ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Αξιολόγηση και Προστασία της Ιδιωτικότητας σε Ενδυτά Συστήματα: Ανάλυση Απειλών και Προτεινόμενα Μέτρα Αντιμετώπισης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Θεοφανούδη Κατερίνας

Επιβλέπουσα: Βασιλική Διαμαντοπούλου

Μέλη εξεταστικής επιτροπής: Γιώργος Σπαθούλας, Μαρία Καρύδα

Σάμος, Οκτώβριος 2026

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο των σπουδών μου στο Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων της Πολυτεχνικής Σχολής του Πανεπιστημίου Αιγαίου.

Θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσά μου, κ. Βασιλική Διαμαντοπούλου, για την εμπιστοσύνη, την καθοδήγηση και τις εύστοχες παρατηρήσεις της καθ' όλη τη διάρκεια εκπόνησης της εργασίας. Ευχαριστώ, επίσης, τα μέλη της εξεταστικής επιτροπής για τον χρόνο που διέθεσαν για την αξιολόγησή της.

Τέλος, οφείλω ένα μεγάλο ευχαριστώ στην οικογένεια και στους φίλους μου για τη στήριξη και την ενθάρρυνσή τους σε όλη τη διάρκεια των σπουδών μου.

© 2026

της

Θεοφανούδη Κατερίνας

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1 Εισαγωγή **1**
1.1 Τα Ενδυτά Συστήματα και το Ζήτημα της Ιδιωτικότητας 1
1.2 Αντικείμενο διπλωματικής 2
1.2.1 Σκοπός της εργασίας *2*
1.2.2 Ερευνητικά Ερωτήματα *2*
1.3 Δομή της διπλωματικής 3
2 Ενδυτά Συστήματα (Wearable Systems) **4**
2.1 Ορισμός και Κατηγορίες Ενδυτών Συστημάτων 4
2.2 Τεχνολογίες και Λειτουργίες 5
2.3 Εφαρμογές και Προκλήσεις 5
3 Κίνδυνοι και Απειλές Ιδιωτικότητας σε Ενδυτά Συστήματα **8**
3.1 Ταξινόμηση και Ανάλυση Απειλών Ιδιωτικότητας 8
3.1.1 Συλλογή και Υπερσυλλογή Δεδομένων *8*
3.1.2 Παρακολούθηση και Καταγραφή Συμπεριφοράς *9*
3.1.3 Διαρροές και Μη Εξουσιοδοτημένη Πρόσβαση *9*
3.1.4 Επαναναγνώριση και Συναγωγή Πληροφοριών *10*
3.1.5 Έλλειψη Διαφάνειας και Ελέγχου *10*
3.1.6 Συμπεράσματα *11*
4 Τεχνολογίες Ενίσχυσης Ιδιωτικότητας για Ενδυτά Συστήματα **12**
4.1 Εισαγωγή 12
4.2 Ανωνυμοποίηση και Ψευδωνυμοποίηση Δεδομένων 13
4.2.1 Ορισμοί και Βασικές Αρχές *13*
4.2.2 Τεχνικές Ψευδωνυμοποίησης *13*
4.2.3 Προκλήσεις και Περιορισμοί *14*
4.3 Ομομορφική Κρυπτογράφηση 14
4.3.1 Ορισμός και Βασικές Αρχές *14*
4.3.2 Εφαρμογή σε Ενδυτά και Πλεονεκτήματα *15*
4.3.3 Περιορισμοί *15*
4.4 Ασφαλής Πολυμερής Υπολογιστική 16
4.4.1 Ορισμός και Εφαρμογή σε Ενδυτά *16*
4.4.2 Τεχνικές SMC *16*
4.4.3 Πλεονεκτήματα SMC *16*
4.4.4 Περιορισμοί *16*
4.5 Διαφορική Ιδιωτικότητα 17
4.5.1 Ορισμός *17*
4.5.2 Εφαρμογή σε Ενδυτά Συστήματα και Πλεονεκτήματα *17*
4.5.3 Περιορισμοί *18*
4.6 Αποδεικτικά Μηδενικής Γνώσης 18
4.6.1 Ορισμός και Εφαρμογή σε Ενδυτά *18*
4.6.2 Τύποι ZKP *19*
4.6.3 Πλεονεκτήματα *19*
4.6.4 Περιορισμοί *19*

4.7 Ομοσπονδιακή Μάθηση 20
4.7.1 Ορισμός 20
4.7.2 Εφαρμογή σε Ενδυτά Συστήματα 20
4.7.3 Προκλήσεις και Περιορισμοί 21
4.8 Κατανεμημένη Αναλυτική 21
4.8.1 Ορισμός 21
4.9 Συμπεράσματα και Συνδυαστικές Προσεγγίσεις 22
5 Νομικό και Κανονιστικό Πλαίσιο 25
5.1 Εισαγωγή 25
5.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων και οι Επιπτώσεις του στα Ενδυτά Συστήματα 26
5.2.1 Το Πεδίο Εφαρμογής του GDPR στα Ενδυτά Συστήματα 26
5.2.2 Οι Βασικές Αρχές 27
5.2.3 Προστασία Δεδομένων από τον Σχεδιασμό και εξ Ορισμού 29
5.2.4 Δικαιώματα των Υποκειμένων των Δεδομένων 30
5.2.5 Προκλήσεις Συμμόρφωσης των Ενδυτών Συστημάτων 30
5.3 Ο Ρόλος των Τεχνολογιών Ενίσχυσης Ιδιωτικότητας (PETs) στη Συμμόρφωση με τον GDPR 32
5.3.1 Η σχέση PETs και GDPR 32
5.3.2 Αντιστοίχιση PETs με Απαιτήσεις του GDPR 33
5.3.3 Η Ανάλυση Αντικτύπου για την Ιδιωτικότητα (PIA) ως Εργαλείο Συμμόρφωσης 34
5.4 Συμπεράσματα 35
6 Μελέτη Περίπτωσης: Έξυπνο Δαχτυλίδι – Ανάλυση και Προτάσεις 36
6.1 Εισαγωγή 36
6.2 Περιγραφή του Έξυπνου Δαχτυλιδιού 36
6.3 Ανάλυση Απειλών με τη Μεθοδολογία LINDDUN 39
6.3.1 Η Μεθοδολογία LINDDUN 39
6.3.2 Τα Βήματα της Μεθοδολογίας 40
6.3.3 Εφαρμογή της Μεθοδολογιας LINDDUN στο έξυπνο δαχτυλίδι 41
6.3.4 Ιεράρχηση Απειλών 43
6.4 Προτάσεις Τεχνολογιών και Μέτρων Προστασίας Ιδιωτικότητας 45
6.4.1 PETs για Αποκάλυψη Πληροφοριών (Disclosure) και Αναγνωρισιμότητα (Identifiability) 45
6.4.2 PETs για Συνδεσιμότητα (Linkability) και Ανιχνευσιμότητα (Detectability) 45
6.4.3 PETs για Έλλειψη Ενημέρωσης (Unawareness) και Μη-Συμμόρφωση (Non-compliance) 46
6.5 Νομική και Κανονιστική Συμμόρφωση των Προτεινόμενων Μέτρων 46
6.6 Συζήτηση Αποτελεσμάτων 49
7 Συμπεράσματα και Μελλοντική Έρευνα 51
7.1 Σύνοψη της Εργασίας 51
7.2 Κύρια Ευρήματα 52
7.3 Συμβολή της Εργασίας 53
7.4 Περιορισμοί και Μελλοντική Έρευνα 53
7.5 Επίλογος 53
Βιβλιογραφία 54

Λίστα Σχημάτων

Σχήμα 1: Διάγραμμα Ροής Δεδομένων (DFD) Επιπέδου 1 για το σύστημα του έξυπνου δαχτυλιδιού 47

Λίστα Πινάκων

Πίνακας 1: Νομικές βάσεις επεξεργασίας σύμφωνα με το Άρθρο 6 του GDPR 33

Πίνακας 2: Σύγκριση των δημοφιλέστερων μοντέλων έξυπνων δαχτυλιδιών 45

Πίνακας 3: Πίνακας αξιολόγησης κινδύνου (Risk Assessment Matrix) για τις απειλές LINDDUN του έξυπνου δαχτυλιδιού 50

Πίνακας 4: Αντιστοίχιση των προτεινόμενων PETs με άρθρα του GDPR 53

Ακρωνύμια

API	Application Programming Interface (Διεπαφή Προγραμματισμού Εφαρμογών)
APEC	Asia-Pacific Economic Cooperation (Cross-Border Privacy Rules)
BLE	Bluetooth Low Energy
CCPA	California Consumer Privacy Act
CGM	Continuous Glucose Monitor (Συνεχής Μετρητής Γλυκόζης)
CNIL	Commission Nationale de l'Informatique et des Libertés (Γαλλική Αρχή Προστασίας Δεδομένων)
DFD	Data Flow Diagram (Διάγραμμα Ροής Δεδομένων)
DID	Decentralized Identifier (Αποκεντρωμένο Αναγνωριστικό)
DP	Differential Privacy (Διαφορική Ιδιωτικότητα)
DPA	Data Processing Agreement (Συμφωνία Επεξεργασίας Δεδομένων)
DPIA	Data Protection Impact Assessment (Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων)
ENISA	European Union Agency for Cybersecurity
FHE	Fully Homomorphic Encryption (Πλήρως Ομομορφική Κρυπτογράφηση)
FL	Federated Learning (Ομοσπονδιακή Μάθηση)
GDPR	General Data Protection Regulation (Γενικός Κανονισμός Προστασίας Δεδομένων)
GPS	Global Positioning System
HE	Homomorphic Encryption (Ομομορφική Κρυπτογράφηση)
HIPAA	Health Insurance Portability and Accountability Act
HRV	Heart Rate Variability (Μεταβλητότητα Καρδιακού Ρυθμού)
IoT	Internet of Things (Διαδίκτυο των Πραγμάτων)
LDP	Local Differential Privacy (Τοπική Διαφορική Ιδιωτικότητα)
LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance
MAC	Media Access Control
PET(s)	Privacy Enhancing Technology/Technologies (Τεχνολογίες Ενίσχυσης Ιδιωτικότητας)
PIA	Privacy Impact Assessment (Ανάλυση Αντικτύπου για την Ιδιωτικότητα)
PIPEDA	Personal Information Protection and Electronic Documents Act (Καναδάς)
PPG	Photoplethysmography (Φωτοπληθυσμογραφία)
SCCs	Standard Contractual Clauses (Πρότυπες Συμβατικές Ρήτρες)
SMC	Secure Multiparty Computation (Ασφαλής Πολυμερής Υπολογιστική)
SpO_2	Κορεσμός οξυγόνου του αίματος
SSI	Self-Sovereign Identity (Αυτοκυρίαρχη Ψηφιακή Ταυτότητα)
TIA	Transfer Impact Assessment (Αξιολόγηση Επιπτώσεων Μεταφοράς)
ZKP	Zero-Knowledge Proof (Αποδεικτικό Μηδενικής Γνώσης)
ΗΚΓ ECG	Ηλεκτροκαρδιογράφημα Electrocardiogram
ΗΜΓ EMG	Ηλεκτρομυογράφημα Electromyogram

Περίληψη

Τα ενδυτά συστήματα (wearable systems), όπως τα έξυπνα ρολόγια, οι ιχνηλάτες φυσικής κατάστασης και οι έξυπνες συσκευές υγείας, συλλέγουν και επεξεργάζονται καθημερινά τεράστιους όγκους προσωπικών και βιομετρικών δεδομένων. Η ραγδαία διάδοσή τους εγείρει σοβαρά ζητήματα ιδιωτικότητας, καθώς η συλλογή, η αποθήκευση και η διάχυση ευαίσθητων πληροφοριών μπορεί να οδηγήσει σε παραβιάσεις με σοβαρές συνέπειες για τους χρήστες.

Η παρούσα διπλωματική εργασία μελετά συστηματικά τα ζητήματα ιδιωτικότητας που προκύπτουν στα ενδυτά συστήματα. Αρχικά παρουσιάζονται οι κατηγορίες, οι τεχνολογίες και οι εφαρμογές τους. Στη συνέχεια, ταξινομούνται και αναλύονται οι κίνδυνοι και οι απειλές ιδιωτικότητας με βάση τη μεθοδολογία LINDDUN, με αναφορά σε πραγματικά περιστατικά παραβίασης δεδομένων (Ultrahuman, Meta Ray-Ban, Whoop). Ακολούθως, εξετάζονται οι κυριότερες Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (PETs) – ανωνυμοποίηση και ψευδωνυμοποίηση, ομομορφική κρυπτογράφηση, ασφαλής πολυμερής υπολογιστική, διαφορική ιδιωτικότητα, αποδεικτικά μηδενικής γνώσης και ομοσπονδιακή μάθηση – και αξιολογείται η δυνατότητα εφαρμογής τους σε συσκευές με περιορισμένους υπολογιστικούς πόρους. Αναλύονται επίσης οι απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), ο ρόλος των PETs στη συμμόρφωση και η μεθοδολογία Ανάλυσης Αντικτύπου για την Ιδιωτικότητα (PIA). Τέλος, το θεωρητικό πλαίσιο εφαρμόζεται σε μελέτη περίπτωσης έξυπνου δαχτυλιδιού, για την οποία καταρτίζεται διάγραμμα ροής δεδομένων, ιεραρχούνται οι απειλές και προτείνεται ένα πολυεπίπεδο σύνολο μέτρων προστασίας, αντιστοιχισμένο με τις απαιτήσεις του GDPR.

Τα αποτελέσματα αναδεικνύουν ότι, παρά τους σημαντικούς τεχνικούς περιορισμούς (υπολογιστικό κόστος, κατανάλωση ενέργειας, απώλεια χρησιμότητας), οι PETs αποτελούν αναγκαία συνιστώσα για την υπεύθυνη ανάπτυξη και χρήση των ενδυτών συστημάτων. Καμία τεχνική δεν επαρκεί από μόνη της· ο συνδυασμός τους, μαζί με οργανωτικά μέτρα και τη συμμόρφωση με το κανονιστικό πλαίσιο, προσφέρει την αποτελεσματικότερη προστασία.

Λέξεις Κλειδιά: *Ιδιωτικότητα, Ενδυτά Συστήματα, LINDDUN, Τεχνολογίες Ενίσχυσης Ιδιωτικότητας, GDPR, Ομομορφική Κρυπτογράφηση, Έξυπνο Δαχτυλίδι*

Abstract

Wearable systems, such as smartwatches, fitness trackers and smart health devices, continuously collect and process vast amounts of personal and biometric data. Their rapid adoption raises serious privacy concerns, as the collection, storage and dissemination of sensitive information may lead to breaches with severe consequences for users.

This thesis systematically studies the privacy issues arising in wearable systems. It first presents the categories, technologies and applications of wearable devices. It then classifies and analyzes privacy risks and threats using the LINDDUN methodology, supported by real-world data breach incidents (Ultrahuman, Meta Ray-Ban, Whoop). Next, it examines the main Privacy Enhancing Technologies (PETs) – anonymization and pseudonymization, homomorphic encryption, secure multiparty computation, differential privacy, zero-knowledge proofs and federated learning – and assesses their applicability to resource-constrained devices. It also analyzes the requirements of the General Data Protection Regulation (GDPR), the role of PETs in achieving compliance, and the Privacy Impact Assessment (PIA) methodology. Finally, the theoretical framework is applied to a smart ring case study, for which a data flow diagram is developed, threats are prioritized, and a multi-layered set of protection measures mapped to GDPR requirements is proposed.

The findings show that, despite significant technical limitations (computational cost, energy consumption, utility loss), PETs constitute a necessary component for the responsible development and use of wearable systems. No single technique is sufficient on its own; their combination, together with organizational measures and compliance with the regulatory framework, provides the most effective protection.

Keywords: *Privacy, Wearable Systems, LINDDUN, Privacy Enhancing Technologies, GDPR, Homomorphic Encryption, Smart Ring*

1 *Εισαγωγή*

1.1 Τα Ενδυτά Συστήματα και το Ζήτημα της Ιδιωτικότητας

Τα ενδυτά συστήματα (wearable systems) αποτελούν μια ταχέως αναπτυσσόμενη κατηγορία τεχνολογιών, η οποία έχει μεταβάλει ριζικά τον τρόπο με τον οποίο ο άνθρωπος αλληλεπιδρά με τις συσκευές και παρακολουθεί την υγεία και την ευεξία του. Στην κατηγορία αυτή περιλαμβάνονται συσκευές όπως τα έξυπνα ρολόγια (smartwatches), οι ιχνηλάτες φυσικής κατάστασης (fitness trackers), τα έξυπνα δαχτυλίδια και γενικότερα συσκευές με ενσωματωμένους αισθητήρες. Μέσω αισθητήρων, επεξεργαστών και λογισμικού, οι συσκευές αυτές επιτρέπουν τη συνεχή συλλογή και ανάλυση μεγάλου όγκου προσωπικών δεδομένων, συχνά ευαίσθητων, όπως βιομετρικά στοιχεία, ιατρικές μετρήσεις και καθημερινές δραστηριότητες του χρήστη. Ωστόσο, η ευρεία χρήση τους θέτει σημαντικά ζητήματα ιδιωτικότητας, καθώς η συλλογή, η αποθήκευση και η επεξεργασία των δεδομένων αυτών, μπορεί να οδηγήσει σε παραβιάσεις ή κακή χρήση, με σοβαρές συνέπειες για τους χρήστες.

Η ιδιωτικότητα στα ενδυτά συστήματα δεν αποτελεί απλώς τεχνικό πρόβλημα, αλλά θεμελιώδες ανθρώπινο δικαίωμα, η προστασία του οποίου απαιτεί την ενσωμάτωση κατάλληλων μέτρων ήδη από τον σχεδιασμό των συστημάτων (Privacy by Design). Οι Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (Privacy Enhancing Technologies – PETs) έχουν αναδειχθεί σε κρίσιμα εργαλεία για την αντιμετώπιση των προκλήσεων αυτών, προσφέροντας τεχνικές όπως η ανωνυμοποίηση, η ομομορφική κρυπτογράφηση και η διαφορική ιδιωτικότητα. Παράλληλα, το ευρωπαϊκό κανονιστικό πλαίσιο, και ιδίως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), θέτει αυστηρές απαιτήσεις για την επεξεργασία των δεδομένων υγείας που συλλέγουν οι συσκευές αυτές.

1.2 Αντικείμενο διπλωματικής

Η παρούσα διπλωματική εργασία έχει ως στόχο να μελετήσει διεξοδικά τα ζητήματα ιδιωτικότητας που προκύπτουν στα ενδυτά συστήματα, να παρουσιάσει τις βασικές απειλές και τους κινδύνους

που σχετίζονται με αυτά και να αναλύσει τις σύγχρονες τεχνολογίες προστασίας που μπορούν να ενσωματωθούν για την ενίσχυση της ιδιωτικότητας, σε συνάρτηση με τις απαιτήσεις του ισχύοντος νομικού πλαισίου.

Μέσα από θεωρητική προσέγγιση, εφαρμογή της μεθοδολογίας ανάλυσης απειλών LINDDUN και μελέτη πραγματικών περιστατικών παραβίασης δεδομένων, αναδεικνύεται ο ρόλος των Τεχνολογιών Ενίσχυσης Ιδιωτικότητας (PETs) στην προστασία των προσωπικών δεδομένων των χρηστών ενδυτών συσκευών. Η θεωρητική ανάλυση εφαρμόζεται τελικά σε μια μελέτη περίπτωσης έξυπνου δαχτυλιδιού (smart ring), για την οποία καταρτίζεται διάγραμμα ροής δεδομένων, πραγματοποιείται ανάλυση και ιεράρχηση απειλών, προτείνονται συγκεκριμένα μέτρα προστασίας και αξιολογείται η συμμόρφωσή τους με τον GDPR.

1.2.1 Σκοπός της εργασίας

Σκοπός της παρούσας διπλωματικής εργασίας είναι η συστηματική διερεύνηση των προκλήσεων ιδιωτικότητας στα ενδυτά συστήματα και η πρόταση ενός συγκεντρωτικού πλαισίου προστασίας. Ειδικότερα, η εργασία επιδιώκει:

1. Την ανάδειξη και ταξινόμηση των απειλών ιδιωτικότητας που αντιμετωπίζουν οι χρήστες ενδυτών συσκευών, μέσω της εφαρμογής της μεθοδολογίας LINDDUN.
2. Την αξιολόγηση της καταλληλότητας των σύγχρονων PETs για συσκευές με περιορισμένους υπολογιστικούς πόρους, όπως τα έξυπνα δαχτυλίδια.
3. Τη διερεύνηση του τρόπου με τον οποίο οι PETs υποστηρίζουν τη συμμόρφωση με τις αρχές και τις υποχρεώσεις του GDPR.
4. Την εφαρμογή του θεωρητικού πλαισίου σε μια συγκεκριμένη μελέτη περίπτωσης (έξυπνο δαχτυλίδι), προτείνοντας συγκεκριμένα μέτρα προστασίας και αξιολογώντας τη νομική τους συμμόρφωση.

Με τον τρόπο αυτό, η εργασία φιλοδοξεί να συμβάλει στην κατανόηση των προκλήσεων ιδιωτικότητας των ενδυτών συστημάτων και να προσφέρει πρακτικές κατευθύνσεις για την ανάπτυξη συσκευών που σέβονται την ιδιωτικότητα από τον σχεδιασμό τους.

