώριση είναι το αποτέλεσμα ενός προβλήματος ταξινόμησης.

Στην κλασική προσέγγιση, οι χρήστες ταξινομούνται χρησιμοποιώντας οκτώ διαφορετικές μεθόδους μηχανικής μάθησης, συγκεκριμένα: μηχανές διανυσμάτων υποστήριξης (SVM), νευρωνικά δίκτυα (NN), τυχαίο δάσος (RF), AdaBoost, λογιστική παλινδρόμηση (LR), naive Bayes, k-πλησιέστερο γείτονα (k-NN) και stacking πάνω στο λογισμικό εξόρυξης δεδομένων Orange. Με την προσέγγιση της βαθιάς μάθησης, συγκρίθηκαν τα αποτελέσματα από την ταξινόμηση των χρονοσειρών συγκρίνοντας τα μοντέλα: πλήρως συνελικτικά νευρωνικά δίκτυα (Full Convolutional Networks - FCN) και Residual Network (ResNet) χρησιμοποιώντας το TensorFlow 2.2.0 - G.P.U. σε Python 3.8.2. Τα πειραματικά αποτελέσματα έδειξαν ότι η βαθιά μάθηση από άκρο σε άκρο μπορεί να επιτύχει τη βέλτιστη απόδοση για την ταξινόμηση χρονοσειρών με αρχιτεκτονικές όπως το FCN και το deep ResNet στην αναγνώριση συμπεριφορικών βιομετρικών χαρακτηριστικών.

5.5 ΟΡΓΑΝΙΣΜΟΙ – ΠΛΑΤΦΟΡΜΕΣ ΠΟΥ ΠΑΡΕΧΟΥΝ ΒΙΟΜΕΤΡΙΚΕΣ ΛΥΣΕΙΣ

Στην παρούσα ενότητα θα παρουσιαστούν οργανισμοί και πλατφόρμες που παρέχουν βιομετρικές λύσεις.

5.5.1 Βιομετρική πιστοποίηση: Crossmatch

Η Crossmatch (πλέον αποτελεί μέλος του ομίλου HID) είναι μια εταιρεία "σύνθετου ελέγχου ταυτότητας και διαχείρισης βιομετρικής ταυτότητας βάσει κινδύνου". Το 2014, συγχωνεύτηκε με την Digital Persona, μια άλλη εταιρεία βιομετρικής τεχνολογίας, για να λανσάρει τη βασική πλατφόρμα βιομετρικών λύσεων για επιχειρήσεις που ονομάζεται DigitalPersona Composite Authentication.

Η πλατφόρμα προσφέρει το "ευρύτερο σύνολο μεθόδων ελέγχου ταυτότητας", συμπεριλαμβανομένης της σάρωσης δακτυλικών αποτυπωμάτων, της αναγνώρισης προσώπου και φωνής και συμπεριφορικών βιομετρικών χαρακτηριστικών, όπως η πληκτρολόγηση, η μετακίνηση και παρακολούθηση ενεργειών του ποντικιού. Τον Νοέμβριο του 2017, η Crossmatch ανακοίνωσε τη συνεργασία της με τη BehavioSec , μια εταιρεία τεχνολογίας βιομετρικής συμπεριφοράς με έδρα τη Σουηδία, η οποία ενισχύει τις λειτουργίες συμπεριφορικών βιομετρικών αναλύσεων της DigitalPersona.

Τον Σεπτέμβριο του 2017, η Crossmatch συνεργάστηκε με το Oxford Computer Group, έναν Golden Partner της Microsoft που προσφέρει λύσεις πιστοποίησης ταυτότητας και ασφάλειας.

Εκτός από την επιχειρηματική πλατφόρμα, η εταιρεία επίσης προσφέρει ένα ευρύ φάσμα βιομετρικών λύσεων, κυρίως, λύσεις σάρωσης και ανίχνευσης δακτυλικών αποτυπωμάτων σε διάφορους επιχειρηματικούς τομείς, συμπεριλαμβανομένων των οικονομικών, της κυβέρνησης, της επιβολής του νόμου, του λιανικού εμπορίου κ.λπ.

Σύμφωνα με τους συγγραφείς [6], [53], αναφορικά με την αναγνώριση προσώπου, αυτά που την καθιστούν ξεχωριστή από την HID είναι τα εξής:

- Ανίχνευση επίθεσης μη ταιριαστής παρουσίασης (Presentation Attack Detection - PAD): Συνδυάζοντας την κατοχυρωμένη τεχνολογία πολυφασματικής απεικόνισης (MultiSpectral Imaging - MSI) με τον αλγόριθμο PAD που πληροί το πρότυπο ISO30107-1, παρέχεται η ισχυρότερη live ανίχνευση ενάντια σε επιθέσεις πλαστογραφίας.

- Συνδυασμός τεχνητής νοημοσύνης και μηχανικής μάθησης: Βασισμένη σε κορυφαίους στον κλάδο αλγόριθμους τεχνητής νοημοσύνης και μηχανικής μάθησης, η τεχνολογία αναγνώρισης προσώπου προσφέρει απαράμιλλη ακρίβεια και ταχύτητα ταιριάσματος. Οι αλγόριθμοι που χρησιμοποιούνται εξασφαλίζουν επαρκή ποικιλομορφία δεδομένων στην αναγνώριση προσώπου.
- Υψηλή απόδοση σε φωτισμό που αποτελεί πρόκληση: Τα προηγμένα συστήματα καμερών που παρέχονται λειτουργούν καλά σε όλα τα είδη περιβαλλόντων και συνθηκών φωτισμού, αντιμετωπίζοντας τις προκλήσεις των καμερών που λειτουργούν σε περιπτώσεις απόλυτου σκοταδιού και έντονου φωτός.
- Κορυφαία κατάταξη NIST: Ο αλγόριθμός για την αναγνώριση προσώπου κατατάσσεται στην πρώτη πεντάδα παγκοσμίως στο Face Recognition Vendor Test (FRVT) του NIST.
- Ανίχνευση μάσκας: Με προηγμένους αλγόριθμους αντιστοίχισης προσώπου, η τεχνολογία αναγνώρισης προσώπου μπορεί να ανιχνεύσει πρόσωπα με μάσκες, κάτι που είναι ένα κρίσιμο χαρακτηριστικό κατά τη διάρκεια μιας πανδημίας.
- Χρήση στο κινητό: Το λογισμικό που παρέχεται υποστηρίζει έλεγχο ταυτότητας προσώπου και εγγράφων σε κινητά, παρέχοντας το υψηλότερο επίπεδο ασφάλειας και άνεσης χρήστη.

5.5.2 Tygart: Αναγνώριση προσώπου

Η Tygart Technology παρέχει ανάλυση βίντεο και φωτογραφιών, καθώς και συστήματα βιομετρικής αναγνώρισης για πελάτες της πολιτείας και της ομοσπονδιακής κυβέρνησης στις Ηνωμένες Πολιτείες. Το βασικό προϊόν της είναι το MXSERVER, ένα "σύστημα εγκληματολογικής ανάλυσης βίντεο και φωτογραφιών" που βασίζεται σε ένα διακομιστή (server). Το σύστημα επεξεργάζεται συλλογές βίντεο και φωτογραφιών που έχουν προέλθει από κατασχεμένους υπολογιστές, κινητά τηλέφωνα, κάρτες SIM και συστήματα παρακολούθησης βίντεο μετατρέποντάς τα σε εργαλεία αναζήτησης. Μέσω του σχεδιασμού του που βασίζεται σε web διεπαφή, το MXSERVER καθιστά δυνατή την ασφαλή ανταλλαγή πληροφοριών δημιουργώντας ένα περιβάλλον στο οποίο οργανισμοί και αναλυτές μπορούν να συνεργάζονται και να μοιράζονται τη συλλογική τους γνώση σε πραγματικό χρόνο, από οπουδήποτε στον κόσμο.