1.2.2 Ερευνητικά Ερωτήματα

Η εργασία επιχειρεί να απαντήσει στα ακόλουθα ερευνητικά ερωτήματα:

1. Ποιες είναι οι κυριότερες απειλές ιδιωτικότητας που προκύπτουν από τη συλλογή και την επεξεργασία δεδομένων σε ενδυτά συστήματα και πώς μπορούν να ταξινομηθούν συστηματικά;
2. Ποιες Τεχνολογίες Ενίσχυσης Ιδιωτικότητας είναι κατάλληλες για ενδυτά συστήματα και ποιοι είναι οι περιορισμοί τους σε συσκευές με περιορισμένους υπολογιστικούς πόρους;
3. Με ποιον τρόπο οι PETs υποστηρίζουν τη συμμόρφωση με τις αρχές και τις υποχρεώσεις του GDPR;

4. Πώς μπορεί το παραπάνω πλαίσιο να εφαρμοστεί σε ένα συγκεκριμένο ένδυτο σύστημα, όπως το έξυπνο δαχτυλίδι;

1.3 Δομή της διπλωματικής

Η δομή της εργασίας έχει ως εξής. Στο Κεφάλαιο 2 παρουσιάζονται τα ενδυτά συστήματα, οι κατηγορίες, οι τεχνολογίες και οι λειτουργίες τους, καθώς και οι εφαρμογές και οι προκλήσεις τους. Στο Κεφάλαιο 3 αναλύονται οι κίνδυνοι και οι απειλές ιδιωτικότητας που σχετίζονται με τα ενδυτά συστήματα. Στο Κεφάλαιο 4 εξετάζονται οι κυριότερες Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (ανωνυμοποίηση και ψευδωνυμοποίηση, ομομορφική κρυπτογράφηση, ασφαλής πολυμερής υπολογιστική, διαφορική ιδιωτικότητα, αποδεικτικά μηδενικής γνώσης, ομοσπονδιακή μάθηση και κατανεμημένη αναλυτική), καθώς και οι συνδυασμοί τους. Στο Κεφάλαιο 5 αναλύεται το νομικό και κανονιστικό πλαίσιο, με έμφαση στον GDPR, στον ρόλο των PETs στη συμμόρφωση και περιλαμβάνεται μια σύντομη αναφορά στην Ανάλυση Αντικτύπου για την Ιδιωτικότητα (PIA) ως εργαλείο συμμόρφωσης. Στο Κεφάλαιο 6 το σύνολο της θεωρητικής ανάλυσης εφαρμόζεται σε μια μελέτη περίπτωσης έξυπνου δαχτυλιδιού. Τέλος, στο Κεφάλαιο 7 συνοψίζονται τα συμπεράσματα της εργασίας και προτείνονται κατευθύνσεις για μελλοντική έρευνα.

2 *Ενδυτά Συστήματα (Wearable Systems)*

2.1 Ορισμός και Κατηγορίες Ενδυτών Συστημάτων

Τα ενδυτά συστήματα αποτελούν μια κατηγορία συσκευών που μπορεί να φορεθεί από τον χρήστη, η οποία ενσωματώνεται σε ρούχα ή φοριέται απευθείας πάνω στο σώμα, προσφέροντας συνεχή παρακολούθηση και συλλογή δεδομένων σχετικά με τη φυσική κατάσταση, τη δραστηριότητα, και άλλες βιομετρικές παραμέτρους του χρήστη.

Οι βασικές κατηγορίες των ενδυτών συστημάτων περιλαμβάνουν:

- **Έξυπνα ρολόγια (Smartwatches):** Συσκευές όπως τα Apple Watch, Samsung Galaxy Watch και Garmin, που προσφέρουν λειτουργίες παρακολούθησης υγείας, ειδοποιήσεων, επικοινωνίας και πλοήγησης.
- **Ιχνηλάτες φυσικής κατάστασης (Fitness Trackers):** Συσκευές όπως τα Fitbit και Xiaomi Mi Band, που εστιάζουν στην καταγραφή δραστηριότητας, θερμίδων, ύπνου και καρδιακών παλμών.
- **Έξυπνα ρούχα (Smart Clothing):** Ενδύματα με ενσωματωμένους αισθητήρες για παρακολούθηση βιοσημάτων, όπως ηλεκτροκαρδιογραφήματα (ΗΚΓ) και ηλεκτρομυογραφήματα (ΗΜΓ). Παράδειγμα αποτελούν τα έξυπνα αθλητικά ενδύματα, όπως μπλούζες(Hexoskin), κάλτσες και παπούτσια για δρομείς που προσαρμόζουν το δέσιμό τους.
- **Ιατρικές φορητές συσκευές (Medical Wearables):** Περιλαμβάνονται όλες οι εξειδικευμένες συσκευές που είναι εγκεκριμένες από υγειονομικούς φορείς για την συνεχή παρακολούθηση των ασθενών.Συσκευές όπως συνεχείς μετρητές γλυκόζης (CGM), απινιδωτές και παρακολουθητές αρτηριακής πίεσης, που χρησιμοποιούνται για την παρακολούθηση ασθενών.
- **Έξυπνα ακουστικά (Smart Earables):** Συσκευές όπως τα ασύρματα ακουστικά με ενσωματωμένους αισθητήρες καρδιακών παλμών και θερμοκρασίας.
- **Έξυπνα γυαλιά (Smart Glasses):** Συσκευές όπως τα Google Glass και Microsoft HoloLens, που προσφέρουν επαυξημένη πραγματικότητα και οπτική πληροφόρηση.

- **Έξυπνα δαχτυλίδια και κοσμήματα (Smart Rings & Jewerly):** Συσκευές όπως το Oura Ring και Samsung Galaxy Ring, που συνδυάζουν τη μόδα με την τεχνολογία, που εστιάζουν στην καταγραφή βιομετρικών δεδομένων.

Οι κατηγορίες αυτές διαφοροποιούνται ως προς τον σκοπό χρήσης, τον τύπο δεδομένων που συλλέγουν και το επίπεδο επεξεργαστικής ικανότητας. Κοινό χαρακτηριστικό όλων είναι η δυνατότητα συνεχούς παρακολούθησης και η σύνδεση με άλλες συσκευές και υπηρεσίες νέφους.

2.2 Τεχνολογίες και Λειτουργίες

Η τεχνολογική πρόοδος οδήγησε στη μείωση του μεγέθους, την αύξηση της ενεργειακής αποδοτικότητας, και τη βελτίωση των αισθητήρων, γεγονός που έχει καταστήσει τα ενδυτά συστήματα πιο προσιτά και διαδεδομένα.

Οι βασικές τεχνολογίες που επιτρέπουν τη λειτουργία των ενδυτών συσκευών είναι οι εξής:

- **Αισθητήρες (Sensors):** Οι αισθητήρες αποτελούν τη θεμελιώδη συνιστώσα των wearable συστημάτων. Οι σύγχρονοι αισθητήρες επιτρέπουν την ακριβή καταγραφή πληθώρας φυσιολογικών και περιβαλλοντικών παραμέτρων. Περιλαμβάνουν βιομετρικούς αισθητήρες όπως, αισθητήρες καρδιακών παλμών (PPG) και κορεσμού του αίματος(SpO_2) και αισθητήρες ηλεκτροδερμικής δραστηριότητας για την καταγραφή του στρες. Αισθητήρες κίνησης, όπως επιταχυνσιόμετρα και γυροσκόπια για καταγραφή βηματισμού και κινησιολογίας. Αισθητήρες περιβάλλοντος, όπως GPS, αισθητήρες θερμοκρασίας και αισθητήρες εγγύτητας που αφορούν την αλληλεπίδραση σύμφωνα με την κατάσταση.
- **Επεξεργαστές και Μικροελεγκτές:** Οι επεξεργαστές χαμηλής κατανάλωσης (όπως ARM Cortex-M) διαχειρίζονται τη συλλογή, επεξεργασία και αποθήκευση δεδομένων, εξασφαλίζοντας αυτονομία μπαταρίας, παρόλο του εξαιρετικά μικρού μεγέθους τους. Οι σύγχρονες γενιές αυτών των επεξεργαστών υποστηρίζουν Υπολογιστική στο Άκρο (Edge Computing), τεχνολογία που επιτρέπει στη συσκευή να αναλύει τα δεδομένα τοπικά χωρίς να περιμένει απάντηση από το σύννεφο (Cloud).
- **Συνδεσιμότητα:** Τα περισσότερα ενδυτά συστήματα υποστηρίζουν Bluetooth Low Energy (BLE), για συνεχή, χαμηλής κατανάλωσης σύνδεση μεταξύ συσκευών. Ακόμη, υποστηρίζουν Wi-Fi, και σε ορισμένες περιπτώσεις κυψελωτή συνδεσιμότητα (4G/5G) για επικοινωνία με κινητές συσκευές και υπηρεσίες νέφους, δίνωντας αυτονομία λειτουργίας. Ορισμένες συσκευές διαθέτουν και Near Field Communication (NFC) για ανέπαφες πληρωμές και γρήγορη σύζευξη.
- **Τεχνητή Νοημοσύνη και Μηχανική Μάθηση:** Αλγόριθμοι μηχανικής μάθησης ενσωματώνονται για την ανάλυση δεδομένων σε πραγματικό χρόνο, η λειτουργία των συσκευών βασίζεται σε υβριδικό μοντέλο επεξεργασίας, ελαφριοί αλγόριθμοι εκτελούνται απευθείας στη συσκευή (Edge AI) για την επιτόπου ανίχνευση κρίσιμων συμβάντων. Ενώ, ο όγκος των ιστορικών δεδομένων μεταφέρεται στο σύννεφο (Cloud AI) για βαθύτερη ανάλυση. Επιπρόσθετα, μέσω της αναγνώρισης προτύπων, τα συστήματα μαθαίνουν τα

μοτίβα συνηθειών, τις βιολογικές σταθερές και ρυθμούς του χρήστη και συμβάλλουν στη δημιουργία προφίλ. Τέλος, η παροχή εξατομικευμένων πληροφοριών υγείας, μέσω προγνωστικής ανάλυσης προειδοποιεί έγκαιρα τον χρήστη για πιθανούς κινδύνους..

- **Αποθήκευση και Διαχείριση Ενέργειας:** Οι μπαταρίες μικρού μεγέθους και τα συστήματα διαχείρισης ενέργειας επιτρέπουν την παρατεταμένη λειτουργία. Στην κατηγορία αυτή ανήκουν Μπαταρίες Λιθίου (Lithium-Ion / Lithium-Polymer) υψηλής ενεργειακής πυκνότητας, οι οποίες συχνά κατασκευάζονται σε εύκαμπτες ή καμπύλες γεωμετρίες για να προσαρμόζονται στο σχήμα της συσκευής (π.χ. σε δαχτυλίδια). Η παρατεταμένη αυτονομία εξασφαλίζεται από εξειδικευμένα Ολοκληρωμένα Κυκλώματα Διαχείρισης Ενέργειας (PMICs - Power Management ICs), τα οποία ελέγχουν δυναμικά την τάση, απενεργοποιούν τα μη χρησιμοποιούμενα υποσυστήματα και ελαχιστοποιούν την απώλεια ρεύματος. Παράλληλα, τεχνολογίες ασύρματης φόρτισης και ενεργειακής συγκομιδής (energy harvesting) βρίσκονται σε ανάπτυξη.

Συνοψίζοντας, οι λειτουργίες των ενδυτών συστημάτων καλύπτουν ένα ευρύ φάσμα εφαρμογών, από την παρακολούθηση υγείας (καρδιακοί παλμοί, ύπνος, δραστηριότητα) έως την ασφάλεια (ανίχνευση πτώσεων, ειδοποιήσεις SOS), την επικοινωνία (κλήσεις, μηνύματα) και την ψυχαγωγία (μουσική, παιχνίδια). Ωστόσο, η συνεχής συλλογή δεδομένων σε πραγματικό χρόνο δημιουργεί προκλήσεις όσον αφορά την επεξεργασία, την αποθήκευση και, κυρίως, την προστασία της ιδιωτικότητας των χρηστών.

2.3 Εφαρμογές και Προκλήσεις

Τα ενδυτά συστήματα βρίσκουν εφαρμογή σε πολλαπλούς τομείς όπως:

- **Τομέας Υγείας:** Παρακολούθηση ζωτικών σημείων, διαχείριση χρόνιων παθήσεων (διαβήτης, καρδιαγγειακές νόσοι), αποκατάσταση ασθενών, τηλεϊατρική και πρόληψη ασθενειών.
- **Αθλητισμός και Φυσική Κατάσταση:** Καταγραφή απόδοσης, βελτιστοποίηση προπόνησης, ανάλυση τεχνικής και πρόληψη τραυματισμών.
- **Επαγγελματικός Χώρος:** Παρακολούθηση εργαζομένων σε επικίνδυνα περιβάλλοντα (π.χ. ανίχνευση τοξικών αερίων), διαχείριση χρόνου εργασίας, βελτίωση παραγωγικότητας.
- **Ασφάλεια και Έκτακτες Ανάγκες:** Ανίχνευση πτώσεων και άμεση αποστολή σημάτων κινδύνου(SOS) με γεωεντοπισμό, παρακολούθηση και προστασίας ευάλωτων ατόμων.
- **Εκπαίδευση και Ψυχαγωγία:** Επαυξημένη πραγματικότητα (AR/VR), διαδραστικά παιχνίδια, εξατομικευμένη και βιωματική μάθηση μέσω έξυπνων αξεσουάρ .

Ωστόσο, οι προκλήσεις που αντιμετωπίζουν είναι εξίσου σημαντικές:

- **Διάρκεια Μπαταρίας:** Η περιορισμένη χωρητικότητα μπαταρίας αποτελεί έναν από τους σημαντικότερους περιορισμούς, καθώς η συνεχής λειτουργία αισθητήρων και ασύρματης επικοινωνίας αυξάνει την κατανάλωση ενέργειας.

- **Ακρίβεια και Αξιοπιστία Δεδομένων:** Η ποιότητα των δεδομένων που συλλέγονται από αισθητήρες μπορεί να επηρεαστεί από την έντονη κίνηση του σώματος, την λανθασμένη θέση της συσκευής και περιβαλλοντικούς παράγοντες που προκαλούν θόρυβο στους αισθητήρες, αυξάνοντας τις πιθανότητες για εσφαλμένες διαγνώσεις.
- **Ιδιωτικότητα και Ασφάλεια:** Η συνεχής συλλογή ευαίσθητων προσωπικών δεδομένων δημιουργεί σοβαρούς κινδύνους για την ιδιωτικότητα των χρηστών. Όπως επισημαίνουν οι Hong et al. (2004), ο σχεδιασμός συστημάτων διάχυτου υπολογισμού (ubiquitous computing) πρέπει να ενσωματώνει μοντέλα ανάλυσης κινδύνων για την προστασία της ιδιωτικότητας από τα πρώτα στάδια ανάπτυξης. Οι κίνδυνοι περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση, διαρροές δεδομένων, κατάχρηση από τρίτους και παραβίαση της ανωνυμίας.
- **Διαλειτουργικότητα:** Η ετερογένεια των συσκευών, πρωτοκόλλων και πλατφορμών δυσχεραίνει την ομαλή ενσωμάτωση και ανταλλαγή δεδομένων.
- **Κανονιστική Συμμόρφωση:** Η τήρηση νομικών πλαισίων όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) απαιτεί αυστηρότερους ελέγχους και τεχνικές λύσεις για την προστασία των δεδομένων. Αναγκαία καθίσταται η διενέργεια Εκτιμήσεων Αντικτύπου (DPIA/PIA) πριν από τη διάθεση των συσκευών στην αγορά.
- **Αποδοχή και Εμπιστοσύνη Χρηστών:** Η ανησυχία των χρηστών σχετικά με τη χρήση των δεδομένων τους και οι επιπτώσεις στην ιδιωτικότητα μπορεί να περιορίσουν την υιοθέτηση των wearable συστημάτων.

Στο πλαίσιο αυτό, η ομοσπονδιακή μάθηση (Federated Learning) αναδεικνύεται ως μια πολλά υποσχόμενη τεχνική που επιτρέπει την εκπαίδευση μοντέλων μηχανικής μάθησης σε κατανεμημένα δεδομένα, χωρίς την ανάγκη συγκέντρωσης προσωπικών δεδομένων σε κεντρικό διακομιστή, μειώνοντας έτσι τους κινδύνους ιδιωτικότητας. Ωστόσο, η ομοσπονδιακή μάθηση παραμένει ευάλωτη σε ορισμένες κυβερνοεπιθέσεις και απαιτεί περαιτέρω ενίσχυση των μηχανισμών άμυνας και κρυπτογράφησης.

Συνολικά, τα ενδυτά συστήματα αποτελούν ένα δυναμικό πεδίο τεχνολογικής και ερευνητικής ανάπτυξης, με τεράστιες προοπτικές στον τομέα της υγείας, του αθλητισμού και της βιομηχανίας. Καθώς παρατηρείται η καθολική υιοθέτηση των συσκευών αυτών, η διασφάλιση της ιδιωτικότητας παίζει καθοριστικό ρόλο για την ευρεία αποδοχή και επιτυχία τους.

3 *Κίνδυνοι και Απειλές Ιδιωτικότητας σε Ενδυτά Συστήματα*

3.1 Ταξινόμηση και Ανάλυση Απειλών Ιδιωτικότητας

Τα ενδυτά συστήματα συλλέγουν, αποθηκεύουν και επεξεργάζονται καθημερινά τεράστιο όγκο προσωπικών και βιομετρικών δεδομένων, όπως τον καρδιακό ρυθμό, το επίπεδο φυσικής δραστηριότητας, την τοποθεσία και άλλες ευαίσθητες πληροφορίες που σχετίζονται με την υγεία των χρηστών. Το γεγονός αυτό δημιουργεί σημαντικούς κινδύνους για την ιδιωτικότητα. Για την αποτίμηση του μεγέθους του προβλήματος, αξίζει να εξεταστεί η έκταση της αγοράς και του όγκου δεδομένων που παράγεται. Το 2024 οι παγκόσμιες αποστολές φορητών συσκευών, στις οποίες συμπεριλαμβάνονται και οι ενδυτές, ξεπέρασαν τα 543 εκατομμύρια τεμάχια, σημειώνοντας αύξηση 6,1% σε σχέση με το προηγούμενο έτος, ενώ προβλέπεται ότι έως το 2029 οι χρήστες έξυπνων ρολογιών θα ανέλθουν σε 740 εκατομμύρια παγκοσμίως. Η άνοδος αυτή οφείλεται σε μεγάλο βαθμό στην τεχνολογική εξέλιξη των αισθητήρων: ένα σύγχρονο έξυπνο ρολόι μπορεί να καταγράφει ανά δευτερόλεπτο δεδομένα για τον καρδιακό ρυθμό και τα βήματα, δημιουργώντας δεκάδες χιλιάδες μεμονωμένα σημεία δεδομένων ανά ημέρα. Με περισσότερες από 500 εκατομμύρια φορητές συσκευές σε χρήση παγκοσμίως, το συνολικό αποτύπωμα δεδομένων του οικοσυστήματος φτάνει τα τρισεκατομμύρια σημεία δεδομένων ετησίως. Στις ενότητες που ακολουθούν οι απειλές που απορρέουν από αυτή την κατάσταση ταξινομούνται σε πέντε βασικές κατηγορίες.

3.1.1 Συλλογή και Υπερσυλλογή Δεδομένων

Το πρόβλημα της υπερσυλλογής εμφανίζεται όταν οι κατασκευαστές και οι πάροχοι υπηρεσιών συλλέγουν δεδομένα πέραν των ελάχιστων λειτουργικά απαραίτητων, παραβιάζοντας έτσι τη θεμελιώδη αρχή της ελαχιστοποίησης των δεδομένων (data minimisation) που επιβάλλει ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης. Όπως επισημαίνεται σε μελέτη του ENISA (2022), η διασφάλιση της τήρησης βασικών αρχών προστασίας δεδομένων,

όπως η διαφάνεια και η ελαχιστοποίηση, δεν είναι πάντοτε εύκολη στο περιβάλλον των φορητών συσκευών.

Η αξία των δεδομένων αυτών είναι ιδιαίτερα υψηλή: σύμφωνα με έκθεση της Trustwave του 2021, τα αρχεία δεδομένων υγειονομικής περίθαλψης αποτιμώνται έως και 250 δολάρια ανά αρχείο, λόγω των εκτεταμένων προσωπικών πληροφοριών που περιέχουν. Ως απόκριση, έχουν θεσπιστεί διάφορες ρυθμίσεις που καθορίζουν το επίπεδο προστασίας των δεδομένων των καταναλωτών. Πλαίσια όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης, ο νόμος HIPAA (Health Insurance Portability and Accountability Act) των Ηνωμένων Πολιτειών, ο νόμος CCPA (California Consumer Privacy Act) της Καλιφόρνιας, ο καναδικός νόμος PIPEDA και οι Διασυνοριακοί Κανόνες Προστασίας της Ιδιωτικής Ζωής της Οικονομικής Συνεργασίας Ασίας-Ειρηνικού (APEC) συγκροτούν ένα παγκόσμιο πλέγμα μέτρων προστασίας, που αποσκοπεί στην ισορροπία μεταξύ της προστασίας του απορρήτου, της τεχνολογικής καινοτομίας και της διαλειτουργικότητας. Ωστόσο, οι εθνικές διαφορές και οι μη διαφανείς πρακτικές τρίτων δημιουργούν ρυθμιστικές «γκρίζες ζώνες», τις οποίες εκμεταλλεύονται εταιρείες εις βάρος του δικαιώματος στην ιδιωτικότητα.