Τα βίντεο και οι φωτογραφίες που έχουν αποθηκευτεί σε διαφορετικά και αποσυνδεδεμένα συστήματα μπορούν πλέον να αναζητηθούν μέσω του διαδικτύου χρησιμοποιώντας την αναγνώριση προσώπου. Η εταιρεία εξυπηρετεί το FBI παρέχοντας υπηρεσίες λειτουργίας και συντήρησης για το αυτοματοποιημένο, εθνικό σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων, [6], [54].

5.5.3 Facewatch: Αναγνώριση προσώπου

Το MXSERVER "θα βοηθήσει στην αποφυγή εγκληματικών και τρομοκρατικών επιθέσεων". Η Facewatch είναι μια εταιρεία με έδρα το Λονδίνο που χρησιμοποιεί την πλατφόρμα αναγνώρισης προσώπου MXSERVER για να βοηθήσει τις επιχειρήσεις και την αστυνομία "να αντιμετωπίσουν το έγκλημα σε χαμηλό επίπεδο". Το σύστημα ειδοποιεί τις επιχειρήσεις όταν εγγεγραμμένοι εγκληματίες εισέρχονται στις εγκαταστάσεις τους. Αυτό το κάνει αντιστοιχίζοντας τις βιομετρικές πληροφορίες προσώπου που είναι αποθηκευμένες σε μια κεντρική λίστα παρακολούθησης. Πρόσφατα, το Facewatch ανακοίνωσε ότι το σύστημα αναγνώρισης προσώπου του που είναι εγκατεστημένο στα BRMalls στη Βραζιλία βοήθησε "να συλλάβουν πέντε σοβαρούς εγκληματίες τους πρώτους δύο μήνες χρήσης". Αυτή η ιστορία – και μια σειρά από άλλες μαρτυρίες από την Facewatch – καλύφθηκαν σε βάθος από το American Security Today τον Οκτώβριο του 2017. Το Facewatch χρησιμοποιεί αυτήν τη στιγμή το MXSERVER ως μηχανή αναγνώρισης προσώπου, αν και μπορεί να λειτουργήσει με οποιοδήποτε σύστημα, [6].

5.5.4 Onfido: Βιομετρικά χαρακτηριστικά προσώπου

Το Onfido με έδρα το Λονδίνο είναι μια διαδικτυακή πλατφόρμα ψηφιακής επαλήθευσης ταυτότητας για επιχειρήσεις. Μεταξύ άλλων κανόνων και τρόπων αυθεντικοποίησης, η Onfido χρησιμοποιεί επίσης βιομετρικά στοιχεία προσώπου, ως πρόσθετο επίπεδο ασφάλειας, για την επαλήθευση μεμονωμένων προσώπων. Η εταιρεία χρησιμοποιεί τεχνολογία μηχανικής μάθησης για να επικυρώσει την ταυτότητα ενός χρήστη και να τη διασταυρώσει με διεθνείς βάσεις δεδομένων και λιστών παρακολούθησης. Η διαδικασία πιστοποίησης με χρήση βιομετρικών στοιχείων προσώπου στον ιστότοπο Onfido για κινητά, είναι ενσωματωμένη σε πολλές εφαρμογές, όπως π.χ. σε μια τραπεζική πλατφόρμα. Για παράδειγμα σε μια τραπεζική πλατφόρμα τα βήματα που πρέπει να ακολουθηθούν είναι τα εξής: Αρχικά, οι φωτογραφίες της άδειας οδήγησης σαρώνονται στο διαδίκτυο. Στη συνέχεια, ο χρήστης ενημερώνεται ότι πρέπει να

πιστοποιηθεί μέσω ενός βίντεο "selfie". Αυτό, εξηγεί η εφαρμογή, γίνεται για να βεβαιωθεί ότι δεν πλαστοπροσωπείται. Στο βίντεο "selfie", δίνεται η οδηγία να εκτελέσει δύο απλά βήματα, όπως να γυρίσει το πρόσωπό αριστερά/δεξιά και να πει δυνατά τους αριθμούς που υποδεικνύονται.

Η εταιρεία έχει συγκεντρώσει περισσότερα από 60 εκατομμύρια δολάρια από μεγάλες εταιρείες όπως τη Microsoft Ventures, τη Salesforce Ventures και τη Crunchfund. Πιο πρόσφατα, η Crane Venture Partners επένδυσε 30 εκατομμύρια δολάρια για να χρηματοδοτήσει το τμήμα έρευνας και ανάπτυξης της εταιρείας στην τεχνολογία μηχανικής μάθησης. Πελάτες της εταιρείας αποτελούν οι ZipCar, Couchsurfing, Revolut και Square. Πρόσφατα, κυκλοφόρησε την πλατφόρμα ενσωμάτωσης στο Salesforce AppExchange, [6].

5.5.5 EyeLock: Αναγνώριση ίριδας

Η EyeLock προσφέρει "προηγμένο έλεγχο ταυτότητας ίριδας για το Διαδίκτυο των πραγμάτων". Το χαρακτηριστικό προϊόν της, Nano NXT, είναι ένα υλικό βιομετρικής αναγνώρισης ίριδας. Το Nano NXT έχει ποσοστό ψευδούς αποδοχής (η πιθανότητα το βιομετρικό σύστημα ασφαλείας να δέχεται μη εξουσιοδοτημένο χρήστη) 1 στα 1,5 μέτρα σε ένα μόνο μάτι.

Σχήμα 26: Η συσκευή Nano NXT, [55].

Παραδείγματα εφαρμογής του Nano NXT αποτελούν το ATM και τα κιόσκια. Αυτό το "ATM του Μέλλοντος" φαίνεται να μην απαιτεί αριθμό κάρτας ή PIN. Το ATM είναι ενσωματωμένο με τη βιομετρική τεχνολογία ίριδας EyeLock, η οποία σε συνδυασμό με την τηλεφωνική εφαρμογή της τράπεζας, αναγνωρίζει το χρήστη και του δίνει πρόσβαση για ανάληψη μετρητών.

Το πιο πρόσφατο καινοτόμο προϊόν της EyeLock είναι το Nano IXT, το οποίο είναι ένας αναγνώστης ελέγχου ταυτότητας ίριδας (τελευταίας τεχνολογίας) εσωτερικού χώρου που σχεδιάστηκε για τον έλεγχο πρόσβασης. Το Nano IXT έχει μεγάλη οθόνη αφής LCD, διπλές κάμερες αυτόματης κλίσης για το πρόσωπο και την ίριδα, ενσωματωμένη συσκευή ανάγνωσης καρτών, λεκτική και οπτική καθοδήγηση χρήστη και υποστήριξη πολλών γλωσσών. Όπως όλα τα προϊόντα της EyeLock, παρέχεται μαζί με την αντίστοιχη εφαρμογή για πελάτες που θέλουν να προσαρμόσουν τις λύσεις ασφαλείας τους για να ενσωματώσουν το Nano IXT με τις δικές τους υπάρχουσες εφαρμογές. Το Nano IXT επαληθεύει την ταυτότητα έως και 30 ατόμων ανά λεπτό με απαράμιλλη ακρίβεια. Επιπλέον, η EyeLock κυκλοφόρησε πρόσφατα την πρόσθετη μονάδα ελέγχου θερμοκρασίας iTemp για το σύστημα ίριδας nano iXT. Το iTemp είναι ένας υπέρυθρος θερμικός αισθητήρας που διαβάζει τη θερμοκρασία του υπό εξέταση αντικειμένου την ίδια στιγμή που οι ίριδές του ελέγχονται. Με το iTemp, δεν χρειάζεται η μετατόπιση του χρήστη σε ξεχωριστή συσκευή για έλεγχο θερμοκρασίας. Το iTemp παρέχει στις επιχειρήσεις ένα πολύ προσιτό και εύκολα αναπτυσσόμενο εργαλείο, για να τις βοηθήσει να αυξήσουν την ασφάλεια του χώρου εργασίας τους παρέχοντας παράλληλα την υψηλότερη ακρίβεια βιομετρικής ταυτότητας για έλεγχο πρόσβασης. Η ρύθμιση του ορίου θερμοκρασίας, η εμφάνιση προσαρμοσμένων μηνυμάτων κατά τη χρήση και η άρνηση πρόσβασης του χρήστη εάν η θερμοκρασία του υπερβαίνει το όριο, είναι από τις πιο σημαντικές δυνατότητες, που μεγιστοποιείται η σημασία τους εν μέσω πανδημίας.