3.1.2 Παρακολούθηση και Καταγραφή Συμπεριφοράς

Πέρα από την ποσοτική διάσταση των δεδομένων, κρίσιμη είναι και η ποιοτική. Τα ενδυτά συστήματα έχουν την ικανότητα να καταγράφουν όχι μόνο βιομετρικά μεγέθη, αλλά και πρότυπα συμπεριφοράς, καθημερινές ρουτίνες, κοινωνικές αλληλεπιδράσεις και τη διάθεση του χρήστη. Η συνεχής παρακολούθηση επιτρέπει τη δημιουργία λεπτομερών ψηφιακών προφίλ (profiling). Η συγκέντρωση των δεδομένων αυτών από τρίτες εταιρείες, για παράδειγμα διαφημιστικές, μπορεί να οδηγήσει σε καταχρηστικές πρακτικές, κοινωνικό αποκλεισμό ή στοχευμένη χειραγώγηση της συμπεριφοράς του καταναλωτή.

3.1.3 Διαρροές και Μη Εξουσιοδοτημένη Πρόσβαση

Η οικονομική αξία των δεδομένων υγείας καθιστά τις συσκευές και τις υποδομές τους ελκυστικό στόχο για επιθέσεις ransomware και κλοπής ταυτότητας. Οι θεωρητικές απειλές γίνονται απτές μέσα από πραγματικά περιστατικά παραβιάσεων των τελευταίων ετών, με χαρακτηριστικότερα τα εξής:

- **Ultrahuman (Μάρτιος 2026):** Σε ένα χαρακτηριστικό περιστατικό, μη εξουσιοδοτημένοι χρήστες κατάφεραν να αποκτήσουν πρόσβαση σε δεδομένα ευεξίας πελατών των έξυπνων δαχτυλιδιών της εταιρείας φορητής τεχνολογίας υγείας Ultrahuman. Η επίθεση πραγματοποιήθηκε μέσω κλοπής διαπιστευτηρίων υπαλλήλου από φορητό υπολογιστή, με τη χρήση κακόβουλου λογισμικού. Οι δράστες απέκτησαν πρόσβαση σε εσωτερικό σύστημα ανάλυσης, θέτοντας σε κίνδυνο τουλάχιστον 700 πελάτες. Το γεγονός αυτό αναδεικνύει ότι ακόμη και τα εσωτερικά συστήματα των εταιρειών αποτελούν αδύναμο

κρίκο, καθώς ένας μόνο υπάλληλος μπορεί να γίνει η πύλη εισόδου για μαζική διαρροή ευαίσθητων δεδομένων.

- **Meta Ray-Ban Smart Glasses (2026):** Σε μια διαφορετική κατηγορία απειλής, η Meta αντιμετώπισε ομαδική αγωγή για τα έξυπνα γυαλιά Ray-Ban με ενσωματωμένη τεχνητή νοημοσύνη. Η αγωγή υποστήριξε ότι η συσκευή λειτουργούσε ως κανάλι συνεχούς επιτήρησης, καταγράφοντας οπτικοακουστικό υλικό χωρίς τη συναίνεση των τρίτων, και θέτοντας τους χρήστες σε κίνδυνο εκβιασμού, κλοπής ταυτότητας και ζημιάς στη φήμη. Η περίπτωση αυτή αποκαλύπτει τις νέες ηθικές και νομικές προκλήσεις των συσκευών που «βλέπουν» και «ακούν» διαρκώς, μετατρέποντας τον δημόσιο χώρο σε ένα αχανές πεδίο συλλογής δεδομένων.
- **Whoop (2025):** Η εταιρεία Whoop βρέθηκε αντιμέτωπη με αγωγή σχετικά με την κοινή χρήση προσωπικών δεδομένων υγείας —όχι μόνο καρδιακών παλμών και προτύπων ύπνου, αλλά και μετρήσεων αναπαραγωγικής υγείας και ιστορικού προβολής βίντεο— χωρίς την ρητή συγκατάθεση των χρηστών. Το περιστατικό αυτό υπογραμμίζει την τάση των εταιρειών να εμπορευματοποιούν τα δεδομένα, θεωρώντας τα ως περιουσιακό στοιχείο, παραβλέποντας τις επιταγές της ενημερωμένης συγκατάθεσης. Σύμφωνα με μαρτυρίες, τα δεδομένα κοινοποιούνταν σε τρίτους διαφημιστές και ερευνητές, γεγονός που συνιστά παραβίαση της εμπιστευτικότητας.

3.1.4 Επαναναγνώριση και Συναγωγή Πληροφοριών

Μια από τις πιο σύνθετες απειλές αφορά την ικανότητα συσχέτισης φαινομενικά ανώνυμων ή αποσπασματικών δεδομένων με σκοπό την πλήρη επαναναγνώριση (re-identification) του ατόμου. Λόγω της μοναδικότητας που παρουσιάζουν τα βιομετρικά και χωρικά δεδομένα (π.χ. το μοτίβο βαδίσματος ή οι καθημερινές διαδρομές GPS), η εφαρμογή απλών τεχνικών συγκάλυψης της ταυτότητας αποδεικνύεται ανεπαρκής. Κακόβουλοι δρώντες ή εξελιγμένοι αλγόριθμοι μηχανικής μάθησης μπορούν να διασταυρώσουν ετερογενή σύνολα δεδομένων από διαφορετικές πηγές και να ανασυνθέσουν την ταυτότητα του χρήστη, εξάγοντας συμπεράσματα για πτυχές της ζωής του που ο ίδιος δεν είχε σκοπό να αποκαλύψει.

3.1.5 Έλλειψη Διαφάνειας και Ελέγχου

Τέλος, μια εξίσου κρίσιμη κατηγορία απειλών αφορά τη θεσμική διάσταση της ιδιωτικότητας: την έλλειψη διαφάνειας, ενημέρωσης και ελέγχου από την πλευρά των χρηστών. Παρά την ύπαρξη νομοθετικών πλαισίων, η εφαρμογή τους στο πεδίο των ενδυτών συσκευών παραμένει προβληματική.

Μια συστηματική ανάλυση των πολιτικών απορρήτου 17 κορυφαίων κατασκευαστών φορητών συσκευών αποκάλυψε σοβαρές ελλείψεις. Η υψηλότερη βαθμολογία κινδύνου καταγράφηκε στις διαστάσεις της διαφάνειας (76%) και της γνωστοποίησης τρωτών σημείων (65%). Οι περισσότερες πολιτικές είναι γραμμένες σε εξαιρετικά δυσνόητη γλώσσα, με εκτενείς νομικές δηλώσεις που

λειτουργούν ως «παγίδες αποδοχής», ωθώντας τον μέσο χρήστη να συναινέσει χωρίς να κατανοεί το πραγματικό εύρος της επεξεργασίας. Εταιρείες όπως η Xiaomi, η Wyze και η Huawei παρουσίασαν τις υψηλότερες σωρευτικές βαθμολογίες κινδύνου, υποδηλώνοντας ότι ορισμένες αγορές εμφανίζουν μεγαλύτερη χαλαρότητα στην τήρηση των κανονιστικών απαιτήσεων.

Σε πολλές περιπτώσεις, ακόμη κι αν ο χρήστης διαπιστώσει ότι τα δεδομένα του χρησιμοποιούνται με ανεπιθύμητο τρόπο, η διαδικασία για την ανάκληση είναι περίπλοκη, μη-προφανής, ή ακόμη και αδύνατη, καθώς τα δεδομένα έχουν ήδη ενσωματωθεί σε ιστορικά αρχεία εκπαίδευσης μοντέλων τεχνητής νοημοσύνης.

Όλα τα παραπάνω οδηγούν σε ένα σοβαρό συμπέρασμα: τα ενδυτά συστήματα δημιουργούν ένα ψηφιακό περιβάλλον όπου ο χρήστης χάνει τον έλεγχο των πιο προσωπικών του πληροφοριών, γεγονός που επιτείνει τις κοινωνικές ανισότητες και υπονομεύει την εμπιστοσύνη στην τεχνολογία. Η έλλειψη ενημέρωσης (Unawareness) αποτελεί την πιο ύπουλη απειλή, καθώς δρα στο παρασκήνιο, διαβρώνοντας συνεχώς την αυτονομία του ατόμου.

Συμπερασματικά, η επισκόπηση των απειλών φανερώνει ότι οι προκλήσεις για την ιδιωτικότητα δεν έχουν μόνο τεχνική, αλλά και θεσμική, οικονομική και ηθική διάσταση. Κρίνεται επομένως αναγκαία η συστηματική ανάλυση των απειλών μέσω δομημένων μεθοδολογιών, όπως η LINDDUN, προκειμένου να σχεδιαστούν αποτελεσματικές στρατηγικές μετριασμού των κινδύνων.

3.1.6 Συμπεράσματα

Η ανάλυση του παρόντος κεφαλαίου κατέδειξε ότι τα ενδυτά συστήματα αντιμετωπίζουν ένα πολυδιάστατο και διαρκώς εξελισσόμενο τοπίο απειλών ιδιωτικότητας. Οι απειλές αυτές εκτείνονται από τη μαζική και συνεχή συλλογή βιομετρικών δεδομένων και την παρακολούθηση συμπεριφοράς έως τις διαρροές, την επαναναγνώριση, την έλλειψη διαφάνειας και τη μη συμμόρφωση με το νομικό πλαίσιο. Όπως αναδείχθηκε, το πρόβλημα δεν είναι αποκλειστικά τεχνικό· συνιστά ταυτόχρονα θεσμική, οικονομική και ηθική πρόκληση, καθώς οι χρήστες συχνά χάνουν τον έλεγχο των πιο προσωπικών τους πληροφοριών, ενώ οι ρυθμιστικές «γκρίζες ζώνες» επιτρέπουν την εκμετάλλευσή τους.

Συμπερασματικά, η κατανόηση του τοπίου των απειλών θέτει τις βάσεις για την επόμενη κρίσιμη φάση: την επιλογή και εφαρμογή των κατάλληλων Τεχνολογιών Ενίσχυσης Ιδιωτικότητας (PETs), οι οποίες θα αναλυθούν στο επόμενο κεφάλαιο.

4 *Τεχνολογίες Ενίσχυσης Ιδιωτικότητας για Ενδυτά Συστήματα*

4.1 Εισαγωγή

Σύμφωνα με την αρχή της «Προστασίας της Ιδιωτικότητας από τον Σχεδιασμό» (Privacy by Design), η ενσωμάτωση κατάλληλων τεχνικών μέτρων από τα πρώτα στάδια σχεδιασμού των συστημάτων κρίνεται απαραίτητη για την αντιμετώπιση απειλών. Σε προηγούμενα κεφάλαια αναδείχθηκε ότι τα ενδυτά συστήματα αντιμετωπίζουν ένα εκτεταμένο φάσμα απειλών ιδιωτικότητας, που εκτείνονται από την υπερσυλλογή δεδομένων και την παρακολούθηση συμπεριφοράς έως τις διαρροές, την επαναναγνώριση και την έλλειψη διαφάνειας.

Οι Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (Privacy Enhancing Technologies – PETs) αποτελούν σημαντικά εργαλεία για την αντιμετώπιση αυτών των προκλήσεων. Σύμφωνα με τον ENISA, οι PETs είναι τεχνολογίες και εργαλεία που υποστηρίζουν τη διαφύλαξη της ιδιωτικότητας και των προσωπικών δεδομένων (ENISA, 2022). Επιδιώκουν να εξισορροπήσουν δύο φαινομενικά αντιφατικούς στόχους: αφενός την αξιοποίηση των δεδομένων για ανάλυση, έρευνα και παροχή υπηρεσιών και αφετέρου την προστασία της ιδιωτικότητας των υποκειμένων των δεδομένων.

Στο πλαίσιο των ενδυτών συστημάτων, οι PETs αποκτούν ιδιαίτερη σημασία λόγω της φύσης των δεδομένων που διαχειρίζονται (ευαίσθητα βιομετρικά και δεδομένα υγείας), των περιορισμένων υπολογιστικών πόρων των συσκευών και της ανάγκης για λειτουργία σε πραγματικό χρόνο. Το παρόν κεφάλαιο παρουσιάζει τις βασικές κατηγορίες PETs που είναι σχετικές με τα ενδυτά συστήματα, αναλύοντας τις αρχές λειτουργίας τους, τα πλεονεκτήματα και τους περιορισμούς τους.

4.2 Ανωνυμοποίηση και Ψευδωνυμοποίηση Δεδομένων

4.2.1 Ορισμοί και Βασικές Αρχές

Η ανωνυμοποίηση (anonymization) και η ψευδωνυμοποίηση (pseudonymization) αποτελούν δύο θεμελιώδεις τεχνικές για την προστασία της ιδιωτικότητας, οι οποίες στοχεύουν στη παρεμπόδιση ή στην αδυναμία σύνδεσης των δεδομένων με το υποκείμενό τους.

Η ψευδωνυμοποίηση είναι η διαδικασία αντικατάστασης των άμεσων αναγνωριστικών (όπως ονοματεπώνυμο, αριθμός ταυτότητας, διεύθυνση) με ψευδώνυμα (pseudonyms). Πρόκειται για μια αναστρέψιμη διαδικασία: εφόσον κάποιος έχει πρόσβαση στο κατάλληλο κλειδί αντιστοίχισης, μπορεί να επαναφέρει την αρχική ταυτότητα. Ο GDPR αναγνωρίζει την ψευδωνυμοποίηση ως ένα σημαντικό μέτρο προστασίας δεδομένων, το οποίο μπορεί να μειώσει τους κινδύνους για τα υποκείμενα των δεδομένων, αλλά δεν καθιστά τα δεδομένα ανώνυμα.

Η ανωνυμοποίηση, αντιθέτως, αποσκοπεί στην πλήρη και μη αναστρέψιμη αφαίρεση κάθε δυνατότητας σύνδεσης των δεδομένων με το υποκείμενό τους. Τα ανωνυμοποιημένα δεδομένα δεν εμπίπτουν στο πεδίο εφαρμογής του GDPR, καθώς δεν θεωρούνται πλέον προσωπικά δεδομένα. Ωστόσο, όπως αναλύεται στη συνέχεια της ενότητας, η πλήρης ανωνυμοποίηση είναι ιδιαίτερα δύσκολη να επιτευχθεί στην πράξη, ειδικά σε περιβάλλοντα πλούσιων δεδομένων.

4.2.2 Τεχνικές Ψευδωνυμοποίησης

Στα ενδυτά συστήματα, η ψευδωνυμοποίηση μπορεί να εφαρμοστεί σε διάφορα στάδια της επεξεργασίας δεδομένων:

- **Αντικατάσταση με τυχαίους αναγνωριστικούς κωδικούς:** Κάθε χρήστης αντιστοιχίζεται σε ένα μοναδικό, τυχαίο αναγνωριστικό (UUID), το οποίο χρησιμοποιείται σε όλες τις εσωτερικές διεργασίες. Το αρχείο αντιστοίχισης φυλάσσεται σε ασφαλές περιβάλλον με αυστηρούς ελέγχους πρόσβασης.
- **Tokenization:** Τα ευαίσθητα δεδομένα (π.χ., αναγνωριστικά συσκευής, διευθύνσεις MAC) αντικαθίστανται από μη-αναστρέψιμα tokens, τα οποία παράγονται μέσω κρυπτογραφικών συναρτήσεων κατακερματισμού (hashing).
- **Κρυπτογραφική ψευδωνυμοποίηση:** Χρήση κρυπτογραφικών τεχνικών που επιτρέπουν την επεξεργασία των δεδομένων υπό το ψευδώνυμο, χωρίς να αποκαλύπτεται η πραγματική ταυτότητα.

Η ψευδωνυμοποίηση αποτελεί μια πρακτική λύση για πολλές εφαρμογές ενδυτών συστημάτων, καθώς επιτρέπει την ανάλυση δεδομένων (π.χ., στατιστικές μελέτες, εκπαίδευση μοντέλων) χωρίς την άμεση έκθεση των αναγνωριστικών των χρηστών. Ωστόσο, η ψευδωνυμοποίηση από μόνη της δεν επαρκεί για την προστασία από την επαναναγνώριση.

4.2.3 Προκλήσεις και Περιορισμοί

Παρά τη χρησιμότητά τους, τόσο η ανωνυμοποίηση όσο και η ψευδωνυμοποίηση παρουσιάζουν σημαντικούς περιορισμούς, ειδικά στο πλαίσιο των ενδυτών συστημάτων:

- **Κίνδυνος επαναναγνώρισης (re-identification):** Όπως αναδείχθηκε στο Κεφάλαιο 3, ακόμη και μετά την αφαίρεση των άμεσων αναγνωριστικών, ο συνδυασμός διαφορετικών συνόλων δεδομένων μπορεί να οδηγήσει στην ταυτοποίηση του υποκειμένου. Τα βιομετρικά δεδομένα (π.χ., καρδιακός ρυθμός, πρότυπα βηματισμού) παρουσιάζουν μοναδικές διακυμάνσεις που λειτουργούν σχεδόν σαν «αποτύπωμα», καθιστώντας την πλήρη ανωνυμοποίηση εξαιρετικά δύσκολη.
- **Απώλεια χρησιμότητας δεδομένων:** Οι τεχνικές ανωνυμοποίησης που είναι αποτελεσματικές (π.χ., γενίκευση, συσσωμάτωση) συχνά οδηγούν σε σημαντική απώλεια της λεπτομέρειας και της χρησιμότητας των δεδομένων για ανάλυση.
- **Περιορισμένη προστασία από συναγωγή πληροφοριών:** Η ανωνυμοποίηση δεν προστατεύει από τη συναγωγή νέων πληροφοριών (inference) από τα δεδομένα. Για παράδειγμα, ακόμη κι αν τα δεδομένα βηματισμού είναι ανωνυμοποιημένα, μπορούν να χρησιμοποιηθούν για να συναχθεί το ύψος, το βάρος και η ηλικία του χρήστη.
- **Πολυπλοκότητα εφαρμογής σε πραγματικό χρόνο:** Οι συσκευές wearables λειτουργούν σε πραγματικό χρόνο και διαθέτουν περιορισμένους υπολογιστικούς πόρους. Η εφαρμογή προηγμένων τεχνικών ανωνυμοποίησης επί της συσκευής μπορεί να είναι υπολογιστικά απαιτητική.

Λαμβάνοντας υπόψη αυτούς τους περιορισμούς, η σύγχρονη έρευνα έχει στραφεί σε πιο προηγμένες τεχνικές, όπως η διαφορική ιδιωτικότητα, η ομομορφική κρυπτογράφηση και η ομοσπονδιακή μάθηση, οι οποίες επιτρέπουν την εξαγωγή χρήσιμων πληροφοριών από τα δεδομένα χωρίς να τα αποκαλύπτουν.

4.3 Ομομορφική Κρυπτογράφηση

4.3.1 Ορισμός και Βασικές Αρχές

Η ομομορφική κρυπτογράφηση (Homomorphic Encryption – HE) είναι μια κρυπτογραφική τεχνική που επιτρέπει την εκτέλεση υπολογισμών σε κρυπτογραφημένα δεδομένα, χωρίς να απαιτείται η αποκρυπτογράφησή τους. Τα αποτελέσματα των υπολογισμών προκύπτουν επίσης κρυπτογραφημένα και, όταν αποκρυπτογραφηθούν, ταυτίζονται με τα αποτελέσματα που θα προέκυπταν αν οι υπολογισμοί είχαν εκτελεστεί στα αρχικά (μη κρυπτογραφημένα) δεδομένα.

Η ιδιότητα αυτή καθιστά την ομομορφική κρυπτογράφηση ιδιαίτερα ελκυστική για εφαρμογές ενδυτών συστημάτων, όπου ευαίσθητα δεδομένα υγείας πρέπει να υποβάλλονται σε ανάλυση από τρίτους (π.χ., παρόχους υπηρεσιών νέφους, ερευνητικά κέντρα) χωρίς να αποκαλύπτονται τα ίδια τα δεδομένα.

Πλήρως Ομομορφική Κρυπτογράφηση (Fully Homomorphic Encryption – FHE): Οι πρώτες υλοποιήσεις ομομορφικής κρυπτογράφησης υποστήριζαν μόνο συγκεκριμένες πράξεις (π.χ., μόνο πρόσθεση ή μόνο πολλαπλασιασμό). Η πλήρως ομομορφική κρυπτογράφηση, που παρουσιάστηκε για πρώτη φορά από τον Gentry το 2009, επιτρέπει την εκτέλεση οποιουδήποτε υπολογισμού σε κρυπτογραφημένα δεδομένα. Πρακτικά σχήματα FHE περιλαμβάνουν τα BFV (Brakerski-Fan-Vercauteren) για ακέραιους αριθμούς, CKKS (Cheon-Kim-Kim-Song) για προσεγγιστικούς πραγματικούς αριθμούς (ιδιαίτερα χρήσιμο για δεδομένα υγείας), και TFHE για υπολογισμούς με δυαδικά δεδομένα

4.3.2 Εφαρμογή σε Ενδυτά και Πλεονεκτήματα

Σε ένα τυπικό σενάριο, τα δεδομένα από τους αισθητήρες της wearable συσκευής κρυπτογραφούνται στην ίδια τη συσκευή χρησιμοποιώντας ένα σχήμα FHE και αποστέλλονται σε έναν διακομιστή νέφους. Ο διακομιστής εκτελεί τους απαραίτητους υπολογισμούς (π.χ., ανάλυση καρδιακών παλμών, ανίχνευση ανωμαλιών) απευθείας πάνω στα κρυπτογραφημένα δεδομένα και επιστρέφει τα κρυπτογραφημένα αποτελέσματα στη συσκευή, η οποία τα αποκρυπτογραφεί. Σε κανένα σημείο της διαδικασίας ο διακομιστής δεν έχει πρόσβαση στα αρχικά δεδομένα.

Τα πλεονεκτήματα της τεχνικής αυτής είναι:

- Συμμόρφωση με την αρχή της ελαχιστοποίησης δεδομένων.
- Πλήρης προστασία των δεδομένων κατά την επεξεργασία από τρίτους.
- Δυνατότητα αξιοποίησης υπηρεσιών νέφους χωρίς να διακυβεύεται η ιδιωτικότητα.

4.3.3 Περιορισμοί

Παρόλα τα παραπάνω προκύπτουν οι εξής περιορισμοί:

- **Υπολογιστικό κόστος:** Η FHE είναι εξαιρετικά υπολογιστικά απαιτητική. Ένας απλός πολλαπλασιασμός σε κρυπτογραφημένα δεδομένα μπορεί να είναι χιλιάδες φορές πιο αργός από τον αντίστοιχο σε αποκρυπτογραφημένα δεδομένα.
- **Μέγεθος δεδομένων:** Τα κρυπτογραφημένα δεδομένα είναι σημαντικά μεγαλύτερα από τα αρχικά, γεγονός που δημιουργεί προβλήματα αποθήκευσης και μετάδοσης.
- **Περιορισμένοι πόροι συσκευής:** Οι wearable συσκευές διαθέτουν περιορισμένη υπολογιστική ισχύ και μπαταρία, γεγονός που καθιστά δύσκολη την εκτέλεση κρυπτογράφησης FHE επί της συσκευής. Έρευνες εξετάζουν ελαφρύτερες κρυπτογραφικές μεθόδους που παρέχουν προστασία σε πραγματικό χρόνο για περιορισμένες wearable συσκευές

Ωστόσο, η ομομορφική κρυπτογράφηση αποτελεί ένα από τα πλέον υποσχόμενα πεδία έρευνας για την ασφαλή επεξεργασία δεδομένων υγείας, με εφαρμογές σε σενάρια όπως η ασφαλής ιατρική διάγνωση και η παρακολούθηση υγείας με έξυπνες wearable συσκευές.

4.4 Ασφαλής Πολυμερής Υπολογιστική

4.4.1 Ορισμός και Εφαρμογή σε Ενδυτά

Η Ασφαλής Πολυμερής Υπολογιστική (Secure Multiparty Computation – SMC) είναι μια κρυπτογραφική τεχνική που επιτρέπει σε πολλά μέρη να υπολογίσουν από κοινού μια συνάρτηση των εισόδων τους, χωρίς να αποκαλύψουν τις εισόδους τους μεταξύ τους. Κάθε μέρος γνωρίζει μόνο τη δική του είσοδο και το τελικό αποτέλεσμα, αλλά τίποτα για τις εισόδους των άλλων.

Στο πλαίσιο των ενδυτών συστημάτων, η SMC μπορεί να εφαρμοστεί σε σενάρια όπου πολλαπλές οντότητες (π.χ., διαφορετικά νοσοκομεία, ερευνητικά κέντρα, κατασκευαστές συσκευών) επιθυμούν να συνεργαστούν για την ανάλυση δεδομένων υγείας, χωρίς να μοιράζονται τα ευαίσθητα δεδομένα των ασθενών τους. Παραδείγματα περιλαμβάνουν:

- **Στατιστική ανάλυση σε κατανεμημένα δεδομένα:** Υπολογισμός μέσων όρων, διακυμάνσεων ή άλλων στατιστικών μεγεθών (π.χ. μέσος όρος καρδιακών παλμών ανά ηλικιακή ομάδα) χωρίς αποκάλυψη ατομικών εγγραφών.
- **Εκπαίδευση μοντέλων μηχανικής μάθησης:** Πολλαπλοί φορείς συνεργάζονται για την εκπαίδευση ενός μοντέλου, χωρίς να αποκαλύπτουν τα δεδομένα τους.
- **Ασφαλής συσχέτιση δεδομένων:** Σύνδεση δεδομένων από διαφορετικές πηγές (π.χ., δεδομένα wearable συσκευών με ιατρικά αρχεία) χωρίς αποκάλυψη ταυτοτήτων.

4.4.2 Τεχνικές SMC

Οι βασικές τεχνικές που χρησιμοποιούνται στην SMC περιλαμβάνουν:

- **Κατάτμηση μυστικών (Secret Sharing):** Κάθε είσοδος διασπάται σε πολλά τμήματα (shares), τα οποία κατανέμονται στα μέρη. Κανένα μέρος δεν μπορεί να ανασυνθέσει την είσοδο μόνο του.
- **Αόριστη μεταφορά (Oblivious Transfer):** Επιτρέπει σε ένα μέρος να λάβει μια τιμή από μια λίστα που κατέχει ένα άλλο μέρος, χωρίς το δεύτερο να μάθει ποια τιμή επιλέχθηκε.
- **Συγκαλυμμένα κυκλώματα (Garbled Circuits):** Επιτρέπουν την εκτέλεση υπολογισμών χωρίς αποκάλυψη των εισόδων.

4.4.3 Πλεονεκτήματα SMC

Τα κύρια πλεονεκτήματα της Ασφαλούς Πολυμερούς Υπολογιστικής είναι:

- Πλήρης προστασία των δεδομένων κατά τη συνεργατική ανάλυση.
- Δυνατότητα συμμετοχής πολλαπλών μερών χωρίς εμπιστοσύνη σε κεντρικό διαμεσολαβητή.
- Εφαρμογή σε διάφορους τύπους υπολογισμών.

4.4.4 Περιορισμοί

Οι κυριότεροι περιορισμοί της είναι οι εξής:

- **Υπολογιστική πολυπλοκότητα:** Η SMC απαιτεί εκτεταμένες επικοινωνίες μεταξύ των μερών, γεγονός που αυξάνει τον χρόνο εκτέλεσης, επιβαρύνοντας τις ένδυτες συσκευές που διαθέτουν χαμηλότερη επεξεργαστική ισχύ.
- **Επικοινωνιακό κόστος:** Το κόστος επικοινωνίας μπορεί να είναι σημαντικό, ειδικά για πολύπλοκους υπολογισμούς, οπότε αυξάνεται η κατανάλωση της μπαταρίας.
- **Απαιτήσεις συγχρονισμού:** Όλα τα μέρη πρέπει να συμμετέχουν ταυτόχρονα στον υπολογισμό.

Σε συνδυασμό με την ομομορφική κρυπτογράφηση, η SMC αποτελεί μια ισχυρή λύση για σενάρια όπου πολλαπλοί φορείς επιθυμούν να συνεργαστούν χωρίς να διακυβεύσουν την ιδιωτικότητα των δεδομένων τους.

4.5 Διαφορική Ιδιωτικότητα

4.5.1 Ορισμός

Η Διαφορική Ιδιωτικότητα (Differential Privacy – DP) είναι μια μαθηματική προσέγγιση για την προστασία της ιδιωτικότητας κατά τη δημοσίευση στατιστικών πληροφοριών από ένα σύνολο δεδομένων. Σε αντίθεση με τις παραδοσιακές τεχνικές ανωνυμοποίησης, η DP παρέχει αυστηρές μαθηματικές εγγυήσεις για το επίπεδο προστασίας της ιδιωτικότητας, ανεξάρτητα από τις γνώσεις που μπορεί να έχει ένας επιτιθέμενος.

Η βασική ιδέα της διαφορικής ιδιωτικότητας είναι η εξής: η παρουσία ή η απουσία οποιουδήποτε μεμονωμένου ατόμου στο σύνολο δεδομένων δεν πρέπει να επηρεάζει σημαντικά το αποτέλεσμα μιας στατιστικής ερώτησης. Αυτό επιτυγχάνεται με την προσθήκη ελεγχόμενου θορύβου (συνήθως από την κατανομή Laplace ή Gauss) στα αποτελέσματα των ερωτήσεων. Η ποσότητα του θορύβου ρυθμίζεται από μια παράμετρο που ονομάζεται προϋπολογισμός ιδιωτικότητας (privacy budget), που συμβολίζεται με το γράμμα ε (έψιλον). Μικρότερες τιμές του ε συνεπάγονται ισχυρότερη προστασία της ιδιωτικότητας αλλά μεγαλύτερη απώλεια ακρίβειας. Αντίθετα μεγαλύτερες τιμές του ε εγγυώνται υψηλότερη ακρίβεια των στατιστικών αποτελεσμάτων, αλλά ασθενέστερη προστασίας της ιδιωτικότητας.

Τοπική Διαφορική Ιδιωτικότητα (Local Differential Privacy – LDP): Στην κλασική διαφορική ιδιωτικότητα, ο θόρυβος προστίθεται από τον διαχειριστή του συνόλου δεδομένων πριν από τη δημοσίευση. Στην τοπική διαφορική ιδιωτικότητα, ο θόρυβος προστίθεται από κάθε χρήστη στα δεδομένα του, πριν αυτά αποσταλούν στον συλλέκτη. Αυτό είναι ιδιαίτερα σημαντικό για τα ενδυτά συστήματα, όπου τα δεδομένα παράγονται σε αποκεντρωμένες συσκευές(όπου προστίθεται ο θόρυβος) και αποστέλλονται σε κεντρικούς διακομιστές.

4.5.2 Εφαρμογή σε Ενδυτά Συστήματα και Πλεονεκτήματα

Στα ενδυτά συστήματα, η διαφορική ιδιωτικότητα μπορεί να εφαρμοστεί σε σενάρια όπως:

- **Δημοσίευση στατιστικών υγείας:** Οι ερευνητές μπορούν να δημοσιεύουν στατιστικά στοιχεία για πληθυσμούς (π.χ., μέσος καρδιακός ρυθμός, πρότυπα ύπνου) χωρίς να αποκαλύπτουν πληροφορίες για μεμονωμένα άτομα.
- **Εκπαίδευση μοντέλων μηχανικής μάθησης:** Η διαφορική ιδιωτικότητα μπορεί να ενσωματωθεί στη διαδικασία εκπαίδευσης, διασφαλίζοντας ότι το εκπαιδευμένο μοντέλο δεν αποκαλύπτει πληροφορίες για συγκεκριμένα δείγματα εκπαίδευσης.
- **Παρακολούθηση υγείας σε πραγματικό χρόνο:** Η LDP επιτρέπει τη συλλογή δεδομένων από χιλιάδες wearable συσκευές για την ανίχνευση επιδημιολογικών τάσεων, χωρίς να διακυβεύεται η ιδιωτικότητα των ατόμων.

Τα πλεονεκτήματα της τεχνικής είναι:

- **Μαθηματικές εγγυήσεις:** Παρέχει αυστηρά αποδείξιμη προστασία.
- **Ανθεκτικότητα σε επιθέσεις:** Προστατεύει ακόμη και όταν ο επιτιθέμενος έχει πρόσβαση σε βοηθητικές πληροφορίες.
- **Ποσοτικοποίηση της ιδιωτικότητας:** Ο προϋπολογισμός ιδιωτικότητας επιτρέπει την ακριβή ρύθμιση του επιπέδου προστασίας.

4.5.3 Περιορισμοί

Οι κυριότεροι περιορισμοί της είναι οι εξής:

- **Απώλεια χρησιμότητας:** Ο θόρυβος που προστίθεται για την προστασία της ιδιωτικότητας μειώνει την ακρίβεια των αποτελεσμάτων.
- **Διαχείριση του προϋπολογισμού:** Κάθε ερώτηση καταναλώνει μέρος του προϋπολογισμού ιδιωτικότητας. Μετά από πολλές ερωτήσεις, ο προϋπολογισμός εξαντλείται και η προστασία εξασθενεί.
- **Παράμετροι:** Η επιλογή της κατάλληλης τιμής του ε είναι κρίσιμη και εξαρτάται αποκλειστικά από την εφαρμογή.

Πρόσφατες έρευνες έχουν δείξει ότι η διαφορική ιδιωτικότητα μπορεί να εφαρμοστεί αποτελεσματικά σε δεδομένα wearable συσκευών, επιτυγχάνοντας σημαντική μείωση του σφάλματος και προσφέροντας πρακτικές και κλιμακώσιμες λύσεις για τη δημοσίευση δεδομένων υγείας.

4.6 Αποδεικτικά Μηδενικής Γνώσης

4.6.1 Ορισμός και Εφαρμογή σε Ενδυτά

Τα Αποδεικτικά Μηδενικής Γνώσης (Zero-Knowledge Proofs – ZKP) είναι κρυπτογραφικά πρωτόκολλα που επιτρέπουν σε ένα μέρος (τον αποδεικνύοντα – prover) να αποδείξει σε ένα άλλο μέρος (τον επαληθευτή – verifier) ότι ένας ισχυρισμός είναι αληθής, χωρίς να αποκαλύψει οποιαδήποτε άλλη πληροφορία πέραν της αλήθειας του ισχυρισμού.

Στα ενδυτά συστήματα, η τεχνική αυτή βρίσκει εφαρμογή στα εξής σενάρια:

- **Επαλήθευση ταυτότητας χωρίς αποκάλυψη βιομετρικών:** Ένας χρήστης μπορεί να αποδείξει ότι είναι ο κάτοχος μιας συσκευής χωρίς να αποκαλύψει τα βιομετρικά του δεδομένα.
- **Απόδειξη συμμόρφωσης με στόχους υγείας:** Ο χρήστης αποδεικνύει ότι πέτυχε έναν στόχο άσκησης (π.χ., 10.000 βήματα) χωρίς να αποκαλύψει τα ακριβή δεδομένα βηματισμού του.
- **Επαλήθευση εγκυρότητας δεδομένων:** Επιτρέπει την επαλήθευση ότι τα δεδομένα που αποστέλλονται από μια wearable συσκευή είναι έγκυρα και δεν έχουν παραποιηθεί, χωρίς να αποκαλύπτεται το περιεχόμενό τους.
- **Ασφαλής συγκέντρωση σε ομοσπονδιακή μάθηση:** Οι συμμετέχοντες μπορούν να αποδείξουν ότι συνεισέφεραν έγκυρες ενημερώσεις στο μοντέλο, χωρίς να αποκαλύψουν τις τοπικές τους ενημερώσεις.

4.6.2 Τύποι ZKP

Οι κυριότεροι τύποι ZKP είναι οι εξής:

- **zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge):** Συμπαγή, μη-διαδραστικά αποδεικτικά, με μικρό μέγεθος και γρήγορη επαλήθευση.
- **zk-STARKs (Zero-Knowledge Scalable Transparent ARguments of Knowledge):** Κλιμακώσιμα και διαφανή αποδεικτικά (δεν απαιτούν αξιόπιστη εγκατάσταση), αλλά μεγαλύτερα σε μέγεθος.
- **Bulletproofs:** Μικρά, μη-διαδραστικά αποδεικτικά, κατάλληλα για εφαρμογές με περιορισμένους πόρους.

4.6.3 Πλεονεκτήματα

- **Πλήρης προστασία της ιδιωτικότητας:** Δεν αποκαλύπτεται καμία πληροφορία πέραν της αλήθειας του ισχυρισμού.
- **Επαληθευσιμότητα:** Ο επαληθευτής μπορεί να ελέγξει την αλήθεια του ισχυρισμού χωρίς να εμπιστεύεται τον αποδεικνύοντα.
- **Ευελιξία:** Μπορούν να εφαρμοστούν σε πολλά διαφορετικά σενάρια.

4.6.4 Περιορισμοί

- **Υπολογιστικό κόστος:** Η δημιουργία αποδεικτικών (ειδικά zk-SNARKs) απαιτεί σημαντική υπολογιστική ισχύ.
- **Πολυπλοκότητα:** Η σχεδίαση και υλοποίηση ZKP απαιτεί εξειδικευμένες γνώσεις κρυπτογραφίας.

- **Αξιόπιστη εγκατάσταση (trusted setup):** Ορισμένα σχήματα (π.χ., zk-SNARKs) απαιτούν μια φάση αξιόπιστης εγκατάστασης, η οποία εισάγει ένα σημείο ευπάθειας, αν κρατηθούν αντίγραφα κλειδιών κατά την εγκατάσταση.

Πρόσφατες έρευνες έχουν δείξει ότι τα ZKP μπορούν να εφαρμοστούν αποτελεσματικά σε περιβάλλοντα wearable, με χρόνους δημιουργίας αποδεικτικών της τάξης των 4,7 ms, καθιστώντας τα κατάλληλα για εφαρμογές σε πραγματικό χρόνο.

4.7 Ομοσπονδιακή Μάθηση

4.7.1 Ορισμός

Η Ομοσπονδιακή Μάθηση (Federated Learning – FL) είναι μια τεχνική μηχανικής μάθησης που επιτρέπει σε πολλές συσκευές ή οργανισμούς να εκπαιδεύσουν από κοινού ένα μοντέλο, χωρίς να ανταλλάσσουν ή να συγκεντρώνουν τα δεδομένα τους.

Η διαδικασία λειτουργίας της ομοσπονδιακής μάθησης περιλαμβάνει τα ακόλουθα βήματα:

1. **Αρχικοποίηση:** Ένας κεντρικός διακομιστής (server) στέλνει ένα αρχικό μοντέλο σε όλες τις συμμετέχουσες συσκευές (clients).
2. **Τοπική εκπαίδευση:** Κάθε συσκευή εκπαιδεύει το μοντέλο χρησιμοποιώντας μόνο τα τοπικά δεδομένα της, που παραμένουν στη συσκευή.
3. **Αποστολή ενημερώσεων:** Αντί για τα δεδομένα, κάθε συσκευή στέλνει πίσω στον διακομιστή μόνο τις ενημερώσεις του μοντέλου (π.χ., τα βάρη ή τις κλίσεις του νευρωνικού δικτύου).
4. **Συγκέντρωση (Aggregation):** Ο διακομιστής συλλέγει όλες τις ενημερώσεις και τις συνδυάζει (συνήθως με μια μέση τιμή – Federated Averaging) για να δημιουργήσει μια νέα, βελτιωμένη έκδοση του κεντρικού μοντέλου.
5. **Επανάληψη:** Η διαδικασία επαναλαμβάνεται για πολλούς γύρους, μέχρι το μοντέλο να φτάσει στην επιθυμητή απόδοση.

4.7.2 Εφαρμογή σε Ενδυτά Συστήματα

Η ομοσπονδιακή μάθηση είναι ιδιαίτερα κατάλληλη για τα ενδυτά συστήματα για διάφορους λόγους:

- **Προστασία της ιδιωτικότητας:** Τα ευαίσθητα δεδομένα υγείας παραμένουν στις συσκευές των χρηστών.
- **Μείωση μεταφοράς δεδομένων:** Αντί να μεταφέρονται τεράστιοι όγκοι δεδομένων στο νέφος, μεταφέρονται μόνο μικρότερα πακέτα ενημερώσεων του μοντέλου.
- **Εξατομίκευση:** Το μοντέλο μπορεί να προσαρμοστεί στις ιδιαίτερες συνθήκες κάθε χρήστη (π.χ., διαφορετικά πρότυπα ύπνου, καρδιακών παλμών).
- **Κλιμάκωση:** Μπορεί να υποστηρίξει εκατομμύρια συσκευές ταυτόχρονα.

Παραδείγματα εφαρμογών περιλαμβάνουν:

- **Πρόβλεψη καρδιακών επεισοδίων:** Εκπαίδευση μοντέλου για την πρόβλεψη καρδιακών ανωμαλιών χρησιμοποιώντας δεδομένα από χιλιάδες έξυπνα ρολόγια, χωρίς τα δεδομένα να φεύγουν από τις συσκευές.
- **Παρακολούθηση ασθενειών:** Ανίχνευση πρώιμων σημείων νόσου (π.χ., COVID-19) από δεδομένα καρδιακών παλμών και θερμοκρασίας.
- **Βελτιστοποίηση προπόνησης:** Εξατομικευμένες προτάσεις άσκησης βασισμένες σε δεδομένα από πολλούς χρήστες.