Σχήμα 27: Nano IXT με τον προαιρετικό iTemp θερμικό αισθητήρα, [55].

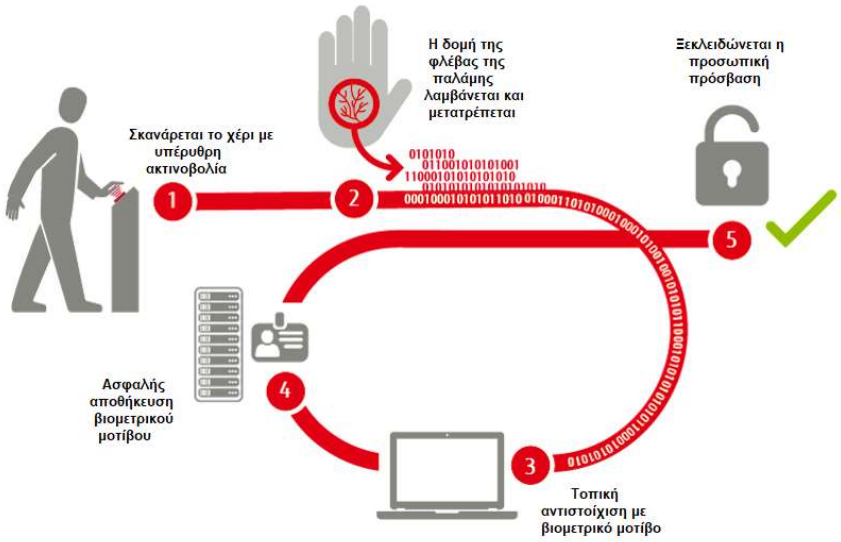
Η εταιρεία κατέχει περισσότερες από 75 πατέντες για την αποκλειστική βιομετρική τεχνολογία της. Αναφέρει επίσης διάφορους συνεργάτες που χρησιμοποιούν και μεταπωλούν τις βιομετρικές λύσεις της, όπως οι STANLEY Security Solutions, ViaTouch Media και Central Security Distribution, [6].

5.5.6 Fujitsu Frontech: αναγνώριση φλέβας

Η βιομετρική λύση με υπογραφή από τη Fujitsu Frontech, με έδρα την Ιαπωνία, είναι ο αισθητήρας PalmSecure, μια συσκευή ελέγχου ταυτότητας που σαρώνει τις φλέβες στην παλάμη χωρίς να χρειάζεται ο χρήστης να έρθει σε επαφή με τη συσκευή. Τον Μάιο του 2017, η εταιρεία ανακοίνωσε ότι η Fujitsu Korea και η Fujitsu Frontech συνεργάστηκαν για την παροχή της τεχνολογίας αναγνώρισης φλεβών στην κορεατική εταιρεία Lotte Card Co Ltd για την υποστήριξη ενός συστήματος πληρωμών χωρίς κάρτα και χωρίς μετρητά.

Σχήμα 28: Αισθητήρας PalmSecure, [56].

"Το PalmSecure δεν αποθηκεύει πληροφορίες για τη φλέβα της παλάμης σε σχήμα εικόνας, αλλά μετατρέπει τις πληροφορίες του μοτίβου της φλέβας σε δεδομένα που δεν μπορούν να αποκρυπτογραφηθούν, τα αντιστοιχεί με ένα βιομετρικό μοτίβο, και στη συνέχεια το κρυπτογραφεί, το αποθηκεύει και επιτρέπει την πρόσβαση", δήλωσε η εταιρεία. Η διαδικασία αυτή φαίνεται και στο Σχήμα 29.



Σχήμα 29: Τεχνολογία ελέγχου ταυτότητας φλέβας παλάμης με τη συσκευή Fujitsu PalmSecure, [56].

Η μειωμένη αιμοσφαιρίνη μέσα στη φλέβα απορροφά τις υπέρυθρες ακτίνες που καθιστούν δυνατή τη "διάκριση των μοτίβων των φλεβών που διαφέρουν από άτομο σε άτομο", πρόσθεσε η εταιρεία. Επίσης, δεδομένου ότι τα μοτίβα των φλεβών δεν αλλάζουν, όπως και άλλοι βιομετρικοί παράγοντες, αυτή η διαδικασία περιλαμβάνει μόνο μια φορά μόνο εγγραφή. Από τις 31 Μαρτίου 2017, περίπου 770.000 συσκευές PalmSecure έχουν αποσταλεί σε 60 χώρες και

περισσότεροι από 70 εκατομμύρια άνθρωποι κάνουν χρήση αυτής της βιομετρικής συσκευής, ισχυρίζεται η Fujitsu, [6].

5.5.7 BehavioSec: συμπεριφορικά βιομετρικά χαρακτηριστικά

Η BehavioSec με έδρα τη Σουηδία δήλωσε ότι χρησιμοποιεί συνεχή μηχανική μάθηση για τον έλεγχο ταυτότητας των χρηστών με βάση τα μοτίβα συμπεριφοράς τους, όπως την πίεση, το γυροσκόπιο, τη ζώνη χτυπήματος κουμπιού, την κίνηση, την επιτάχυνση, τις ενέργειες του ποντικιού κ.λπ.

Δεδομένου ότι το ατομικό μοτίβο συμπεριφοράς κάθε ατόμου δεν διαμορφώνεται μόνο από βιομετρικά χαρακτηριστικά, όπως ο τρόπος με τον οποίο κινεί το χέρι του, αλλά επηρεάζεται επίσης από περισσότερους κοινωνικούς και ψυχολογικούς παράγοντες, όπως αν είναι η μητρική γλώσσα αυτή που γράφει, είναι σχεδόν αδύνατο να αντιγραφεί ή μιμηθεί το βιομετρικό προφίλ συμπεριφοράς κάποιου άλλου. Το πρώτο βήμα ξεκινά όταν ένας χρήστης αρχίζει να συνδέεται και να αλληλεπιδρά με την εφαρμογή ή τον ιστότοπο, όπως κάνει πάντα. Το BehavioSec είναι απολύτως διαφανές για τον τελικό χρήστη, καθώς έχει εξαλείψει εντελώς την ανάγκη για εκπαίδευση του χρήστη, καθώς η εμπειρία χρήσης είναι απολύτως κατανοητή. Καθώς ο χρήστης αλληλεπιδρά, η πλατφόρμα BehavioSec συλλέγει συνεχώς και αθόρυβα σήματα συμπεριφοράς για ανάλυση από τη μηχανή μηχανικής μάθησης. Αυτό σημαίνει ότι τα δεδομένα συλλέγονται όχι μόνο μία φορά κατά τη σύνδεση του χρήστη, αλλά καθ' όλη τη διάρκεια της διαδραστικής συνεδρίας για τη συνεχή επαλήθευση ότι το συγκεκριμένο άτομο παραμένει νόμιμο από την είσοδο του στο σύστημα έως την έξοδο από αυτό. Τέλος, παρέχεται ένας δείκτης γνησιότητας σε πραγματικό χρόνο, επιτρέποντας στους νόμιμους χρήστες να αλληλεπιδρούν χωρίς πρόσθετους ελέγχους, παράλληλα με την αποφυγή επιθέσεων κακόβουλων χρηστών στον υπάρχοντα οργανισμό. Τα βήματα φαίνονται στο Σχήμα 30.

Σχήμα 30: Βήματα BehavioSec πλατφόρμας στο υπό εξέταση (ως προς την ασφάλεια) σύστημα.

Το 2012, η Αμερικανική Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων Άμυνας επένδυσε στην τεχνολογία της, ανέφερε η εταιρεία. Ωστόσο, δεν αναφέρει για πόσο καιρό βρισκόταν σε εξέλιξη η χρηματοδότηση ή πόσα χρήματα ήταν η επένδυση. Η BehavioSec ανέφερε επίσης ότι εξασφαλίζει περισσότερες από 5 δισεκατομμύρια συναλλαγές ετησίως, αν και δεν παρείχε πληροφορίες για τους τύπους συναλλαγών. Πρόσφατα, η τεχνολογία BehavioSec ενσωματώθηκε στην πλατφόρμα DigitalPersona της Crossmatch, [6].

5.6 ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΒΛΕΨΕΙΣ ΣΤΗ ΒΙΟΜΕΤΡΙΚΗ ΤΕΧΝΟΛΟΓΙΑ

Σύμφωνα με μια έκθεση Tractica του 2017, τα έσοδα από τεχνολογίες βιομετρικού υλικού και λογισμικού θα αυξηθούν σε 15,1 δισεκατομμύρια δολάρια παγκοσμίως έως το 2025, με λόγο σύνθετο ρυθμό ετήσιας ανάπτυξης (Compound Annual Growth Rate - CAGR) 22,9%. Η έκθεση προβλέπει επίσης ότι τα συνολικά έσοδα από βιομετρικές τεχνολογίες από το 2016 έως το 2025 θα ανέλθουν σε 69,8 δισεκατομμύρια δολάρια. Η έκθεση αναλύει 142 περιπτώσεις χρήσης και συμπεραίνει ότι το μεγαλύτερο κομμάτι εσόδων από τη βιομετρική τεχνολογία θα προέρχεται από την αναγνώριση δακτυλικών αποτυπωμάτων, την αναγνώριση φωνής, την αναγνώριση ίριδας και την αναγνώριση προσώπου. Οι μεγαλύτερες αγορές εφαρμογών για τις βιομετρικές τεχνολογίες, σύμφωνα με την έκθεση, θα είναι η ασφάλεια των καταναλωτών, των οικονομικών, της υγειονομικής περίθαλψης, της φυσικής ασφάλειας και της ασφάλειας πληροφορικής σε επίπεδο κυβέρνησης και επιχειρήσεων. Η αγορά αναγνώρισης ίριδας θα αυξηθεί από 676,6 εκατομμύρια δολάρια το 2016 σε 4,1 δισεκατομμύρια δολάρια μέχρι το 2025, σύμφωνα με την έκθεση. Κατά τη διάρκεια αυτής της 10ετούς περιόδου, οι παγκόσμιες αποστολές συσκευών αναγνώρισης ίριδας θα αυξηθούν από 10,7 εκατομμύρια μονάδες σε 61,6 εκατομμύρια μονάδες ετησίως, με 277,4 εκατομμύρια συνολικές αποστολές. Τα παγκόσμια έσοδα των βιομετρικών επιχειρήσεων θα φτάσουν τα 1,7 δισεκατομμύρια δολάρια έως το 2024, με συνολικά έσοδα 7,9 δισεκατομμύρια δολάρια την περίοδο 2015-2024, με 28% CAGR, σύμφωνα με έκθεση της Tractica του 2016. Οι κλάδοι της υγειονομικής περίθαλψης και των χρηματοοικονομικών παρουσιάζουν τις περισσότερες δυνατότητες για αύξηση εσόδων εντός της 10ετίας 2015-2024, [6].

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η τεχνολογία εξελίσσεται γρήγορα, δημιουργώντας περισσότερους υποψήφιους φορείς επίθεσης και αυξάνοντας τα τρωτά σημεία για επίθεση. Κάθε μήνα φαίνεται να υπάρχουν περισσότερες ειδήσεις για παραβιάσεις δεδομένων, τόσο μεγάλες όσο και μικρές. Καθώς αυτά τα συμβάντα συνεχίζουν να αυξάνονται, οι οργανισμοί μαθαίνουν ότι πρέπει να αναλάβουν δράση, και γρήγορα, με νέα μέτρα ασφαλείας. Οι εταιρείες στρέφουν τώρα την προσοχή τους από τις πολιτικές κωδικών πρόσβασης στις λύσεις βιομετρικής επαλήθευσης ταυτότητας, χωρίς να λαμβάνουν υπόψη όλες τις συνέπειες.

6.1 ΣΗΜΑΣΙΑ ΒΙΟΜΕΤΡΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

Η βιομετρική βιομηχανία επεκτείνεται γρήγορα, καθώς τα εργαλεία και η τεχνολογία ενσωματώνονται στην καθημερινή ζωή. Υποτίθεται ότι ο κλάδος θα μπορούσε να αξίζει έως και 68,6 δισεκατομμύρια δολάρια σε μόλις πέντε χρόνια. Υπάρχει η σκέψη ότι οι κωδικοί πρόσβασης είναι υπεύθυνοι για τα περισσότερα ζητήματα ασφάλειας ευρείας κλίμακας. Κατά μία έννοια, αυτό είναι το ήμισυ της αλήθειας, αλλά δεν είναι οι κωδικοί πρόσβασης που αποτυγχάνουν – είναι το γεγονός ότι τα άτομα επαναχρησιμοποιούν τους κωδικούς πρόσβασης συνεχώς. Η επαναχρησιμοποίηση κωδικού πρόσβασης σημαίνει ότι μόλις κλαπούν τα διαπιστευτήρια ενός χρήστη από έναν λογαριασμό ή έναν ιστότοπο που έχει παραβιαστεί, οι χάκερ μπορούν να έχουν πρόσβαση σε πολλούς άλλους, σημαντικούς λογαριασμούς και να αποκτήσουν πρόσβαση στο δίκτυο.

Φαίνεται λογικό για τους οργανισμούς να αναζητούν άλλες λύσεις, και υπάρχουν ακόμη και η επιθυμία για συστήματα ασφαλείας χωρίς κωδικούς πρόσβασης. Η πιο αξιόλογη μέθοδος επαλήθευσης ταυτότητας έχει αποδειχθεί ότι είναι η βιομετρική, ένα πεδίο που έχει επεκταθεί δραματικά την τελευταία δεκαετία. Ενώ η βιομετρική τεχνολογία είναι χρήσιμη για πολλές καταστάσεις, παρουσιάζει το δικό της σύνολο προκλήσεων και ελαττωμάτων, όπως ακριβώς κάνουν οι κωδικοί πρόσβασης.