4.7.3 Προκλήσεις και Περιορισμοί

- **Ετερογένεια δεδομένων (Non-IID):** Τα δεδομένα σε κάθε συσκευή είναι συνήθως μη-αντιπροσωπευτικά του συνόλου, γεγονός που δυσκολεύει την εκπαίδευση.
- **Επικοινωνιακό κόστος:** Η συνεχής ανταλλαγή ενημερώσεων μοντέλων μπορεί να δημιουργήσει μεγάλη επιβάρυνση.
- **Περιορισμένοι πόροι συσκευής:** Οι wearable συσκευές έχουν περιορισμένη υπολογιστική ισχύ και μπαταρία, γεγονός που καθιστά δύσκολη την εκπαίδευση πολύπλοκων μοντέλων.
- **Ευπάθεια σε επιθέσεις:** Παρά τα πλεονεκτήματά της, η FL παραμένει ευάλωτη σε επιθέσεις, όπως η δηλητηρίαση μοντέλου (model poisoning) και η συναγωγή πληροφοριών από τις ενημερώσεις.

Για την αντιμετώπιση αυτών των προκλήσεων, πρόσφατες έρευνες προτείνουν την ενσωμάτωση της FL με άλλες PETs, όπως η διαφορική ιδιωτικότητα, η ομομορφική κρυπτογράφηση και τα ZKP, για την παροχή ισχυρότερων εγγυήσεων προστασίας.

4.8 Κατανεμημένη Αναλυτική

4.8.1 Ορισμός

Η Κατανεμημένη Αναλυτική (Distributed Analytics) αποτελεί μια ευρύτερη κατηγορία τεχνικών που επιτρέπουν την εκτέλεση αναλυτικών εργασιών σε δεδομένα κατανεμημένα σε πολλαπλές τοποθεσίες, χωρίς να απαιτείται η συγκέντρωσή τους. Περιλαμβάνει τεχνικές όπως:

- **Κατανεμημένη επεξεργασία ερωτημάτων:** Εκτέλεση στατιστικών ερωτήσεων σε κατανεμημένα δεδομένα.
- **Ομοσπονδιακή στατιστική:** Υπολογισμός στατιστικών μεγεθών (μέσος όρος, διάμεσος, διακύμανση) χωρίς συγκέντρωση δεδομένων.
- **Κατανεμημένη εξόρυξη δεδομένων:** Εφαρμογή αλγορίθμων εξόρυξης δεδομένων σε κατανεμημένα σύνολα.

Η κατανεμημένη αναλυτική συμπληρώνει την ομοσπονδιακή μάθηση, προσφέροντας λύσεις για σενάρια όπου δεν απαιτείται εκπαίδευση μοντέλων αλλά απλή στατιστική ανάλυση ή εξαγωγή συμπερασμάτων.

4.9 Συμπεράσματα και Συνδυαστικές Προσεγγίσεις

Η ανάλυση των Τεχνολογιών Ενίσχυσης Ιδιωτικότητας (PETs) που προηγήθηκε ανέδειξε ότι κάθε επιμέρους τεχνική προσφέρει μοναδικά πλεονεκτήματα αλλά ταυτόχρονα φέρει σημαντικούς περιορισμούς. Η διαπίστωση αυτή οδηγεί σε ένα θεμελιώδες συμπέρασμα: **η βέλτιστη στρατηγική προστασίας της ιδιωτικότητας για ένα ένδυτο σύστημα σπάνια βασίζεται σε μία μόνο τεχνολογία**. Αντιθέτως, ο συνδυασμός διαφορετικών PETs επιτρέπει την αξιοποίηση των πλεονεκτημάτων της κάθε μίας, αντισταθμίζοντας παράλληλα τους περιορισμούς της, και δημιουργώντας ένα πολυεπίπεδο αμυντικό σύστημα που καλύπτει το σύνολο των απειλών που περιγράφονται στο Κεφάλαιο 3.

Διαφορετικές τεχνικές αντιμετωπίζουν διαφορετικές κατηγορίες απειλών, και η ταυτόχρονη εφαρμογή τους καθιστά εξαιρετικά δύσκολη την παραβίαση της ιδιωτικότητας, ακόμη κι αν μία από τις τεχνικές καταστραφεί ή παρακαμφθεί. Ο συνδυασμός τεχνικών δημιουργεί ένα ολιστικό σύστημα προστασίας που καλύπτει όλες τις φάσεις του κύκλου ζωής των δεδομένων – από τη συλλογή και τη μετάδοση έως την αποθήκευση, την επεξεργασία, την ανάλυση και τη δημοσίευση αποτελεσμάτων.

Μεταξύ των πλέον υποσχόμενων υβριδικών προσεγγίσεων συγκαταλέγεται ο συνδυασμός της ομοσπονδιακής μάθησης με τη διαφορική ιδιωτικότητα. Σε αυτό το σχήμα, οι επιμέρους συσκευές εκπαιδεύουν τοπικά μοντέλα μηχανικής μάθησης, διατηρώντας τα δεδομένα υγείας των χρηστών αποκλειστικά στις ίδιες τις συσκευές. Οι ενημερώσεις των μοντέλων που αποστέλλονται στον κεντρικό διακομιστή υφίστανται επεξεργασία με προσθήκη ελεγχόμενου θορύβου, διασφαλίζοντας ότι ακόμη κι αν ένας επιτιθέμενος υποκλέψει ή αποκτήσει πρόσβαση στις ενημερώσεις, δεν μπορεί να συναγάγει πληροφορίες για μεμονωμένους χρήστες. Το πλεονέκτημα αυτού του συνδυασμού είναι ότι αντιμετωπίζει ταυτόχρονα δύο σημαντικές απειλές: την αποκάλυψη δεδομένων κατά τη μετάδοση των ενημερώσεων και τη δυνατότητα συναγωγής προσωπικών πληροφοριών από το εκπαιδευμένο μοντέλο. Σε εφαρμογές παρακολούθησης καρδιακών παλμών, για παράδειγμα, η τοπική εκπαίδευση μοντέλων σε δεδομένα εκατομμυρίων χρηστών επιτρέπει την ανίχνευση ανωμαλιών χωρίς να αποκαλύπτεται ποτέ ο καρδιακός ρυθμός ενός μεμονωμένου ατόμου, ενώ η προσθήκη θορύβου στις ενημερώσεις εξασφαλίζει ότι ακόμη και η συμβολή ενός συγκεκριμένου χρήστη παραμένει κρυφή.

Ένας εξίσου ισχυρός συνδυασμός είναι αυτός της ομοσπονδιακής μάθησης με την ομομορφική κρυπτογράφηση. Σε αυτή την περίπτωση, οι ενημερώσεις των τοπικών μοντέλων κρυπτογραφούνται πριν από την αποστολή τους στον κεντρικό διακομιστή, χρησιμοποιώντας ένα σχήμα πλήρως ομομορφικής κρυπτογράφησης (FHE). Ο διακομιστής εκτελεί τη διαδικασία

συγκέντρωσης (aggregation) των ενημερώσεων απευθείας πάνω στα κρυπτογραφημένα δεδομένα, χωρίς ποτέ να τα αποκρυπτογραφεί. Μόνο μετά την ολοκλήρωση της συγκέντρωσης, το τελικό κρυπτογραφημένο μοντέλο αποστέλλεται πίσω στις συσκευές για αποκρυπτογράφηση. Το σχήμα αυτό παρέχει το απόλυτο επίπεδο προστασίας, καθώς ο διακομιστής δεν έχει πρόσβαση σε κανένα στάδιο στα αποκρυπτογραφημένα δεδομένα ή στις επιμέρους ενημερώσεις. Παρότι το υπολογιστικό κόστος παραμένει σημαντικό, η ανάπτυξη ελαφρύτερων σχημάτων FHE και η χρήση εξειδικευμένων επιταχυντών υλικού καθιστούν σταδιακά εφικτή την υλοποίησή του ακόμη και σε συσκευές με περιορισμένους πόρους, ανοίγοντας τον δρόμο για εφαρμογές όπως η ασφαλής τηλεϊατρική διάγνωση και η απομακρυσμένη παρακολούθηση ασθενών με χρόνια νοσήματα.

Ο τρίτος σημαντικός συνδυασμός αφορά την ενσωμάτωση των αποδεικτικών μηδενικής γνώσης (ZKP) στην ομοσπονδιακή μάθηση. Τα ZKP επιτρέπουν την επαλήθευση της εγκυρότητας των ενημερώσεων που αποστέλλουν οι συσκευές, χωρίς να αποκαλύπτεται το περιεχόμενό τους. Αυτό είναι κρίσιμο για την αντιμετώπιση επιθέσεων δηλητηρίασης μοντέλου (model poisoning), όπου κακόβουλοι συμμετέχοντες αποστέλλουν σκόπιμα παραποιημένες ενημερώσεις για να υπονομεύσουν το τελικό μοντέλο. Με τη χρήση ZKP, κάθε συσκευή μπορεί να αποδείξει ότι η ενημέρωσή της υπολογίστηκε σωστά βάσει των τοπικών δεδομένων και ότι ακολουθεί τα συμφωνηθέντα πρωτόκολλα, χωρίς να χρειάζεται να αποκαλύψει ούτε τα δεδομένα ούτε την ίδια την ενημέρωση. Ο συνδυασμός αυτός ενισχύει σημαντικά την ασφάλεια και την αξιοπιστία της ομοσπονδιακής μάθησης, καθιστώντας την κατάλληλη για εφαρμογές υψηλής ευαισθησίας, όπου η ακεραιότητα των δεδομένων και η εμπιστοσύνη μεταξύ των συμμετεχόντων είναι ζωτικής σημασίας.

Σε πιο ολοκληρωμένα σχήματα, παρατηρείται η ταυτόχρονη εφαρμογή τριών ή περισσότερων τεχνολογιών. Πρόσφατες μελέτες έχουν δείξει ότι ολοκληρωμένα πλαίσια PETs που ενσωματώνουν πολλαπλές τεχνικές μπορούν να μειώσουν τους κινδύνους ιδιωτικότητας έως και 70%, διατηρώντας παράλληλα την κλινική χρησιμότητα των δεδομένων και την απόδοση του συστήματος. Συγκεκριμένα, έρευνες σε υβριδικά συστήματα που συνδυάζουν ελαφριά κρυπτογράφηση, επιλεκτική χρήση blockchain για την ασφαλή καταγραφή των ενημερώσεων, και ομοσπονδιακή μάθηση με διαφορική ιδιωτικότητα, κατέδειξαν ότι η ακρίβεια των ιατρικών προβλέψεων παραμένει σε ικανοποιητικά επίπεδα, ενώ οι χρόνοι απόκρισης σε πραγματικό χρόνο είναι συμβατοί με τις απαιτήσεις των wearable εφαρμογών.

Η επιλογή του κατάλληλου συνδυασμού PETs, ωστόσο, δεν αποτελεί μια στατική ή μονοσήμαντη απόφαση. Αντιθέτως, πρόκειται για μια δυναμική διαδικασία που πρέπει να λαμβάνει υπόψη τις συγκεκριμένες απαιτήσεις κάθε εφαρμογής. Παράγοντες όπως η ευαισθησία των δεδομένων, οι διαθέσιμοι υπολογιστικοί πόροι της συσκευής (επεξεργαστική ισχύς, μνήμη, κατανάλωση μπαταρίας), οι απαιτήσεις ταχύτητας απόκρισης (πραγματικός χρόνος έναντι μαζικής ανάλυσης), το κόστος υλοποίησης και συντήρησης, καθώς και οι νομικές υποχρεώσεις που απορρέουν από το εκάστοτε ρυθμιστικό πλαίσιο (π.χ., GDPR), επηρεάζουν την τελική απόφαση. Η

τάση της σύγχρονης έρευνας κινείται προς την ανάπτυξη ευέλικτων και προσαρμόσιμων πλαισίων PETs, που επιτρέπουν τη δυναμική επιλογή και ρύθμιση των τεχνικών ανάλογα με το εκάστοτε σενάριο χρήσης και το επίπεδο απειλής. Τα πλαίσια αυτά ενσωματώνουν μηχανισμούς αυτόματης αξιολόγησης κινδύνου και προσαρμογής των παραμέτρων προστασίας σε πραγματικό χρόνο, εξασφαλίζοντας βέλτιστη ισορροπία μεταξύ ασφάλειας και απόδοσης. Παράλληλα, η ανάπτυξη τυποποιημένων διεπαφών και πρωτοκόλλων επιτρέπει τη διαλειτουργικότητα μεταξύ διαφορετικών PETs και την ενσωμάτωσή τους σε υπάρχοντα συστήματα χωρίς σημαντικές τροποποιήσεις, διευκολύνοντας την υιοθέτησή τους από τη βιομηχανία.

Εν κατακλείδι, ο στρατηγικός συνδυασμός Τεχνολογιών Ενίσχυσης Ιδιωτικότητας αποτελεί το κλειδί για την ουσιαστική προστασία των προσωπικών δεδομένων στα ενδυτά συστήματα. Η πολυεπίπεδη προσέγγιση, που αξιοποιεί τα πλεονεκτήματα κάθε τεχνικής και αντισταθμίζει τους περιορισμούς της, δημιουργεί ένα ανθεκτικό και ολοκληρωμένο σύστημα άμυνας. Η ενσωμάτωση αυτών των συνδυαστικών προσεγγίσεων από τα πρώτα στάδια σχεδιασμού, σύμφωνα με την αρχή του Privacy by Design, διασφαλίζει ότι η καινοτομία στον τομέα των wearables προχωρά παράλληλα με τον σεβασμό του θεμελιώδους δικαιώματος της ιδιωτικότητας, ενισχύοντας την εμπιστοσύνη των χρηστών και διασφαλίζοντας τη βιωσιμότητα των εφαρμογών σε ένα αυστηροποιούμενο ρυθμιστικό περιβάλλον.

5 Νομικό και Κανονιστικό Πλαίσιο

5.1 Εισαγωγή

Οι παραπάνω ενότητες ανέδειξαν το γεγονός ότι η προστασία των προσωπικών δεδομένων στα ενδυτά συστήματα δεν είναι αποκλειστικά τεχνικό ζήτημα. Αντιθέτως, η αποτελεσματική προστασία της ιδιωτικότητας απαιτεί την ταυτόχρονη εφαρμογή τεχνικών, οργανωτικών και νομικών μέτρων. Το παρόν κεφάλαιο εξετάζει το νομικό και κανονιστικό πλαίσιο που διέπει την επεξεργασία προσωπικών δεδομένων στα ενδυτά συστήματα, με έμφαση στον Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation – GDPR) της Ευρωπαϊκής Ένωσης, ο οποίος αποτελεί το πλέον επιδραστικό ρυθμιστικό κείμενο παγκοσμίως.

Ο GDPR, ο οποίος τέθηκε σε εφαρμογή τον Μάιο του 2018, εφαρμόζεται σε όλες τις συσκευές wearables που συλλέγουν προσωπικά δεδομένα ατόμων εντός της Ευρωπαϊκής Ένωσης, ανεξάρτητα από την τοποθεσία του κατασκευαστή. Τα δεδομένα υγείας και φυσικής κατάστασης που συλλέγονται από έξυπνα ρολόγια, ιχνηλάτες φυσικής κατάστασης και ιατρικές συσκευές παρακολούθησης ταξινομούνται ως ευαίσθητα δεδομένα υγείας σύμφωνα με το Άρθρο 9 του GDPR, απαιτώντας το υψηλότερο επίπεδο προστασίας και ρητή συγκατάθεση για την επεξεργασία τους. Η μη συμμόρφωση με τον Κανονισμό μπορεί να οδηγήσει σε πρόστιμα έως και 4% του ετήσιου κύκλου εργασιών ή 20 εκατομμύρια ευρώ, όποιο από τα δύο είναι υψηλότερο.

Το κεφάλαιο αναλύει τις βασικές αρχές του GDPR που είναι σχετικές με τα ενδυτά συστήματα, τις απαιτήσεις συμμόρφωσης και τον ρόλο των PETs στην επίτευξή τους, καθώς γίνεται αναφορά και στη μεθοδολογία της Ανάλυσης Αντικτύπου για την Ιδιωτικότητα (Privacy Impact Assessment - PIA) ως εργαλείο για την προληπτική αξιολόγηση και διαχείριση των κινδύνων ιδιωτικότητας.

5.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων και οι Επιπτώσεις του στα Ενδυτά Συστήματα

5.2.1 Το Πεδίο Εφαρμογής του GDPR στα Ενδυτά Συστήματα

Ο GDPR εφαρμόζεται ανεξάρτητα από την έδρα του κατασκευαστή, εφόσον η συσκευή επεξεργάζεται δεδομένα φυσικών προσώπων που βρίσκονται στην Ευρωπαϊκή Ένωση ή

παρακολουθεί τη συμπεριφορά τους εντός της ΕΕ (Άρθρο 3). Ως φορητή τεχνολογία (wearable technology) νοείται κάθε συσκευή που φοριέται στο σώμα και επεξεργάζεται προσωπικά δεδομένα φυσικών προσώπων, συμπεριλαμβανομένων των έξυπνων ρολογιών, των ιχνηλατών φυσικής κατάστασης, των ιατρικών συσκευών παρακολούθησης, των έξυπνων ρούχων και των συνδεδεμένων ιατρικών συσκευών.

Σημαντική είναι η διαφοροποίηση μεταξύ προσωπικών δεδομένων και δεδομένων υγείας. Το άρθρο 9 του GDPR ορίζει τα δεδομένα υγείας ως κάθε πληροφορία που αφορά τη σωματική ή ψυχική κατάσταση υγείας ενός φυσικού προσώπου και απαιτείται ρητή συγκατάθεση. Όσον αφορά τις φορητές συσκευές, ο ορισμός αυτός καλύπτει πολύ περισσότερα από τα προφανή ιατρικά δεδομένα. Ακόμη και δεδομένα που φαίνονται αβλαβή μπορούν να αποκαλύψουν πληροφορίες σχετικά με την υγεία, όταν συνδυαστούν ή αναλυθούν σε βάθος χρόνου. Στα δεδομένα υγείας συμπεριλαμβάνονται: βιομετρικές μετρήσεις, ενδείξεις ιατρικών συσκευών, δείκτες φυσικής κατάστασης και οποιαδήποτε δεδομένα που αποκαλύπτουν την κατάσταση της υγείας ή τη σωματική κατάσταση. Αντίθετα, άλλα προσωπικά δεδομένα μπορούν να υποβληθούν σε επεξεργασία βάσει των νομικών βάσεων που ορίζονται στο άρθρο 6. Στα προσωπικά δεδομένα συγκαταλέγονται: προτιμήσεις συσκευών, τα στοιχεία επικοινωνίας που συγχρονίζονται από smartphone, τα προφίλ χρηστών και βασικές πληροφορίες τοποθεσίας.

Ωστόσο, υπάρχουν και τα σενάρια μεικτών δεδομένων όπου η συμμόρφωση περιπλέκεται. Όταν η παρακολούθηση βασικής λειτουργίας δραστηριότητας μπορεί να μετατραπεί σε επεξεργασία δεδομένων υγείας, προκύπτει ένα σενάριο αυτής της κατηγορίας. Για παράδειγμα, ο συνδυασμός του αριθμού βημάτων με την παρακολούθηση της τοποθεσίας για την εξαγωγή συμπερασμάτων σχετικά με την κατάσταση της υγείας. Συνδυασμοί αυτής της φύσεως επιβάλλουν αυστηρές νομικές απαιτήσεις.

Για να κριθεί αν τα δεδομένα που συλλέγει μια ένδυτη συσκευή εμπίπτουν στις ειδικές κατηγορίες δεδομένων, μπορεί να εφαρμοστεί το ακόλουθο μοντέλο αξιολόγησης:

- **Αξιολόγηση περιεχομένου (Content Evaluation):** Είναι τα δεδομένα άμεσες βιομετρικές μετρήσεις;
- **Ανάλυση συμφραζομένων (Context Analysis):** Χρησιμοποιούνται τα δεδομένα για παρακολούθηση υγείας;
- **Πρότυπα χρήσης (Usage Patterns):** Περιλαμβάνουν μακροχρόνια παρακολούθηση υγείας;
- **Προσδιορισμός επίδρασης (Effect Determination):** Παράγουν πληροφορίες για την υγεία;
- **Χαρακτηριστικά παραδείγματα δεδομένων που ταξινομούνται ως δεδομένα υγείας είναι:** μετρήσεις καρδιακού ρυθμού, δείκτες ποιότητας ύπνου, δείκτες επιπέδου άγχους, δεδομένα έντασης προπόνησης, ακόμα και ο αριθμός βημάτων μπορεί να θεωρηθεί δεδομένο υγείας όταν αναλύεται με σκοπό την αξιολόγηση της κατάστασης υγείας ή της ιατρικής κατάστασης ενός ατόμου. Συμπερασματικά, οι βασικές πληροφορίες δραστηριότητας της καθημερινής ζωής μπορούν να συσχετιστούν με την υγεία όταν

συνδυάζονται με αλγόριθμους για την εκτίμηση κινδύνων ασθενειών ή καταστάσεων ψυχικής υγείας. Αυτή η ευρεία ερμηνεία αντανακλά την παραδοχή της ΕΕ ότι οι φορητές συσκευές αποκαλύπτουν προσωπικές λεπτομέρειες σχετικά με την υγεία μέσω εξελιγμένης επεξεργασίας δεδομένων.