6.2 GDPR ΚΑΙ ΒΙΟΜΕΤΡΙΑ

Η ασφάλεια με χρήση βιομετρικής τεχνολογίας έχει θεωρηθεί από πολλούς ως το "μέλλον της ασφάλειας". Η ικανότητα αναγνώρισης ενός ατόμου με βάση τα μοναδικά φυσικά και συμπεριφορικά χαρακτηριστικά του, όπως αναφέρθηκε, είναι ένα πιθανό όφελος για πολλές

εταιρείες, συμβάλλοντας στη βελτίωση της ασφάλειας, στην παρακολούθηση και διαχείριση της παρουσίας των εργαζομένων. Ομοίως, με τους κωδικούς πρόσβασης που φέρεται να αντιπροσωπεύουν περισσότερο από το 80% των παραβιάσεων της ασφάλειας στο χώρο εργασίας. Η ασφάλεια με χρήση βιομετρικής τεχνολογίας και ο έλεγχος ταυτότητας είναι σημαντικά πιο αποτελεσματικοί για την καταπολέμηση της απάτης και της ανάρμοστης συμπεριφοράς.

Ωστόσο, η εισαγωγή του Γενικού Κανονισμού Προστασίας Δεδομένων (General Data Protection Regulation – GDPR) και οι ανησυχίες σχετικά με τα ευαίσθητα δεδομένα έχουν αυξήσει την ανάγκη για αποσαφήνιση της διαδικασίας χρήσης βιομετρικών δεδομένων σε επιχειρήσεις. Το πιο συνηθισμένο ζήτημα σχετίζεται με ανησυχίες των εργαζομένων σχετικά με την αποθήκευση και τη χρήση των προσωπικών τους δεδομένων. Ως εκ τούτου, επισημαίνονται ορισμένες από τις κοινές παρανοήσεις σχετικά με τα βιομετρικά στοιχεία και τη συμμόρφωσή τους με το GDPR εξηγώντας πώς τα συστήματα αναγνώρισης ταυτότητας με χρήση βιομετρικής τεχνολογίας μπορούν να βοηθήσουν στην άμβλυνση αυτών των φόβων, [22].

Το σύνολο των κανόνων του GDPR ορίζει την ασφάλεια με χρήση βιομετρικής τεχνολογίας ως "προσωπικά δεδομένα που προκύπτουν από ειδική τεχνική επεξεργασία που σχετίζονται με τα φυσικά, φυσιολογικά ή συμπεριφορικά χαρακτηριστικά ενός φυσικού προσώπου, τα οποία επιτρέπουν ή επιβεβαιώνουν τη μοναδική ταυτοποίηση αυτού του φυσικού προσώπου". Καθώς τα βιομετρικά δεδομένα ταξινομούνται ως "ειδική κατηγορία" προσωπικών δεδομένων, οι διαχειριστές των δεδομένων αυτών πρέπει να πληρούν μία από τις παρακάτω προϋποθέσεις κατά την κυκλοφορία της τεχνολογίας, [58]:

- Το υποκείμενο των δεδομένων να έχουν δώσει ρητή συγκατάθεση για τη χρήση βιομετρικού ελέγχου ταυτότητας.
- Η ασφάλεια με χρήση βιομετρικής τεχνολογίας είναι απαραίτητη για τους σκοπούς της εκπλήρωσης των υποχρεώσεων και της άσκησης των ειδικών δικαιωμάτων του υπευθύνου επεξεργασίας δεδομένων ή του υποκειμένου των δεδομένων στους τομείς της απασχόλησης, της κοινωνικής ασφάλισης και του δικαίου της κοινωνικής προστασίας.
- Η επεξεργασία των βιομετρικών στοιχείων είναι κρίσιμη για την προστασία των ζωτικών συμφερόντων των δεδομένων του υποκειμένου.
- Η επεξεργασία είναι απαραίτητη για τον χώρο εργασίας και την άσκηση υπεράσπισης νομικών αξιώσεων.

- Τα βιομετρικά στοιχεία είναι απαραίτητα για λόγους δημοσίου συμφέροντος.

Ενώ η νομοθεσία απαγορεύει την επεξεργασία ευαίσθητων προσωπικών δεδομένων, αναγνωρίζει τις εξελίξεις στον βιομετρικό έλεγχο ταυτότητας. Ομοίως, υπάρχουν ορισμένες βάσεις που δικαιολογούν την επεξεργασία του, συμπεριλαμβανομένης της ρητής συναίνεσης των υποκείμενων των τα δεδομένα υπόκεινται σε επεξεργασία, της εκτέλεσης συγκεκριμένων συμβάσεων ή για συγκεκριμένους σκοπούς, αναφερόμενοι στον επαγγελματικό τομέα, π.χ. στα πλαίσια μιας εταιρείας.

Στην εποχή του GDPR, είναι εύκολο να κατανοήσουμε τις πολλές παρανοήσεις που μπορεί να έχουν ορισμένοι με τις βιομετρικές πληροφορίες. Κοιτάζοντας πίσω αρκετά χρόνια πριν, η απόκριση στα βιομετρικά δεδομένα και στον έλεγχο ταυτότητας ήταν σε μεγάλο βαθμό "αρνητική". Ωστόσο, πολλές βιομηχανίες πλέον υιοθετούν την τεχνολογία λόγω της ευκολίας επεξεργασίας, των δυνατοτήτων απομακρυσμένης διαχείρισης και, φυσικά, της αυξημένης ασφάλειας. Ένα άλλο σημαντικό πλεονέκτημα της βιομετρίας στην εποχή του GDPR είναι η αξιοπιστία και η ευκολία, ειδικά καθώς προσφέρουν ταυτόχρονη εγγραφή δακτυλικών αποτυπωμάτων σε πολλές τοποθεσίες.

Ωστόσο, η βιομετρική επαλήθευση θα πρέπει να συνοδεύεται από διαφάνεια με τους εμπλεκομένους. Οι προσωπικές πληροφορίες και οι εικόνες δακτυλικών αποτυπωμάτων δε θα πρέπει να αποθηκεύονται και η υιοθέτηση της τεχνολογίας θα χρησιμεύσει μόνο στη διευκόλυνση και την ασφάλεια της επαγγελματικής ζωής. Ένας αναγνώστης βιομετρικών χαρακτηριστικών, μπορεί να χρησιμοποιεί μόνο μια σαρωμένη εικόνα ενός δακτυλικού αποτυπώματος για διασταύρωση με αποθηκευμένα πρότυπα σε έναν ξεχωριστό πίνακα ελέγχου (εγκατεστημένο σε ασφαλές σημείο) για τον έλεγχο ταυτότητας του χρήστη.

Οι νέοι αμυντικοί μηχανισμοί συνοδεύονται από βελτιώσεις και ασφάλεια για τις νέες απειλές. Ωστόσο, οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται τις πιο πρόσφατες τεχνολογίες χρησιμοποιώντας πιο εξελιγμένες τεχνικές όπως η βαθιά μάθηση π.χ. για να μιμηθούν τη φωνή και να ξεπεράσουν προσεγγίσεις όπως η αναγνώριση φωνής. Η βιομετρική τεχνολογία από μόνη της δεν μπορεί να χρησιμοποιηθεί ως αυτόνομος μηχανισμός για την προστασία των συσκευών του κυβερνοχώρου, επειδή ένας χάκερ θα εξακολουθεί να βρει εισόδους επίθεσης στο σύστημα. Αντίθετα, θα πρέπει να χρησιμοποιείται προσεκτικά και έξυπνα, σε συνδυασμό με άλλες μεθόδους ελέγχου ταυτότητας, όπως κωδικούς πρόσβασης και pin, διασφαλίζοντας παράλληλα το

GDPR των χρηστών. Η υιοθέτηση μιας πολυεπίπεδης προσέγγισης είναι ο ευκολότερος τρόπος για να διασφαλιστεί η ασφάλεια του οργανισμού. Η λογική είναι παρόμοια με τη χρήση μεθόδων ελέγχου ταυτότητας σε ζεύγη που αλληλοσυμπληρώνονται, [1], [2].

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Ochieng J., Biometrics and Cybersecurity, (2021, November 10), retrieved from https://cyberexperts.com/biometrics-and-cybersecurity/
2. Enzoic, How Biometrics Measure Up and Why They Aren't the Cure-All for Cybersecurity, (2021, November 15), retrieved from https://securityboulevard.com/2020/11/how-biometrics-measure-up-and-why-they-arent-the-cure-all-for-cybersecurity/
3. Agrawal R., All you need to know about biometrics and cyber security, (2021, November 16), retrieved from https://blog.ipleaders.in/need-know-biometrics-cyber-security/#Biometric_Data
4. Belhadj F., Biometric system for identification and authentication, (2017), Computer Vision and Pattern Recognition, Ecole nationale Supérieure en Informatique Alger.
5. Olorunsola O. S., Assessment of privacy and security perception of biometric technology case study of Kaduna state tertiary academic institutions, (2021, November 16) retrieved from https://onlinelibrary.wiley.com/doi/full/10.1002/spy2.124
6. Madhavan R., AI in Biometrics and Security – Current Business Applications, (2021, November 17), retrieved from https://emerj.com/ai-sector-overviews/ai-in-biometrics-current-business-applications/
7. Sennaar K., Facial Recognition Applications – Security, Retail, and Beyond, (2021, November 17), retrieved from https://emerj.com/ai-sector-overviews/facial-recognition-applications/
8. Naveen J., Biometrics is smart, but AI is smarter. Here's why, (2021, November 17), retrieved from https://www.allerin.com/blog/biometrics-is-smart-but-ai-is-smarter-heres-why
9. Li J.h., (2018), Cyber security meets artificial intelligence: a survey, Springerlink.
10. Gomez M., Drozdowski P., Rathgebb C., Patinoc J., Todiscoc M., Nautschc A., Damerd N., Priesnitzb J., Evansc N., Buschb C., (2021), Biometrics in the Era of COVID-19: Challenges and Opportunities.
11. Obaidat M. S., Traore I., Woungang I., (2019), Biometric Based Physical and Cybersecurity Systems, Springer.
12. Benarous L., Kadri B., and Bouridane A., (2017), A Survey on Cyber Security Evolution and Threats: Biometric Authentication Solutions, Springer.

13. Kour J., Hanmandlu M., Ansari A.Q., (2016), Biometrics in Cyber Security, DESIDOC.
14. Mogos G., (2020), Biometrics in cyber defense, MATEC Web of Conferences 309, 02003.
15. Dsouza J., Elezabeth L., Mishra V. P., Jain R., (2019), Security in Cyber-Physical Systems, IEEE.
16. Geers K., (2011), Strategic Cyber Security, Tallinn.
17. Wikipedia, Computer Security, (2021, November 17), retrieved from https://en.wikipedia.org/wiki/Computer_security
18. Pfleeger C.P., Pfleeger S.L., Margulies J., (2015), Security in Computing, 5th edn., Prentice Hall, Upper Saddle River, NJ.
19. Gu Q., Liu P., (2007), Denial of Service Attacks, Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, 3, 454–468.
20. Sen S., Clark J.A., Tapiador J.E., (2011), Security threats in mobile ad hoc networks, in Security of Self- Organizing Networks: MANET, WSN, WMN, VANET, Auerbach Publications.
21. Martin S., Tokutomi M., (2012), Password Cracking, researchers report, Arizona University, USA.
22. Dentons, GDPR Update - Biometric Data, (2021, November 18), retrieved from https://www.dentons.com/en/insights/alerts/2020/december/22/gdpr-update-biometric-data
23. Stolfo S.J., Bellovin S.M., Hershkop S., Keromytis A.D., (2008), Insider Attack and Cyber Security Beyond the Hacker, Springer.
24. Abomhara M., Koien G.M., (2014), Security and privacy in the internet of things: current status and open issues, Privacy and Security in Mobile Systems (PRISMS), International Conference on IEEE.
25. Benarous L., Djoudi M., Bouridane A., (2015), Etudes Comparatives d' outils de stéganographie et d'outils de stéganalyse: Application aux images et aux vidéos, Amar Telidji University, Laghouat, Algeria.
26. Pavlyushchik M.A., (2010), Method and system for antimalware scanning with variable scan settings, Patent U.S. 7725941 B1.

27. Scarfone K., Mell P., (2007), Guide to Intrusion Detection and Prevention Systems (IDPS), NIST special publication, 800, 94.
28. Martin C., (2008), Intrusion detection and prevention systems in the industrial automation and control systems environment, Process Control Systems Industry Conference, Industrial Defender Inc.
29. Stone M., Firewalls explained: the different firewall types and technologies, (2021, November 20), retrieved from https://cybersecurity.att.com/blogs/security-essentials/what-is-a-firewall-types-technologies-explained
30. Meah J., 10 Ways Virtualization Can Improve Security, (2021, November 20), retrieved from https://www.techopedia.com/2/31007/trends/virtualization/10-ways-virtualization-can-improve-security
31. Traore I., Alshahrani M., Obaidat MS., (2018), State of the art and perspectives on traditional and emerging biometrics: A survey. Security and Privacy, 1: e44.
32. Diaz V., (2015), Legal challenges of biometric immigration control systems, Mexican Law Rev. 7(1), 1–28.
33. Abaza A., Ross A., Hebert C., Harrison M.A.F., Nixon M.S., (2013), A survey on ear biometrics, ACM Comput. Surv. 45(2), 35.
34. Rawlson K., Explainer: Facial Thermography, (2021, November 20), retrieved from https://www.biometricupdate.com/201308/explainer-facial-thermography
35. Biometric Solutions, Fingerprint Recognition, (2021, November 21), retrieved from https://www.biometric-solutions.com/fingerprint-recognition.html
36. Barbosa I.B., Theoharis T., Abdallah A.E., (2016), On the use of fingernail images as transient biometric identifiers Biometric recognition using fingernail images, Mach. Vis. Appl. 27(1), 65–76.
37. Schneegass S., Oualil Y., Bulling A., (2016), SkullConduct: biometric user identification on eyewear computers using bone conduction through the skull, Proceedings of the 34th ACM SIGCHI Conference on Human Factors in Computing Systems.
38. Çelik O., (2018), A Research on Machine Learning Methods and Its Applications, Journal of Educational Technology and Online Learning.