5.2.2 Οι Βασικές Αρχές

Ο GDPR επιβάλλει ένα ολοκληρωμένο σύνολο αρχών και απαιτήσεων που διέπουν κάθε πτυχή της επεξεργασίας προσωπικών δεδομένων από φορητές συσκευές. Ο Κανονισμός χαρακτηρίζεται ως «βασιζόμενος σε αρχές» (principles-based), με το Άρθρο 5 να θεσπίζει επτά θεμελιώδεις αρχές, τις οποίες οι υπεύθυνοι επεξεργασίας οφείλουν να τηρούν σε κάθε στάδιο της συλλογής και της επεξεργασίας:

1. **Αρχή της Νομιμότητας, Αμεροληψίας και Διαφάνειας (Lawfulness, Fairness and Transparency):** τα δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Αυτό σημαίνει ότι οι χρήστες φορητών συσκευών πρέπει να ενημερώνονται με σαφήνεια και προσβασιμότητα για το ποια δεδομένα συλλέγονται, πώς χρησιμοποιούνται, ποιος τα επεξεργάζεται και για ποιο σκοπό.
2. **Αρχή του Περιορισμού του Σκοπού (Purpose Limitation):** τα δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς. Στα ενδυτά συστήματα, αυτό σημαίνει ότι τα δεδομένα που συλλέγονται για την παρακολούθηση της φυσικής κατάστασης δεν μπορούν να χρησιμοποιηθούν για διαφημιστικούς σκοπούς ή να κοινοποιηθούν σε τρίτους για σκοπούς που δεν έχουν γνωστοποιηθεί εκ των προτέρων στον χρήστη.
3. **Αρχή της Ελαχιστοποίησης Δεδομένων (Data Minimisation):** τα δεδομένα είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς που υποβάλλονται σε επεξεργασία. Η αρχή αυτή είναι ιδιαίτερα κρίσιμη για τις φορητές συσκευές, οι οποίες λόγω της συνεχούς λειτουργίας τους διατρέχουν αυξημένο κίνδυνο υπερσυλλογής δεδομένων. Οι κατασκευαστές οφείλουν να περιορίζουν τη συλλογή δεδομένων αποκλειστικά σε όσα είναι απολύτως απαραίτητα για την παροχή της υπηρεσίας.
4. **Αρχή της Ακρίβειας (Accuracy):** τα δεδομένα είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται. Πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας. Στις φορητές συσκευές, η ακρίβεια των αισθητήρων και η ορθή ερμηνεία των βιομετρικών μετρήσεων αποκτούν ιδιαίτερη σημασία, καθώς λανθασμένα δεδομένα μπορούν να οδηγήσουν σε εσφαλμένα συμπεράσματα για την υγεία των χρηστών.
5. **Αρχή του Περιορισμού της Αποθήκευσης (Storage Limitation):** τα δεδομένα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων

μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς και υπό τον όρο ότι εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων. Οι κατασκευαστές ενδυτών συσκευών οφείλουν να καθορίζουν σαφείς πολιτικές διατήρησης δεδομένων και να διαγράφουν τα δεδομένα όταν παύουν να εξυπηρετούν τον αρχικό σκοπό συλλογής τους.

6. **Αρχή της Ακεραιότητας και Εμπιστευτικότητας (Integrity and Confidentiality):** τα δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων. Στις ενδυτές συσκευές, συνεπάγεται την εφαρμογή μέτρων όπως η κρυπτογράφηση, οι έλεγχοι πρόσβασης και η ασφαλής μετάδοση δεδομένων.
7. **Αρχή της Λογοδοσίας (Accountability):** ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις παραπάνω αρχές. Η αρχή αυτή επιβάλλει στους κατασκευαστές φορητών συσκευών την τήρηση αναλυτικών αρχείων των δραστηριοτήτων επεξεργασίας και την ικανότητα τεκμηρίωσης κάθε μέτρου που λαμβάνεται για την προστασία των δεδομένων.

Πέρα από τις αρχές του Άρθρου 5, κάθε επεξεργασία πρέπει να στηρίζεται σε νόμιμη βάση. Το Άρθρο 6 ορίζει ότι η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις έξι προϋποθέσεις που συνοψίζονται στον Πίνακα 1.

Πίνακας 1: *Νομικές βάσεις επεξεργασίας σύμφωνα με το Άρθρο 6 του GDPR*

Νομική βάση	Περιγραφή
Συγκατάθεση (Consent)	Το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς.
Εκτέλεση σύμβασης (Contract)	Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο είναι συμβαλλόμενο μέρος ή για τη λήψη μέτρων κατ' αίτησή του πριν από τη σύναψη σύμβασης.
Νομική υποχρέωση (Legal obligation)	Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας.
Ζωτικά συμφέροντα (Vital interests)	Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.
Δημόσιο συμφέρον (Public task)	Η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.
Έννομο συμφέρον (Legitimate interests)	Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτου, εκτός εάν υπερισχύουν τα συμφέροντα ή τα θεμελιώδη δικαιώματα του υποκειμένου, ιδίως εάν πρόκειται για παιδί.

Ωστόσο, η πλειονότητα των ενδυτών συσκευών συλλέγει δεδομένα υγείας, για την επεξεργασία των οποίων απαιτείται κατά κανόνα ρητή συγκατάθεση (Άρθρο 9 παρ. 2 στοιχ. α). Το Άρθρο 9 του GDPR ορίζει ως «ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα» (special categories of personal data), μεταξύ άλλων, τα βιομετρικά δεδομένα που υποβάλλονται σε επεξεργασία με σκοπό τη μονοσήμαντη ταυτοποίηση φυσικού προσώπου και τα δεδομένα που αφορούν την υγεία.

5.2.3 Προστασία Δεδομένων από τον Σχεδιασμό και εξ Ορισμού

Το Άρθρο 25 του GDPR επιβάλλει δύο συμπληρωματικές υποχρεώσεις που αποσκοπούν στην ενσωμάτωση της προστασίας της ιδιωτικότητας σε όλα τα στάδια ανάπτυξης ενός συστήματος:

1. **Προστασία Δεδομένων από τον Σχεδιασμό (Data Protection by Design):** Ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.
2. **Προστασία Δεδομένων εξ Ορισμού (Data Protection by Default):** Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους.

Οι υποχρεώσεις αυτές αποκτούν ιδιαίτερη σημασία για τα ενδυτά συστήματα, καθώς η συνεχής λειτουργία τους αυξάνει τον κίνδυνο υπερσυλλογής και οι προεπιλεγμένες ρυθμίσεις πρέπει να ελαχιστοποιούν αυτόματα τη συλλογή δεδομένων και να παρέχουν επιλογές τμηματικής συγκατάθεσης.

5.2.4 Δικαιώματα των Υποκειμένων των Δεδομένων

Ο GDPR κατοχυρώνει μια σειρά δικαιωμάτων των υποκειμένων των δεδομένων, τα οποία αποκτούν ιδιαίτερη σημασία στο πλαίσιο των φορητών συσκευών:

1. **Δικαίωμα Πρόσβασης (Right of Access - Άρθρο 15):** Οι χρήστες έχουν το δικαίωμα να λαμβάνουν αντίγραφο των προσωπικών τους δεδομένων και πληροφορίες σχετικά με την επεξεργασία τους.
1. **Δικαίωμα Διόρθωσης (Right to Rectification - Άρθρο 16):** Οι χρήστες μπορούν να ζητούν τη διόρθωση ανακριβών δεδομένων υγείας ή αλγοριθμικών ερμηνειών.

1. **Δικαίωμα Διαγραφής (Right to Erasure / Right to be Forgotten - Άρθρο 17):** Οι χρήστες έχουν το δικαίωμα να ζητούν τη διαγραφή των δεδομένων τους όταν οι σκοποί έχουν εκπληρωθεί ή όταν ανακαλούν τη συγκατάθεσή τους.
1. **Δικαίωμα Φορητότητας (Right to Data Portability - Άρθρο 20):** Οι χρήστες μπορούν να λαμβάνουν τα δεδομένα τους σε δομημένη μορφή και να τα μεταφέρουν σε άλλον πάροχο.

Οι κατασκευαστές φορητών συσκευών οφείλουν να παρέχουν φιλικές προς τον χρήστη διεπαφές που να επιτρέπουν την άσκηση των δικαιωμάτων αυτών με εύκολο και προσβάσιμο τρόπο.

5.2.5 Προκλήσεις Συμμόρφωσης των Ενδυτών Συστημάτων

Η εφαρμογή των ανωτέρω αρχών και απαιτήσεων του GDPR στα ενδυτά συστήματα αντιμετωπίζει μοναδικές προκλήσεις που απορρέουν από τα ιδιαίτερα χαρακτηριστικά των συσκευών αυτών:

1. **Συνεχής λειτουργία:** Η συνεχής και αδιάλειπτη λειτουργία των ενδυτών συστημάτων αυξάνει σημαντικά τον κίνδυνο υπερσυλλογής δεδομένων και διαρροών. Σε αντίθεση με τις παραδοσιακές εφαρμογές όπου η συλλογή δεδομένων είναι στιγμιαία ή περιοδική, τα ενδυτά συστήματα καταγράφουν συνεχώς ευαίσθητες πληροφορίες για την υγεία, την τοποθεσία, τη συμπεριφορά και τις καθημερινές συνήθειες των χρηστών. Αυτή η αδιάλειπτη καταγραφή σημαίνει ότι ακόμη και αν η συγκατάθεση του χρήστη έχει ληφθεί για έναν συγκεκριμένο σκοπό, η συνεχιζόμενη ροή δεδομένων μπορεί να οδηγήσει σε δευτερογενείς χρήσεις που δεν καλύπτονται από την αρχική συναίνεση, παραβιάζοντας την αρχή του περιορισμού του σκοπού. Παράλληλα, οι χρήστες συχνά αγνοούν το πλήρες εύρος της συλλογής δεδομένων που λαμβάνει χώρα στο παρασκήνιο, γεγονός που εγείρει ζητήματα διαφάνειας.
2. **Συγκατάθεση σε πραγματικό χρόνο:** Η δυσκολία λήψης έγκυρης και ενημερωμένης συγκατάθεσης σε πραγματικό χρόνο αποτελεί μια από τις σημαντικότερες προκλήσεις. Οι περισσότεροι χρήστες καλούνται να συναινέσουν σε μια εφάπαξ διαδικασία εγκατάστασης της συσκευής ή της συνοδευτικής εφαρμογής, χωρίς να έχουν πλήρη επίγνωση του εύρους των δεδομένων που θα συλλεχθούν και του τρόπου χρήσης τους σε βάθος χρόνου. Η συνεχής λειτουργία των ενδυτών συσκευών καθιστά δύσκολη την περιοδική επανεξέταση και την ανάκληση της συγκατάθεσης, ειδικά όταν οι αλλαγές στις πολιτικές απορρήτου δεν κοινοποιούνται με σαφή και εμφανή τρόπο. Απαιτείται η εφαρμογή τμηματικής συγκατάθεσης (granular consent), με σαφείς εξηγήσεις για κάθε κατηγορία δεδομένων, η παροχή τακτικών προτροπών ανανέωσης της συγκατάθεσης και η προσφορά εύκολων επιλογών ανάκλησης, χωρίς να επηρεάζονται οι βασικές λειτουργίες της συσκευής. Ωστόσο, η υλοποίηση τέτοιων μηχανισμών σε συσκευές με περιορισμένη διεπαφή χρήστη (π.χ., μικρές οθόνες ή καθόλου οθόνη) αποτελεί πρόσθετη πρόκληση.
3. **Διασυνοριακή ροή δεδομένων:** Η διασυνοριακή ροή δεδομένων αποτελεί μια ακόμη σημαντική πρόκληση για τη συμμόρφωση με τον GDPR. Πολλές φορητές συσκευές αποθηκεύουν και επεξεργάζονται δεδομένα σε διακομιστές τρίτων παρόχων ή κατασκευαστών που βρίσκονται εκτός της Ευρωπαϊκής Ένωσης, συχνά σε χώρες με διαφορετικά ή λιγότερο αυστηρά πλαίσια προστασίας δεδομένων. Οι κατασκευαστές

οφείλουν να διασφαλίζουν ότι οι μεταφορές δεδομένων προς τρίτες χώρες συμμορφώνονται με τα Άρθρα 44–49 του GDPR, τα οποία απαιτούν την ύπαρξη κατάλληλων εγγυήσεων. Αυτό περιλαμβάνει τη χρήση Πρότυπων Συμβατικών Ρητρών (Standard Contractual Clauses – SCCs), την υιοθέτηση συμπληρωματικών μέτρων για την προστασία ευαίσθητων δεδομένων υγείας (όπως η κρυπτογράφηση από άκρο σε άκρο και οι αυστηροί έλεγχοι πρόσβασης), καθώς και τη διενέργεια αξιολογήσεων επιπτώσεων μεταφοράς (Transfer Impact Assessments – TIAs) για την αξιολόγηση του επιπέδου προστασίας στη χώρα προορισμού.

4. **Κοινοποίηση σε τρίτους:** Η κοινοποίηση δεδομένων σε τρίτους αποτελεί μια ακόμη διάσταση των προκλήσεων συμμόρφωσης. Οι τρίτοι καθίστανται από κοινού υπεύθυνοι ή εκτελούντες την επεξεργασία, και η συνεργασία μαζί τους απαιτεί σαφείς συμφωνίες επεξεργασίας δεδομένων (Data Processing Agreements – DPAs), οι οποίες καθορίζουν με ακρίβεια το αντικείμενο, τη διάρκεια, τη φύση και τον σκοπό της επεξεργασίας. Απαιτούνται επίσης αυστηροί έλεγχοι πρόσβασης μέσω API με τμηματικά δικαιώματα (granular permissions) και διαφάνεια ως προς την κοινοποίηση: οι χρήστες πρέπει να γνωρίζουν ποιες κατηγορίες δεδομένων κοινοποιούνται και σε ποιους, και να μπορούν να ελέγχουν τις κοινοποιήσεις αυτές.
5. **Ανωνυμοποίηση βιομετρικών δεδομένων:** Η ανωνυμοποίηση δεδομένων σε περιβάλλοντα πλούσιων βιομετρικών δεδομένων είναι εξαιρετικά δύσκολη, καθώς τα μοναδικά πρότυπα καρδιακών παλμών ή βηματισμού μπορούν να λειτουργήσουν ως ψηφιακά αποτυπώματα, επιτρέποντας την επαναναγνώριση ακόμη και μετά την αφαίρεση άμεσων αναγνωριστικών. Αυτό σημαίνει ότι οι παραδοσιακές τεχνικές ψευδωνυμοποίησης, που βασίζονται απλώς στην αντικατάσταση αναγνωριστικών, δεν επαρκούν για την προστασία των χρηστών. Απαιτούνται πιο προηγμένες τεχνικές, όπως η διαφορική ιδιωτικότητα (differential privacy), η ομομορφική κρυπτογράφηση ή η ομοσπονδιακή μάθηση (federated learning), οι οποίες, ωστόσο, εισάγουν σημαντικό υπολογιστικό κόστος και συχνά περιορίζουν τη χρησιμότητα των δεδομένων για ανάλυση.
6. **Περιορισμένοι πόροι συσκευών:** Η περιορισμένη υπολογιστική ισχύς και η κατανάλωση ενέργειας των wearable συσκευών αποτελούν πρόσθετους περιορισμούς στην εφαρμογή των απαιτήσεων του GDPR. Η κρυπτογράφηση, η ψευδωνυμοποίηση και άλλες τεχνικές προστασίας απαιτούν υπολογιστικούς πόρους, οι οποίοι επιβαρύνουν την μπαταρία και ενδέχεται να επηρεάσουν την απόδοση της συσκευής. Οι κατασκευαστές καλούνται να βρουν μια ισορροπία μεταξύ της ισχυρής προστασίας της ιδιωτικότητας και της πρακτικής λειτουργικότητας, χωρίς να υποβαθμίζουν την εμπειρία του χρήστη. Αυτό συχνά οδηγεί σε συμβιβασμούς, όπως η αποστολή δεδομένων στο νέφος για επεξεργασία (αυξάνοντας έτσι τους κινδύνους διασυνοριακής ροής και μη εξουσιοδοτημένης πρόσβασης), αντί της επεξεργασίας επί της συσκευής (on-device processing), η οποία θα ήταν ασφαλέστερη αλλά λιγότερο εφικτή λόγω των περιορισμένων πόρων.

Εν κατακλείδι, οι κατασκευαστές οφείλουν να αντιμετωπίζουν την ιδιωτικότητα όχι ως επιπλέον ρυθμιστικό βάρος, αλλά ως θεμελιώδες χαρακτηριστικό των προϊόντων τους, που μπορεί να αποτελέσει ανταγωνιστικό πλεονέκτημα και να ενισχύσει την εμπιστοσύνη των χρηστών. Η μη συμμόρφωση με τις ανωτέρω απαιτήσεις μπορεί να οδηγήσει σε σοβαρές κυρώσεις, συμπεριλαμβανομένων διοικητικών προστίμων έως 20 εκατομμύρια ευρώ ή έως 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών, όποιο είναι υψηλότερο (Άρθρο 83 παρ. 5).

5.3 Ο Ρόλος των Τεχνολογιών Ενίσχυσης Ιδιωτικότητας (PETs) στη Συμμόρφωση με τον GDPR

5.3.1 Η σχέση PETs και GDPR

Οι Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (Privacy Enhancing Technologies – PETs), που αναλύθηκαν στο Κεφάλαιο 4, λειτουργούν ως βασικά τεχνικά εργαλεία για την έμπρακτη υλοποίηση των νομικών απαιτήσεων του GDPR. Η σχέση μεταξύ PETs και GDPR είναι συμπληρωματική: ο Κανονισμός θέτει τις αρχές και τις υποχρεώσεις, ενώ οι PETs παρέχουν τα μέσα για την εκπλήρωσή τους. Αξιοσημείωτο είναι ότι, η ενσωμάτωση PETs από τον σχεδιασμό (Privacy by Design) δεν αποτελεί απλώς μια βέλτιστη πρακτική, αλλά μια ουσιαστική στρατηγική για τη συμμόρφωση με το Άρθρο 25 του GDPR.

Η βασική λογική είναι ότι οι PETs επιτρέπουν στους κατασκευαστές φορητών συσκευών να ανταποκριθούν στις αυστηρές απαιτήσεις του Κανονισμού, διασφαλίζοντας παράλληλα τη λειτουργικότητα, την απόδοση και τη θετική εμπειρία χρήστη. Χωρίς την εφαρμογή κατάλληλων PETs, η συμμόρφωση με αρχές όπως η ελαχιστοποίηση δεδομένων, ο περιορισμός του σκοπού και η ασφάλεια των δεδομένων καθίσταται εξαιρετικά δύσκολη, ιδιαίτερα σε περιβάλλοντα συνεχούς συλλογής ευαίσθητων βιομετρικών δεδομένων.

5.3.2 Αντιστοίχιση PETs με Απαιτήσεις του GDPR

Η αντιστοίχιση μεταξύ συγκεκριμένων PETs και των απαιτήσεων του GDPR μπορεί να αποτυπωθεί ως εξής:

α) Η Αρχή της Ελαχιστοποίησης Δεδομένων (Άρθρο 5 παρ. 1 στοιχ. γ)

Η αρχή της ελαχιστοποίησης επιτάσσει τη συλλογή μόνο των απολύτως απαραίτητων δεδομένων. Οι PETs που υποστηρίζουν την αρχή αυτή περιλαμβάνουν:

- **Ομοσπονδιακή Μάθηση (Federated Learning):** Επιτρέπει την εκπαίδευση μοντέλων μηχανικής μάθησης χρησιμοποιώντας δεδομένα που παραμένουν στις συσκευές των χρηστών, χωρίς να απαιτείται η συγκέντρωσή τους σε κεντρικές βάσεις. Αυτό μειώνει δραστικά τον όγκο των δεδομένων που αποθηκεύονται και επεξεργάζονται κεντρικά.

- **Επεξεργασία επί της συσκευής (On-device processing):** Η εκτέλεση υπολογισμών απευθείας στη φορητή συσκευή, αντί της αποστολής δεδομένων στο νέφος, περιορίζει τη συλλογή και αποθήκευση ευαίσθητων δεδομένων.
- **Αποδεικτικά Μηδενικής Γνώσης (ZKP):** Επιτρέπουν την επαλήθευση ισχυρισμών (π.χ., ότι ο χρήστης πέτυχε έναν στόχο υγείας) χωρίς να αποκαλύπτονται τα υποκείμενα δεδομένα.

β) Η Αρχή του Περιορισμού του Σκοπού (Άρθρο 5 παρ. 1 στοιχ. β)

Η αρχή αυτή απαιτεί τα δεδομένα να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς. Οι σχετικές PETs περιλαμβάνουν:

- **Ψευδωνυμοποίηση (Pseudonymization):** Η αντικατάσταση άμεσων αναγνωριστικών με ψευδώνυμα επιτρέπει την επεξεργασία δεδομένων για τον αρχικό σκοπό, χωρίς να διευκολύνεται η χρήση τους για άλλους, ασύμβατους σκοπούς.
- **Διαχείριση Συγκατάθεσης μέσω PETs:** Χρήση τεχνικών που επιτρέπουν την τμηματική συγκατάθεση (granular consent) και την εύκολη ανάκλησή της, διασφαλίζοντας ότι η επεξεργασία παραμένει εντός των ορίων που έχει καθορίσει ο χρήστης.

γ) Η Αρχή της Ακεραιότητας και Εμπιστευτικότητας – Ασφάλεια της Επεξεργασίας (Άρθρο 32)

Το Άρθρο 32 απαιτεί την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων για την ασφάλεια των δεδομένων. Οι σχετικές PETs περιλαμβάνουν:

- **Κρυπτογράφηση (Encryption):** Η κρυπτογράφηση κατά τη μετάδοση (in transit) και κατά την αποθήκευση (at rest) αποτελεί βασικό μέτρο προστασίας από μη εξουσιοδοτημένη πρόσβαση.
- **Ομομορφική Κρυπτογράφηση (Homomorphic Encryption – HE):** Επιτρέπει την εκτέλεση υπολογισμών σε κρυπτογραφημένα δεδομένα, χωρίς να απαιτείται η αποκρυπτογράφησή τους. Αυτό είναι ιδιαίτερα σημαντικό για σενάρια όπου τρίτοι πάροχοι (π.χ., υπηρεσίες νέφους) πρέπει να επεξεργαστούν ευαίσθητα δεδομένα υγείας.
- **Ασφαλής Πολυμερής Υπολογιστική (Secure Multiparty Computation – SMC):** Επιτρέπει σε πολλαπλά μέρη να υπολογίσουν από κοινού μια συνάρτηση των εισόδων τους, χωρίς να αποκαλύψουν τις εισόδους τους μεταξύ τους.

δ) Το Δικαίωμα Διαγραφής – «Δικαίωμα στη Λήθη» (Άρθρο 17)

Το δικαίωμα διαγραφής απαιτεί την ικανότητα πλήρους και μη αναστρέψιμης διαγραφής των δεδομένων. Οι σχετικές PETs και πρακτικές περιλαμβάνουν:

- **Ανωνυμοποίηση (Anonymization):** Η πλήρης και μη αναστρέψιμη αφαίρεση κάθε δυνατότητας σύνδεσης των δεδομένων με το υποκείμενό τους καθιστά τα δεδομένα μη αναγνωρίσιμα και εκτός πεδίου εφαρμογής του GDPR.

- **Ασφαλείς Μηχανισμοί Διαγραφής:** Εφαρμογή τεχνικών που διασφαλίζουν ότι τα δεδομένα διαγράφονται πλήρως από όλα τα συστήματα (συσκευή, εφαρμογή, διακομιστές νέφους, αντίγραφα ασφαλείας).

ε) Η Αρχή της Διαφάνειας (Άρθρα 13–14)

Η διαφάνεια απαιτεί σαφή ενημέρωση των χρηστών. Οι σχετικές PETs περιλαμβάνουν:

- **Αποδεικτικά Μηδενικής Γνώσης (ZKP):** Επιτρέπουν την απόδειξη συμμόρφωσης με τους όρους χρήσης ή τις πολιτικές απορρήτου, χωρίς να αποκαλύπτονται ευαίσθητες λεπτομέρειες της επεξεργασίας.

5.3.3 Η Ανάλυση Αντικτύπου για την Ιδιωτικότητα (PIA) ως Εργαλείο Συμμόρφωσης

Πέρα από τις τεχνικές PETs, η συμμόρφωση με τον GDPR απαιτεί και τη διενέργεια Ανάλυσης Αντικτύπου για την Ιδιωτικότητα (Privacy Impact Assessment – PIA), όπως αυτή θεσπίζεται στο Άρθρο 35 του Κανονισμού. Η PIA αποτελεί μια δομημένη διαδικασία αξιολόγησης των κινδύνων που μπορεί να προκύψουν από την επεξεργασία προσωπικών δεδομένων, ιδιαίτερα όταν πρόκειται για ευαίσθητα δεδομένα υγείας, όπως αυτά που διαχειρίζονται τα ενδυτά συστήματα.

Η μεθοδολογία PIA της CNIL, η οποία αποτελεί σημείο αναφοράς για την εφαρμογή του Άρθρου 35, βασίζεται σε τρεις πυλώνες: (α) τις βάσεις γνώσεων (τυπολογίες δεδομένων, κλίμακες κινδύνου), (β) τον κατάλογο μέτρων προστασίας (κρυπτογράφηση, ανωνυμοποίηση, έλεγχοι πρόσβασης) και (γ) το λογισμικό ανοικτού κώδικα που καθοδηγεί τους υπεύθυνους επεξεργασίας βήμα προς βήμα. Η εφαρμογή της σε ένα ενδυτό σύστημα περιλαμβάνει: (1) περιγραφή της επεξεργασίας, (2) αξιολόγηση αναγκαιότητας και αναλογικότητας, (3) αναγνώριση και αξιολόγηση κινδύνων, (4) προσδιορισμό μέτρων μετριασμού και (5) τεκμηρίωση και αναθεώρηση.

Η PIA συνιστά ένα ζωτικό εργαλείο για την προληπτική διαχείριση των κινδύνων ιδιωτικότητας και την αποδεδειγμένη συμμόρφωση με τον GDPR, και θα πρέπει να διενεργείται πριν από την έναρξη οποιασδήποτε επεξεργασίας υψηλού κινδύνου.

5.4 Συμπεράσματα

Το παρόν κεφάλαιο ανέδειξε την κρισιμότητα του νομικού και κανονιστικού πλαισίου για την προστασία της ιδιωτικότητας στα ενδυτά συστήματα. Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) θέτει αυστηρές απαιτήσεις για τη συλλογή, επεξεργασία και αποθήκευση προσωπικών δεδομένων, με τις ειδικές κατηγορίες δεδομένων υγείας (Άρθρο 9) να απολαμβάνουν το υψηλότερο επίπεδο προστασίας. Τα ενδυτά συστήματα, λόγω της συνεχούς λειτουργίας τους και της φύσης των δεδομένων που συλλέγουν, εμπίπτουν σε αυτές τις αυστηρές ρυθμίσεις, απαιτώντας από τους κατασκευαστές και τους παρόχους υπηρεσιών να υιοθετούν ολοκληρωμένες στρατηγικές συμμόρφωσης.

Τέλος, οι Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (PETs) που αναλύθηκαν στο Κεφάλαιο 4 αποτελούν τα βασικά τεχνικά εργαλεία για την επίτευξη της συμμόρφωσης αυτής. Οι τεχνικές δεν

αποτελούν μόνο μέτρα προστασίας της ιδιωτικότητας αλλά διευκολύνουν τη συμμόρφωση με τις νομικές απαιτήσεις. Η ενσωμάτωσή τους από το στάδιο του σχεδιασμού, σύμφωνα με την αρχή του Privacy by Design, αποτελεί την πλέον ενδεδειγμένη πρακτική.

6 *Μελέτη Περίπτωσης: Έξυπνο Δαχτυλίδι – Ανάλυση και Προτάσεις*

6.1 Εισαγωγή

Στο παρόν κεφάλαιο, η θεωρητική ανάλυση των προηγούμενων κεφαλαίων θα εφαρμοστεί σε ένα ένδυτο σύστημα. Σκοπός είναι η ανάδειξη των απειλών ιδιωτικότητας μέσω της μεθοδολογίας LINDDUN, η πρόταση εξατομικευμένων μέτρων μετριασμού με βάση τις Τεχνολογίες Ενίσχυσης Ιδιωτικότητας και η αξιολόγηση της αποτελεσματικότητάς τους σε σχέση με τις απαιτήσεις του GDPR. Το κεφάλαιο οργανώνεται ως εξής: αρχικά περιγράφεται το υπό μελέτη σύστημα, στη συνέχεια παρουσιάζεται και εφαρμόζεται η μεθοδολογία LINDDUN για την ανάδειξη απειλών, ακολουθούν οι προτάσεις μέτρων προστασίας και τέλος συζητούνται τα αποτελέσματα και οι περιορισμοί της ανάλυσης.

Το ένδυτο σύστημα που τίθεται υπό ανάλυση είναι το έξυπνο δαχτυλίδι (smart ring), το οποίο αποτελεί μία από τις πιο πρόσφατες καινοτομίες στον τομέα των συσκευών παρακολούθησης της υγείας, με δυνατότητα καταγραφής δεδομένων σχετικά με τη φυσική κατάσταση, την υγεία και τον ύπνο. Παρά την αυξανόμενη δημοτικότητα των συσκευών αυτών, η επιστημονική έρευνα σχετικά με τις επιπτώσεις τους στην ασφάλεια και την ιδιωτικότητα παραμένει περιορισμένη.

6.2 Περιγραφή του Έξυπνου Δαχτυλιδιού

Τα έξυπνα δαχτυλίδια ανήκουν στην κατηγορία των ενδυτών συστημάτων· φοριούνται στο δάχτυλο και τα δεδομένα που συλλέγουν οι αισθητήρες τους μεταδίδονται μέσω Bluetooth Low Energy (BLE). Τα κύρια πλεονεκτήματά τους σε σύγκριση με άλλες συσκευές παρόμοιων εφαρμογών (π.χ. smartwatches) είναι ο διακριτικός χαρακτήρας και η ευχρηστία τους. Τα πιο διαδεδομένα μοντέλα στην αγορά είναι τα Oura Ring 4, Ultrahuman Ring AIR, RingConn Gen 2 και Samsung Galaxy Ring.

Τα δαχτυλίδια ενσωματώνουν πολλαπλούς αισθητήρες για τη συνεχή παρακολούθηση βιομετρικών και βιοχημικών παραμέτρων. Οι αισθητήρες που συγκαταλέγονται είναι οι εξής:

- **Οπτικός αισθητήρας φωτοπληθυσμογραφίας (PPG):** Χρήση πηγών πράσινου φωτός (μήκος κύματος 520 nm) και κόκκινου φωτός για τη μέτρηση του καρδιακού ρυθμού και της μεταβλητότητας καρδιακών παλμών (HRV).
- **Αισθητήρας οξυγόνου αίματος (SpO_2):** Μέτρηση του κορεσμού οξυγόνου στο αίμα.
- **Αισθητήρας θερμοκρασίας δέρματος:** Παρακολούθηση της θερμοκρασίας του σώματος με ακρίβεια ±0,1°C.
- **Επιταχυνσιόμετρο τριών αξόνων:** Ανίχνευση κίνησης, βημάτων και σωματικής δραστηριότητας.
- **Αισθητήρας βιοχημικών δεικτών (σε προηγμένα μοντέλα):** Μέτρηση γλυκόζης, κετονών, ασκορβικού οξέος, ουρικού οξέος, γαλακτικού οξέος και αλκοόλης από δείκτες του ιδρώτα.

Τα έξυπνα δαχτυλίδια μπορούν να παρακολουθούν σε πραγματικό χρόνο μια ποικιλία δεικτών υγείας. Τα δεδομένα που συλλέγουν σε καθημερινή βάση αφορούν:

- **Βιομετρικά δεδομένα:** Κορεσμός οξυγόνου (SpO2), καρδιακός ρυθμός (HR), θερμοκρασία δέρματος, αναπνευστικός ρυθμός και το επίπεδα άγχους.
- **Δεδομένα ύπνου:** Ποιότητα ύπνου (SQ), στάδια και η διάρκεια αυτού.
- **Δεδομένα δραστηριότητας:** Επίπεδο σωματικής δραστηριότητας και θερμιδική κατανάλωση..
- **Δεδομένα τοποθεσίας:** Συγχρονισμός δεδομένων GPS μέσω του κινητού τηλεφώνου.
- **Δεδομένα κύκλου (για γυναίκες χρήστες):** Παρακολούθηση έμμηνου κύκλου, πρόβλεψη ωορρηξίας και δεδομένα γονιμότητας.

Ο Πίνακας 2 συνοψίζει τα χαρακτηριστικά των μοντέλων έξυπνων δαχτυλιδιών που κατέχουν ηγετική θέση στην αγορά: τα δεδομένα που συλλέγει κάθε μοντέλο, την έκδοση Bluetooth Low Energy (BLE), τους αισθητήρες που χρησιμοποιούνται και τη δυνατότητα ανέπαφων πληρωμών.

Πίνακας 2: *Σύγκριση των δημοφιλέστερων μοντέλων έξυπνων δαχτυλιδιών*

Μοντέλο Δαχτυλιδιού	Δεδομένα που Συλλέγει	BLE έκδοση	Αισθητήρες	Ανέπαφη Πληρωμή
Oura Ring 4	Καρδιακός ρυθμός, HRV, σωματική θερμοκρασία, στάδια ύπνου, δραστηριότητα, SpO2 (επίπεδα οξυγόνου στο αίμα)	4.0	Πράσινο, Κόκκινο, Υπέρυθρο LED, Επιταχυνσιόμετρο, Ψηφιακός αισθητήρας	Όχι
Samsung Galaxy Ring	Καρδιακός ρυθμός, παρακολούθηση ύπνου, SpO2, επίπεδα άγχους, παρακολούθηση δραστηριότητας	5.4	Επιταχυνσιόμετρο, Βιοσήμα, Θερμοκρασία	Ναι
Ultrahuman Ring Air	Καρδιακός ρυθμός, θερμοκρασία σώματος, στάδια ύπνου, δραστηριότητα, μεταβολικός ρυθμός	5.0	PPG, Βιοσήμα, Θερμοκρασία, Κίνηση	Όχι
RingConn Gen 2	Καρδιακός ρυθμός, οξυγόνο στο αίμα (SpO2), παρακολούθηση ύπνου, θερμοκρασία σώματος, στρες	5.2	PPG, Θερμοκρασία, Κίνηση	Όχι

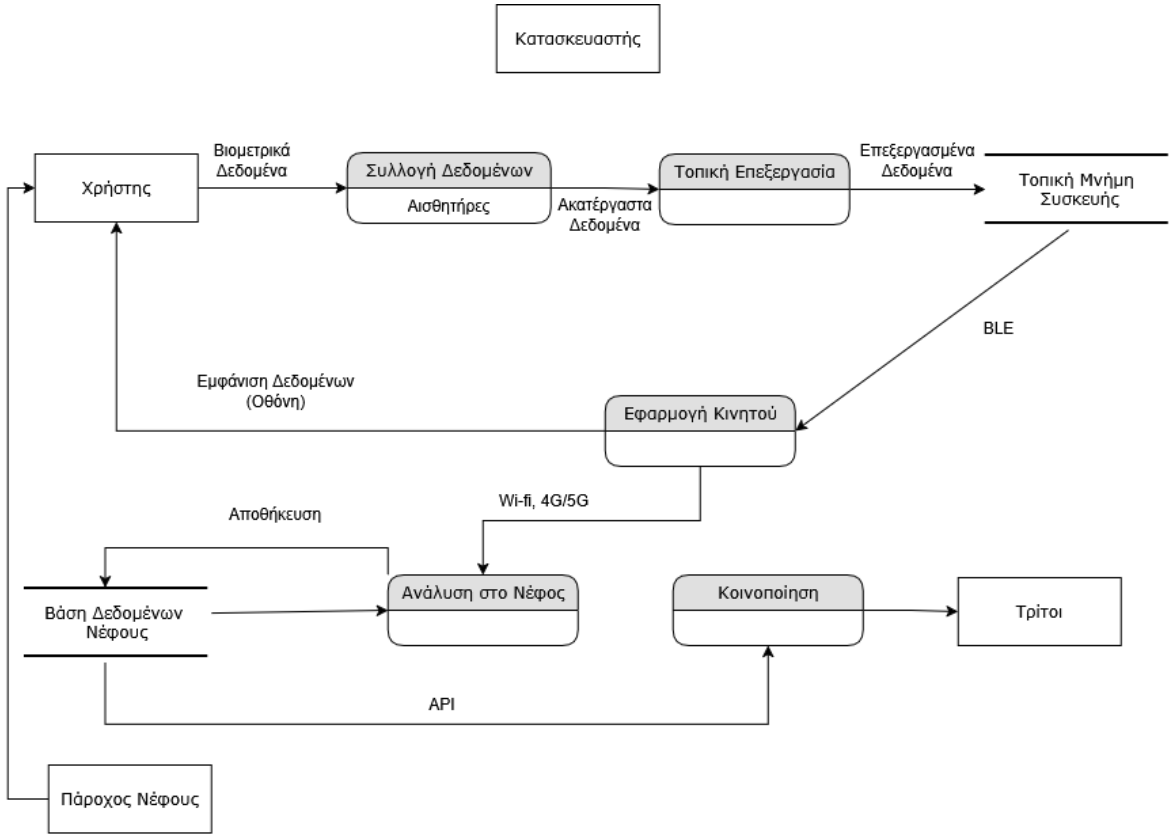
Η ροή των πληροφοριών μέσα στο σύστημα ακολουθεί την εξής διαδρομή:

1. **Συσκευή → Εφαρμογή Κινητού:** Τα δεδομένα μεταδίδονται τοπικά από το δαχτυλίδι στην εφαρμογή του κινητού μέσω Bluetooth Low Energy (BLE). Το BLE αποτελεί το κύριο πρωτόκολλο επικοινωνίας για τα έξυπνα δαχτυλίδια, λόγω της χαμηλής κατανάλωσης ενέργειας.
2. **Εφαρμογή → Νέφος Κατασκευαστή:** Η εφαρμογή συγχρονίζει περιοδικά τα δεδομένα με τους διακομιστές του κατασκευαστή στο νέφος. Η σύνδεση στο νέφος είναι υποχρεωτική για τη λειτουργία του προϊόντος, καθώς τα δεδομένα αποθηκεύονται και αναλύονται κεντρικά.
3. **Νέφος → Τρίτοι:** Τα δεδομένα ενδέχεται να κοινοποιηθούν σε τρίτους φορείς μέσω APIs, όπως:
    - Υποεπεξεργαστές cloud (π.χ., Snowflake).
    - Πλατφόρμες κοινωνικών δικτύων (π.χ., Facebook) για σκοπούς διαφήμισης.
    - Κυβερνητικούς φορείς (π.χ., Υπουργείο Άμυνας ΗΠΑ) σε περιπτώσεις ειδικών συνεργασιών.
    - Ερευνητικά κέντρα σε περιπτώσεις συμμετοχής σε επιστημονικές μελέτες.

Τα εμπλεκόμενα μέρη του συστήματος είναι:

- **Χρήστης:** Το φυσικό πρόσωπο που φοράει τη συσκευή.
- **Κατασκευαστής:** Η εταιρεία που παράγει και διαχειρίζεται το δαχτυλίδι και την εφαρμογή.
- **Πάροχος Υπηρεσιών Νέφους:** Υποδομή αποθήκευσης και επεξεργασίας δεδομένων.
- **Τρίτοι Συνεργάτες:** Διαφημιστικές πλατφόρμες, ασφαλιστικές εταιρείες, ερευνητικοί φορείς, κυβερνητικές υπηρεσίες.

Για την οπτικοποίηση της ροής των δεδομένων, των δεδομένων εισόδου και εξόδου, καθώς και των αποθηκών και των διεργασιών που μετασχηματίζουν τα δεδομένα, καταρτίστηκε με βάση την παραπάνω ανάλυση το Διάγραμμα Ροής Δεδομένων (DFD) του Σχήματος 1.



Σχήμα 1: *Διάγραμμα Ροής Δεδομένων (DFD) Επιπέδου 1 για το σύστημα του έξυπνου δαχτυλιδιού*

Στο Διάγραμμα Ροής Δεδομένων Επιπέδου 1 διακρίνονται τέσσερις εξωτερικές οντότητες (Χρήστης, Κατασκευαστής, Πάροχος Νέφους, Τρίτοι), πέντε διεργασίες (Συλλογή, Τοπική Επεξεργασία, Εφαρμογή Κινητού, Ανάλυση Νέφους, Κοινοποίηση σε Τρίτους) και δύο αποθήκες δεδομένων (Τοπική Μνήμη, Βάση Νέφους). Οι ροές δεδομένων περιλαμβάνουν τη μετάδοση βιομετρικών δεδομένων μέσω BLE από τη συσκευή στην εφαρμογή, τον συγχρονισμό με το νέφος μέσω Wi-Fi και την κοινοποίηση σε τρίτους μέσω API.

6.3 Ανάλυση Απειλών με τη Μεθοδολογία LINDDUN

6.3.1 Η Μεθοδολογία LINDDUN

Η μεθοδολογία LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance) αποτελεί ένα ολοκληρωμένο πλαίσιο μοντελοποίησης απειλών (threat modeling) για την αξιολόγηση των απειλών κατά της ιδιωτικότητας. Αναπτύχθηκε αρχικά στο KU Leuven το 2010 και έκτοτε έχει αποκτήσει ευρεία αναγνώριση, καθώς προτείνεται από φορείς όπως ο ENISA.

Στα περισσότερα λογισμικά συστήματα εντοπίζονται κενά προστασίας της ιδιωτικότητας, τα οποία πρέπει να αντιμετωπιστούν ήδη από τη φάση του σχεδιασμού. Ως απάντηση στο ζήτημα αυτό, το πλαίσιο LINDDUN αντιστοιχίζει σε κάθε απειλή κατά της ιδιωτικότητας μια κατάλληλη στρατηγική μετριασμού και τη συνδέει με συγκεκριμένες τεχνικές λύσεις.

Η μέθοδος LINDDUN εφαρμόστηκε με επιτυχία σε επιχειρηματικό πλαίσιο από εταιρείες και οργανισμούς στους τομείς της αυτοκινητοβιομηχανίας, της υγειονομικής περίθαλψης, της δημόσιας διοίκησης κ.ά. Σύμφωνα με πρόσφατη μελέτη (2022), η μεθοδολογία LINDDUN συγκαταλέγεται μεταξύ των δύο πιο γνωστών στον κλάδο από τους επαγγελματίες της πληροφορικής στον τομέα των απαιτήσεων, καθώς και μεταξύ των δέκα πιο χρησιμοποιούμενων στη βιβλιογραφία.