39. Wei J., (2020), Research on Machine Learning and Its Algorithms and Development, J. Phys.: Conf. Ser. 1544 012003.
40. Ren SQ., He KM., Girshick R., et al., (2017), Faster R-CNN: towards real-time object detection with region proposal networks, IEEE Trans Patt Anal Mach Intell, 39(6): 1137-1149.
41. Korczak J., Hernes M., (2017), Deep learning for financial time series forecasting in a-trader system, Proc Federated Conf. on Computer Science and Information Systems, p.905- 912.
42. Syarif AR., Gata W., (2017), Intrusion detection system using hybrid binary PSO and K-nearest neighborhood algorithm, 11th Int Conf on Information & Communication Technology and System, p.181-186.
43. Dada EG., (2017), A hybridized SVM-kNN-pdAPSO approach to intrusion detection system, Faculty Seminar Series, p. 1-8.
44. Meng DY., Chen H., (2017), MagNet: a two-pronged defense against adversarial examples, Proc ACM Conf on Computer and Communications Security, p.135-147.
45. Olalere M., Abdullah MT., Mahmod R., et al., (2016), Identification and evaluation of discriminative lexical features of malware URL for real-time classification, Int Conf on Computer and Communication Engineering, p.90-95.
46. Kokila RT., Selvi ST., Govindarajan K., (2014), DDoS detection and analysis in SDN-based environment using support vector machine classifier, Proc 6th Int Conf on Advanced Computing, p.205-210.
47. Shahid N., Aleem SA., Naqvi IH., et al., (2012), Support vector machine-based fault detection & classification in smart grids, IEEE Globecom Workshops, p.1526-1531.
48. Vuong T.P., Loukas G., Gan D., et al., (2015), Decision tree-based detection of denial of service and command injection attacks on robotic vehicles, IEEE Int Workshop on Information Forensics and Security, p.1-6.
49. Moon D., Im H., Kim I., et al., (2017), DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks, J Supercomput, 73(7):2881-2895.
50. MasterCard, Mastercard Identity Check Mobile, (2021, November 25), retrieved from https://developer.mastercard.com/product/identity-check-mobile/

51. Alam N. A., Ahsan M., Based M.A., Haider J., Kowalski M., (2021), An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning, Computers & Electrical Engineering, Volume 95, 107387, ISSN 0045-7906.
52. Piugie Y. B. W., Manno J. D., Rosenberger C., Charrier C., (2021), How Artificial Intelligence can be used for Behavioral Identification?, 2021 International Conference on Cyberworlds (CW), Caen, France.
53. HID, Powering Trusted Identities, (2021, November 25), retrieved from https://www.hidglobal.com/
54. Product Information: MXSERVER™ Video & Photo Forensic Analysis System, (2021, November 25), retrieved from http://www.tygart.com/wp-content/uploads/2009/08/MXSERVER_2014.pdf
55. EyeLock, Nano NXT, (2021, November 25), retrieved from https://www.eyelock.com/products/
56. Fujitsu.com, PalmSecure, (2021, November 25), retrieved from https://www.fujitsu.com/jp/group/frontech/en/solutions/business-technology/security/palmsecure/
57. Κουκουφιλίππου Ε., Η εισαγωγή της βιομετρικής τεχνολογίας στην Ε.Ε., (2021, December 15), retrieved from https://www.offlinepost.gr/2021/03/17/h-eisagwgh-ths-biometrikhs-texnologias-sthn-ee/
58. General News, Biometrics and the GDPR: Why you should adopt the technology, (2022, March 22), retrieved from https://ievoreader.com/biometrics-and-the-gdpr-why-you-should-adopt-the-technology/

ΠΑΡΑΡΤΗΜΑ Α

Η εισαγωγή της βιομετρικής τεχνολογίας στην Ε.Ε.

Ήδη από τις απαρχές του 21ου αιώνα, η τεχνολογία έχει γνωρίσει ραγδαία κι αλματώδη ανάπτυξη, αν συγκριθεί με τα επιτεύγματα των δεκαετιών του προηγούμενου ακριβώς αιώνα. Είναι πραγματικά αξιοθαύμαστο το γεγονός ότι μόλις μέσα σε δύο δεκαετίες καταφέραμε να κρατήσουμε κινητό με πλήκτρα -το οποίο ήδη τότε φάνταζε αντικείμενο που ξεπήδησε από ταινία επιστημονικής φαντασίας- και λίγο αργότερα κινητά υψηλής τεχνολογίας, τα οποία λειτουργούν με την αφή, αναγνωρίζουν το δακτυλικό αποτύπωμα, τα χαρακτηριστικά του προσώπου και πραγματοποιούν φωνητικές εντολές. Τα τελευταία που αναφέρθηκαν ονομάζονται βιομετρικά χαρακτηριστικά κι ολοένα κερδίζουν έδαφος στην αγορά τεχνολογικών προϊόντων, ενσαρκώνοντας το μέλλον της τεχνολογικής εξέλιξης.

Η Ευρωπαϊκή Ένωση, με σκοπό να προάγει την έρευνα και την καινοτομία στους χώρους της επιστήμης και της τεχνολογίας, δημιούργησε ένα πρόγραμμα, το Horizon 2020 το οποίο χρηματοδοτείται με έναν γενναιόδωρο προϋπολογισμό, ύψους 80 δις ευρώ. Εκ των 80 δις, περίπου 1,7 δις διοχετεύονται σε ένα υπο-πρόγραμμα του Horizon 2020, το οποίο προωθεί την ανάπτυξη προϊόντων ασφαλείας για αστυνομικές δυνάμεις και ομάδες συνοριακού ελέγχου που ανήκουν τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Ειδικότερα, συμπεριλαμβάνονται τεχνολογίες που βασίζονται στην Τεχνητή Νοημοσύνη (AI), μη επανδρωμένα drones, λογισμικό επαυξημένης πραγματικότητας (Augmented Reality=AR), σε εφαρμογές αναγνώρισης προσώπου, ίριδας, φωνής και φλεβών (βιομετρικά χαρακτηριστικά) και ό,τι άλλο είναι χρήσιμο για να επιτυγχάνεται η απαιτούμενη εποπτεία.

Και μόνο η ιδέα εφαρμογής αυτών των προϊόντων στη μελλοντική καθημερινή μας ζωή φαντάζει δυστοπική-οργουελική σκηνή. Στην πραγματικότητα, όμως, όλα αυτά εκ χρονικής απόψεως δεν είναι παρά μία ανάσα μακριά. Μερικά από τα βιομετρικά χαρακτηριστικά είναι ήδη ενσωματωμένα στα smartphones, με την δική μας συναίνεση, τα drones αποτελούν πλέον ένα σημαντικό κομμάτι του στρατιωτικού τομέα ενώ η Τεχνητή Νοημοσύνη εξελίσσεται γοργά. Βέβαια, σε καμία περίπτωση δεν είναι αποδεκτή η δαιμονοποίηση των νέων τεχνολογιών και η έμμονη προσκόλληση σε παλαιολιθικές κι απαρχαιωμένες τεχνολογικές επιτυχίες. Κρούεται,

εντούτοις, ο κώδων του κινδύνου για τις εκφάνσεις των νέων τεχνολογιών που καταστρατηγούν θεμελιώδη ανθρώπινα δικαιώματα και ξεπερνούν τα λεπτά και δυσδιάκριτα όρια της βιοηθικής.

Μέχρι στιγμής, το πρώτο προϊόν που αφορά τον έλεγχο εισόδου δια των ευρωπαϊκών συνόρων με την επωνυμία iBorderCtrl, είναι γεγονός. Πρόκειται για έναν ανιχνευτή ψεύδους Τεχνητής Νοημοσύνης (AI lie detector) ο οποίος είναι ικανός, όπως ισχυρίζονται οι δημιουργοί του, να αναγνωρίζει μικρο-εκφράσεις του προσώπου -μορφασμούς- οι οποίοι δύνανται να "προδώσουν" τους ψευδείς ισχυρισμούς του ατόμου που ομιλεί ενώ απαντά σε ερωτήσεις που του τίθενται. Η ανάπτυξη της εφαρμογής απορρόφησε 45 εκατ. ευρώ από το πρόγραμμα Horizon, λειτούργησε πιλοτικά στα χερσαία σύνορα της Λιθουανίας, της Ουγγαρίας και της Ελλάδας, ωστόσο συνάντησε σκόπελο στην προσπάθεια πλήρους εφαρμογής σε όλα τα μέλη της Ε.Ε. Ο "σκόπελος" αυτός φέρει όνομα και είναι ο Γερμανός ευρωβουλευτής Patrick Breyer από τον μικρό κομματικό σχηματισμό των Πειρατών. Ο Γερμανός ευρωβουλευτής ζήτησε πρόσβαση στα έγγραφα που εγκρίνουν το iBorderCtrl βασιζόμενος στους ευρωπαϊκούς νόμους και στα δικαιώματα περί διαφάνειας. Η Ε.Ε. αρνήθηκε την πρόσβαση στα έγγραφα, ισχυριζόμενη την προστασία εμπορικών δικαιωμάτων που αφορούν την εφαρμογή iBorderCtrl. Ο Patrick Breyer προχώρησε σε αγωγή κατά της Ε.Ε., ζητώντας άρση του αδικαιολόγητου απορρήτου επί των εγγράφων και η υπόθεση παραπέμφθηκε προς εκδίκαση στο Ευρωπαϊκό Δικαστήριο (ECJ). Επιπροσθέτως, η εφαρμογή σε πείραμα που διενεργήθηκε απέτυχε, κρίνοντας λανθασμένα πως το άτομο ψευδόταν ενώ στην πραγματικότητα έλεγε την αλήθεια.

Η Ε.Ε. προσπαθεί εντατικά να ανταγωνιστεί την τεχνολογία και τις πρακτικές ασφαλείας που ισχύουν στις Ηνωμένες Πολιτείες της Αμερικής, στην Κίνα και στη Ρωσία. Η Ένωση, όμως, δεν εμφανίζει χαρακτηριστικά των πολιτικών συστημάτων αυτών των χωρών. Αποτελεί ένα κράμα εθνικοτήτων, ιδεολογιών και οικονομικών συμφερόντων. Κατά συνέπεια, συνιστά δικαίωμα όλων των ευρωπαίων πολιτών, σύμφωνα με την αρχή της διαφάνειας που διέπει το ευρωπαϊκό κράτος δικαίου, η πρόσβαση σε πρωτοβουλίες της Ένωσης μέσω εγγράφων, έτσι ώστε να γνωρίζουν με σαφήνεια οι πολίτες σε ποιες ενέργειες διοχετεύονται τα χρήματα που καταβάλουν δια της φορολογίας που τους επιβάλλεται. Προσχήματα περί προστασίας «εμπορικών συμφερόντων», δημιουργούν μονάχα δεύτερες σκέψεις και κινούν υποψίες που οδεύουν σε υποθέσεις για παράνομα κονδύλια, διαφθορά κι «ανήθικους» σκοπούς. Η Ε.Ε. φαίνεται να τρέμει στην ιδέα άσκησης κριτικής στις συγκεκριμένες τεχνολογικές πρωτοβουλίες, εφόσον κάτι τέτοιο

θα έβλαπτε την πώληση των επερχόμενων προϊόντων ασφαλείας τα οποία είναι περιζήτητα σε άλλες αγορές.

Αξιοσημείωτο είναι το γεγονός πως από το κονδύλι για έρευνα ενδυνάμωσης της κρατικής ασφάλειας, έχει επωφεληθεί σε μεγάλο βαθμό ο ιδιωτικός τομέας, απορροφώντας περίπου το 42% και συμμετέχοντας ως κύριος εταίρος σε projects, ενώ ο δημόσιος τομέας και τα ινστιτούτα ερευνών λαμβάνουν πολύ μικρότερο κομμάτι της πίτας. Για την χορήγηση της χρηματοδότησης σε τέτοιου είδους προγράμματα υπάρχει το συμβουλευτικό σώμα PASAG (Protection and Security Advisory Group), το οποίο επίσης αποτελείται στην πλειοψηφία του από παράγοντες του ιδιωτικού τομέα που επωφελούνται ανάλογα με το που προσπαθούν να διοχετεύσουν τους πόρους. Τις τελικές αποφάσεις πράγματι τις παίρνει το Ευρωκοινοβούλιο, αλλά είναι ευρέως γνωστό το μέγεθος της πίεσης που ασκείται από τον ιδιωτικό τομέα με το lobbying. Πλέον, η προστασία των ατομικών δικαιωμάτων και ελευθεριών δεν απειλείται μόνο από το κράτος, αλλά και από τους ισχυρούς ιδιωτικούς οργανισμούς.

Σε αυτό το σημείο βρισκόμαστε λοιπόν μπροστά σε μία διάσταση απόψεων. Από τη μία κρατεί η άποψη ότι δεν πρέπει να σταματάμε την εξέλιξη της τεχνολογίας, κι από την άλλη δυναμώνει η άποψη πως οι δημόσιες αρχές δεν πρέπει να αποκρύπτουν πληροφορίες για θέματα μαζικής εποπτείας των πολιτών, οπτική που αντικειμενικά ανακόπτει την πορεία της τεχνολογικής εξέλιξης. Τον γόρδιο δεσμό καλείται να λύσει η επιστήμη της βιοηθικής η οποία προς το παρόν είναι έρμαιο οικονομικών συμφερόντων στις ευρωπαϊκές διαδικασίες για δημιουργία προϊόντων ασφαλείας με βιομετρικά στοιχεία. Οι επιτροπές κωλύονται να λειτουργήσουν απρόσκοπτα και ορθολογικά λόγω των μεγάλων πιέσεων που δέχονται από τα lobbies, ενδεχομένως κι από λειτουργούς του δημόσιου τομέα, για να εγκρίνουν projects, τα οποία όπως δηλώνουν είναι εξ' αρχής -γεγενημένης της ιδέας- «ανήθικα». Η βιομετρική τεχνολογία θέτει σε κίνδυνο τα κεκτημένα πολυετών αγώνων για την όσο το δυνατόν μεγαλύτερη εξάλειψη των διακρίσεων, απειλεί στοιχειώδη ανθρώπινα δικαιώματα που αφορούν τα προσωπικά δεδομένα και την προσωπικότητα και εγείρει σημαντικά ερωτήματα σχετικά με την αποθήκευση, την επεξεργασία και το διαμοιρασμό των βιομετρικών χαρακτηριστικών που θα συλλέγονται για εμπορικούς φυσικά σκοπούς.

Οι τρομοκρατικές ενέργειες, ιδιαίτερα αυτές στην αρχή του αιώνα, οι συνεχείς μεταναστευτικές και προσφυγικές ροές, είναι γεγονότα που επικαλείται η Ε.Ε. για να προωθήσει

την ανάπτυξη, τη χρήση προϊόντων εποπτείας και την εισαγωγή αυτής της τεχνολογίας. Η βιομετρική τεχνολογία, στο στάδιο που βρίσκεται, είναι εξαιρετικά αμφισβητήσιμη κι αμφιλεγόμενη. Από τη στιγμή που δε συμβαδίζει με τις ευρωπαϊκές αρχές και τα δικαιώματα των ευρωπαίων πολιτών, αλλά και δεν ελέγχεται κατάλληλα από τις αρμόδιες επιτροπές, είναι αθέμιτη η έγκρισή της και η πώλησή της στην αστυνομική και στρατιωτική αγορά. Ελάχιστες ελευθερίες μας έχουν απομείνει που δεν έχει αποκόψει η υπέρμετρη ασκούμενη εποπτεία από τα μέσα κοινωνικής δικτύωσης, το διαδίκτυο και από τις εφαρμογές γεωεντοπισμού ή καταγραφής ήχου, κι αυτό πάλι, μάλλον, αμφισβητείται, [57].