Το όνομά της αποτελεί ακρωνύμιο των επτά κατηγοριών απειλών που πραγματεύεται:

- Linkability (Συνδεσιμότητα): απόκτηση περισσότερων πληροφοριών για ένα άτομο ή μια ομάδα μέσω της συσχέτισης στοιχείων δεδομένων ή ενεργειών χρηστών.
- Identifiability (Αναγνωρισιμότητα): αναγνώριση της ταυτότητας ενός ατόμου.
- Non-repudiation (Μη-Απάρνηση): η δυνατότητα απόδοσης ενός ισχυρισμού (δηλαδή της γνώσης ότι κάποιος έκανε ή είπε κάτι) σε ένα συγκεκριμένο άτομο, αυτό οδηγεί στην απώλεια της «εύλογης άρνησης» (plausible deniability).
- Detectability (Ανιχνευσιμότητα): η δυνατότητα ανίχνευσης της εμπλοκής ενός ατόμου μέσω παρατήρησης.
- Disclosure of information (Αποκάλυψη Πληροφοριών): οι περιπτώσεις στις οποίες η αποκάλυψη προσωπικών δεδομένων προς, εντός και από το σύστημα θεωρείται προβληματική.
- Unawareness (Έλλειψη Ενημέρωσης): η ανεπαρκής ενημέρωση και συμμετοχή των ατόμων όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων.
- Non-compliance (Μη-Συμμόρφωση): το σύστημα αποκλίνει από τις βέλτιστες πρακτικές, τα πρότυπα και τη νομοθεσία σχετικά με την ασφάλεια και τη διαχείριση δεδομένων, με αποτέλεσμα την ελλιπή διαχείριση των κινδύνων.

6.3.2 Τα Βήματα της Μεθοδολογίας

Η εφαρμογή της μεθοδολογίας LINDDUN ακολουθεί μια συστηματική διαδικασία τριών βασικών βημάτων:

Βήμα 1: Μοντελοποίηση του Συστήματος (System Modeling): Καταρτίζεται το Διάγραμμα Ροής Δεδομένων (DFD), το οποίο απεικονίζει τις εξωτερικές οντότητες, τις διεργασίες, τις αποθήκες δεδομένων και τις ροές δεδομένων του συστήματος. Το DFD για το έξυπνο δαχτυλίδι παρουσιάζεται στο Σχήμα 1 (Ενότητα 6.2).

Βήμα 2: Ανάδειξη Απειλών (Threat Elicitation): Για κάθε στοιχείο του DFD εξετάζονται συστηματικά οι επτά κατηγορίες LINDDUN, με τη χρήση καταλόγου δέντρων απειλών (threat trees) που παρέχει η μεθοδολογία. Στόχος είναι ο εντοπισμός συγκεκριμένων απειλών για το υπό ανάλυση σύστημα. Η ανάδειξη των απειλών για το έξυπνο δαχτυλίδι παρουσιάζεται στην Ενότητα 6.3.3.

Βήμα 3: Διαχείριση Απειλών (Threat Management): Οι απειλές που αναδείχθηκαν αξιολογούνται ως προς την πιθανότητα εμφάνισης και τη σοβαρότητα της επίπτωσής τους, ιεραρχούνται βάσει υπολογιζόμενου βαθμού κινδύνου (Risk Score) και για κάθε μία προτείνονται

κατάλληλα μέτρα μετριασμού, κυρίως μέσω Τεχνολογιών Ενίσχυσης Ιδιωτικότητας (PETs). Η ιεράρχηση και οι προτάσεις μέτρων παρουσιάζονται στις Ενότητες 6.3.4 και 6.4 & 6.5 αντίστοιχα.

6.3.3 Εφαρμογή της Μεθοδολογίας LINDDUN στο έξυπνο δαχτυλίδι

Πριν από την ανάλυση των απειλών με τη μεθοδολογία LINDDUN, κρίνεται σκόπιμο να αναφερθούν ορισμένες ευπάθειες ασφαλείας που έχουν εντοπιστεί στα πιο διαδεδομένα εμπορικά μοντέλα έξυπνων δαχτυλιδιών:

1. **Επικοινωνία σε μη κρυπτογραφημένη μορφή (Cleartext):** Μετάδοση ευαίσθητων βιομετρικών δεδομένων χωρίς χρήση πρωτοκόλλων κρυπτογράφηση.
2. **Μη αυθεντικοποιημένες ενημερώσεις λογισμικού (Firmware):** Δυνατότητα εγκατάστασης κακόβουλου λογισμικού λόγω απουσίας μηχανισμών επαλήθευσης ταυτότητας.
3. **Έλλειψη ενημερωμένης συγκατάθεσης χρήστη:** Παραβίαση της αρχής της ενημερωμένης συγκατάθεσης κατά τη συλλογή και επεξεργασία των δεδομένων.
4. **Περιορισμένη διεπαφή χρήστη (User Interface):** Τα δαχτυλίδια δεν διαθέτουν οθόνη, περιορίζοντας τον έλεγχο του χρήστη και αυξάνοντας τον κίνδυνο μη ανιχνευμένων ευπαθειών.
5. **Ευπάθειες πρωτοκόλλου BLE:** Μη αυθεντικοποιημένη πρόσβαση μέσω Bluetooth Low Energy, επιτρέποντας σε κοντινούς επιτιθέμενους να συνδεθούν στη συσκευή χωρίς προηγούμενη ζεύξη.

Αντιπροσωπευτικό περιστατικό είναι η παραβίαση δεδομένων της Ultrahuman (Μάρτιος 2026), κατά την οποία μη εξουσιοδοτημένα πρόσωπα απέκτησαν πρόσβαση σε δεδομένα ευεξίας περίπου 700 χρηστών μέσω κλοπής διαπιστευτηρίων υπαλλήλου. Η επίθεση στόχευσε το εσωτερικό σύστημα ανάλυσης δεδομένων (analytics) και όχι τα ίδια τα δαχτυλίδια, αναδεικνύοντας την ευπάθεια του υποστηρικτικού συστήματος νέφους (cloud backend).

Με βάση τις γνωστές ευπάθειες των συστημάτων της αγοράς και το διάγραμμα ροής δεδομένων, αναδεικνύονται οι ακόλουθες απειλές ανά κατηγορία του πλαισίου LINDDUN.

Linkability (Συνδεσιμότητα)

Ο συνδυασμός και η σύνδεση δεδομένων από διαφορετικές πηγές μπορεί να αποκαλύψει πληροφορίες που δεν είναι προφανείς από μεμονωμένα σύνολα δεδομένων. Αναφορικά με τα έξυπνα δαχτυλίδια:

- Η σύνδεση δεδομένων καρδιακών παλμών με δεδομένα τοποθεσίας μπορεί να αποκαλύψει αν ο χρήστης αντιμετωπίζει προβλήματα υγείας και επισκέπτεται τακτικά καρδιολογικό ιατρείο. Παρόμοια σύνδεση δεδομένων μπορεί να υλοποιηθεί και για τα υπόλοιπα βιομετρικά δεδομένα που συλλέγει.

- Η σύνδεση δεδομένων τοποθεσίας με δεδομένα επιπέδου άγχους μπορεί να αποκαλύψει πληροφορίες για τη θέση του ατόμου στον χώρο εργασίας του ή για τις συνθήκες εργασίας, ιδίως αν συνδυαστούν δεδομένα πολλών χρηστών.
- Η σύνδεση δεδομένων κύκλου (για γυναίκες χρήστες) με δεδομένα δραστηριότητας μπορεί να αποκαλύψει εγκυμοσύνη ή άλλες αναπαραγωγικές καταστάσεις.

Identifiability (Αναγνωρισιμότητα)

Η αναγνώριση ενός ατόμου μέσω ενός έξυπνου δαχτυλιδιού μπορεί να προκύψει από τα βιομετρικά δεδομένα που αυτό συλλέγει, και συγκεκριμένα από:

- το μοναδικό πρότυπο μεταβλητότητας καρδιακών παλμών (HRV) του χρήστη, ακόμη και σε ψευδωνυμοποιημένα δεδομένα, λειτουργεί ως βιομετρικό αποτύπωμα·
- το μοναδικό μοτίβο βηματισμού και κίνησης, μέσω ανάλυσης των δεδομένων του επιταχυνσιόμετρου·
- τη θερμοκρασία του δέρματος και τον αναπνευστικό ρυθμό, που παρουσιάζουν ατομικές διακυμάνσεις που επιτρέπουν τη διαφοροποίηση του χρήστη από άλλα άτομα.

Non-repudiation (Μη-Απάρνηση)

Τα δεδομένα που συλλέγει το δαχτυλίδι μπορούν να χρησιμοποιηθούν για να αμφισβητήσουν ή να επιβεβαιώσουν ισχυρισμούς του χρήστη:

- Σε εργασιακό πλαίσιο, τα δεδομένα ύπνου και δραστηριότητας μπορούν να χρησιμοποιηθούν για την αξιολόγηση της παραγωγικότητας ή της ετοιμότητας του εργαζομένου.
- Σε ασφαλιστικό πλαίσιο, τα δεδομένα παρακολούθησης της υγείας μπορούν να συμβάλλουν στην καλύτερη κατανόηση των προσωπικών θεμάτων υγείας ενός ατόμου, τα οποία μπορούν να χρησιμοποιηθούν εναντίον του ίδιου ατόμου σε ασφαλιστικές αιτήσεις ή νομικές κατηγορίες.

Detectability (Ανιχνευσιμότητα)

Αφορά την ικανότητα ενός τρίτου να ανιχνεύσει ότι το άτομο φοράει τη συσκευή, λόγω της συνεχούς εκπομπής σημάτων BLE από το δαχτυλίδι. Πιο συγκεκριμένα:

- **Μη αυθεντικοποιημένη σύνδεση BLE:** Ευπάθειες όπως το CVE-2026-89034 (TCH QRing R20_B006) επιτρέπουν σε κοντινούς επιτιθέμενους να συνδεθούν στη συσκευή χωρίς τη διαδικασία ζεύξης.
- **Ανίχνευση παρουσίας:** Η συνεχής εκπομπή σημάτων BLE μπορεί να χρησιμοποιηθεί για την ανίχνευση της φυσικής παρουσίας του χρήστη σε συγκεκριμένους χώρους.

Disclosure of Information (Αποκάλυψη Πληροφοριών)

Η διαρροή ευαίσθητων ιατρικών δεδομένων αποτελεί σημαντική απειλή:

- **Περιστατικά παραβίασης νέφους:** Η διαρροή στην Ultrahuman (2026) απέδειξε τον κίνδυνο αποκάλυψης δεδομένων ευεξίας, ιστορικού συναλλαγών και στοιχείων επικοινωνίας (Ultrahuman - 700 χρήστες).
- **Επικοινωνία σε cleartext:** Αποστολή ευαίσθητων δεδομένων χωρίς κρυπτογράφηση, εκθέτει τις επικοινωνίες σε επιθέσεις υποκλοπής.
- **Κοινοποίηση σε τρίτους:** Αποστολή δεδομένων σε πλατφόρμες όπως το Facebook για διαφημιστικούς σκοπούς.
- **Ενσωμάτωση SDK τρίτων:** Η χρήση ενσωματωμένων πακέτων ανάπτυξης λογισμικού (third-party SDKs) στην εφαρμογή κινητού για σκοπούς ανάλυσης συμπεριφοράς (analytics), παρακολούθησης (tracking) ή διαφήμισης, τα οποία ενδέχεται να συλλέγουν και να μεταδίδουν αυτόματα βιομετρικά δεδομένα και στοιχεία ταυτοποίησης σε εξωτερικούς παρόχους.

Unawareness (Έλλειψη Ενημέρωσης)

Οι χρήστες συχνά δεν γνωρίζουν την έκταση της επεξεργασίας των δεδομένων τους, λόγω περιορισμένης ή ανεπαρκούς ενημέρωσης:

- **Διεθνής μεταφορά δεδομένων:** Πολιτικές απορρήτου, όπως της Ultrahuman, αναφέρουν ότι τα δεδομένα μπορούν να μεταφερθούν και να αποθηκευτούν σε οποιαδήποτε χώρα, συμπεριλαμβανομένων των ΗΠΑ, και ότι η χρήση του προϊόντος συνεπάγεται συγκατάθεση σε αυτό.
- **Κοινοποίηση σε τρίτους:** Οι χρήστες συχνά δεν γνωρίζουν ότι τα δεδομένα τους κοινοποιούνται σε ασφαλιστικές εταιρείες ή ερευνητικούς φορείς.
- **Συνεργασία με κυβερνητικούς φορείς:** Συνεργασίες όπως της Oura με το Υπουργείο Άμυνας των ΗΠΑ έχουν προκαλέσει ανησυχίες στους χρήστες, παρά τις διαβεβαιώσεις της εταιρείας ότι τα δεδομένα δεν κοινοποιούνται χωρίς ρητή συγκατάθεση.

Non-compliance (Μη-Συμμόρφωση)

Το σύστημα ενδέχεται να μην τηρεί βέλτιστες πρακτικές ασφάλειας και διαχείρισης δεδομένων, με αποτέλεσμα παραβιάσεις του GDPR όπως οι εξής:

- **Έλλειψη ρητής συγκατάθεσης (Άρθρο 9):** Τα δεδομένα υγείας απαιτούν ρητή συγκατάθεση, η οποία συχνά λαμβάνεται μέσω εκτενών όρων χρήσης που οι χρήστες δεν διαβάζουν.
- **Παραβίαση της αρχής της ελαχιστοποίησης (Άρθρο 5 παρ. 1 στοιχ. γ):** Συλλογή περισσότερων δεδομένων από τα απαραίτητα, για τον δηλωθέντα σκοπό επεξεργασίας. .
- **Διεθνής μεταφορά δεδομένων (Άρθρα 44–49):** Μεταφορά δεδομένων σε χώρες εκτός ΕΕ χωρίς επαρκείς εγγυήσεις.
- **Έλλειψη διαφάνειας (Άρθρα 13–14):** Οι πολιτικές απορρήτου είναι δυσνόητες και δεν εξηγούν σαφώς τη χρήση των δεδομένων.

6.3.4 Ιεράρχηση Απειλών

Η αξιολόγηση της επικινδυνότητας των απειλών LINDDUN για τα έξυπνα δαχτυλίδια βασίζεται στην Πιθανότητα (Likelihood, κλίμακα 1–5) εκδήλωσης κάθε απειλής και στην Επίπτωση (Impact, κλίμακα 1–5) που αυτή έχει στα προσωπικά δεδομένα και στην ιδιωτικότητα του χρήστη. Ο βαθμός κινδύνου υπολογίζεται ως εξής:

$$Risk\ Score = Likelihood \times Impact$$

Τα κριτήρια αξιολόγησης είναι ποιοτικά και συνυπολογίζουν τα τεχνικά χαρακτηριστικά των συσκευών, τα γνωστά κενά ασφαλείας και τα πραγματικά περιστατικά της αγοράς. Ενδεικτικά, η τεκμηρίωση της επικινδυνότητας για την κορυφαία απειλή **Disclosure of Information** (Risk Score = 25) προέκυψε από την ακόλουθη ανάλυση:

- **Πιθανότητα (Likelihood = 5 / Σχεδόν Βέβαιο):** Η εκδήλωση της απειλής θεωρείται εξαιρετικά πιθανή λόγω των πολλαπλών σημείων έκθεσης του συστήματος (όπως η μετάδοση δεδομένων σε cleartext μέσω BLE, οι ευπάθειες στις υποδομές cloud και η ενσωματωση SDKs τρίτων), σε συνδυασμό με την ύπαρξη πραγματικών, καταγεγραμμένων περιστατικών στην αγορά (π.χ. παραβίαση δεδομένων στην Ultrahuman).
- **Επίπτωση (Impact = 5 / Καταστροφικό):** Η διαρροή αφορά ευαίσθητα προσωπικά και βιομετρικά δεδομένα υγείας, των οποίων η έκθεση σε μη εξουσιοδοτημένα τρίτα μέρη έχει μόνιμο και **μη αναστρέψιμο χαρακτήρα** (καθώς τα δεδομένα που έχουν ήδη διαρρεύσει στο νέφος ή σε εξωτερικούς συνεργάτες δεν μπορούν να ανακληθούν ή να διαγραφούν οριστικά).

Αντίστοιχη μεθοδολογική προσέγγιση και ανάλυση κινδύνου ακολουθήθηκε για τις υπόλοιπες κατηγορίες LINDDUN, τα αποτελέσματα της αξιολόγησης παρουσιάζονται στον Πίνακα 3, ταξινομημένα κατά φθίνουσα σειρά κινδύνου.

Πίνακας 3: *Πίνακας αξιολόγησης κινδύνου (Risk Assessment Matrix) για τις απειλές LINDDUN του έξυπνου δαχτυλιδιού*

Απειλή LINDDUN	Πιθανότητα (1-5)	Επίπτωση (1-5)	Risk Score	Επίπεδο Κινδύνου	Περιγραφή
Disclosure of Information	5	5	25	Κρίσιμος	Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα υγείας (π.χ., Ultrahuman breach) ή υποκλοπή μέσω ανασφαλούς BLE.
Non-compliance	5	4	20	Κρίσιμος	Έλλειψη ρητής συγκατάθεσης (Άρθρο 9) ή παράνομη διεθνής μεταφορά δεδομένων (Άρθρα 44–49) σε χώρες εκτός ΕΕ.
Linkability	4	4	16	Υψηλός	Σύνδεση δεδομένων υγείας με τοποθεσία για δημιουργία προφίλ

Απειλή LINDDUN	Πιθανότητα (1-5)	Επίπτωση (1-5)	Risk Score	Επίπεδο Κινδύνου	Περιγραφή
Identifiability	3	5	15	Υψηλός	Αναγνώριση χρήστη από μοναδικά πρότυπα HRV ή βηματισμού ακόμη και σε ψευδωνυμοποιημένα δεδομένα.
Unawareness	5	3	15	Υψηλός	Άγνοια χρήστη για κοινοποίηση δεδομένων σε τρίτους ή για αλλαγές στην πολιτική απορρήτου.
Detectability	3	3	9	Μέτριος	Ανίχνευση φυσικής παρουσίας χρήστη μέσω συνεχούς εκπομπής σημάτων BLE
Non-repudiation	2	4	8	Μέτριος	Χρήση δεδομένων για αμφισβήτηση ισχυρισμών σε ασφαλιστικό ή εργασιακό πλαίσιο.

Οι κλίμακες αξιολόγησης που χρησιμοποιήθηκαν είναι οι εξής:

Κλίμακα Πιθανότητας (1–5)

1. Σπάνιο (Rare)
2. Απίθανο (Unlikely)
3. Δυνατό (Possible)
4. Πιθανό (Likely)
5. Σχεδόν Βέβαιο (Almost Certain)

Κλίμακα Επίπτωσης (1–5)

1. Αμελητέο (Negligible)
2. Μικρό (Minor)
3. Μέτριο (Moderate)
4. Σοβαρό (Major)
5. Καταστροφικό (Catastrophic)

Βαθμός κινδύνου (Risk Score) – Καθορισμός επιπέδου κινδύνου

- **1 – 4:** Χαμηλός (Low)
- **5 – 9:** Μέτριος (Medium)
- **10 – 16:** Υψηλός (High)
- **17 – 25:** Κρίσιμος (Critical)

6.4 Προτάσεις Τεχνολογιών και Μέτρων Προστασίας Ιδιωτικότητας

Για την αντιμετώπιση των παραπάνω απειλών ιδιωτικότητας σε ένα έξυπνο δαχτυλίδι μπορούν να εφαρμοστούν οι ακόλουθες PETs, τόσο σε επίπεδο συσκευής όσο και σε επίπεδο εφαρμογής και νέφους. Οι προτάσεις οργανώνονται ανά ομάδα απειλών LINDDUN.

6.4.1 PETs για Αποκάλυψη Πληροφοριών (Disclosure) και Αναγνωρισιμότητα (Identifiability)

Κρυπτογράφηση End-to-End

- **Εφαρμογή:** Κρυπτογράφηση των βιομετρικών δεδομένων (PPG signals, θερμοκρασία) απευθείας στον μικροεπεξεργαστή του δαχτυλιδιού πριν από την αποστολή μέσω BLE. Τα κλειδιά αποκρυπτογράφησης διατηρούνται μόνο στη συσκευή του χρήστη (zero-knowledge cloud architecture).

Ομομορφική Κρυπτογράφηση

- **Εφαρμογή:** Επιτρέπει στον διακομιστή (Cloud) να εκτελεί υπολογισμούς και αναλύσεις (π.χ. υπολογισμός φάσεων ύπνου) πάνω σε κρυπτογραφημένα δεδομένα χωρίς να τα αποκρυπτογραφεί ποτέ κατά την επεξεργασία.

Διαφορική Ιδιωτικότητα

- **Εφαρμογή:** Προσθήκη ελεγχόμενου μαθηματικού «θορύβου» στα βιομετρικά δεδομένα πριν από την αποστολή τους στο cloud για ανάλυση ή εκπαίδευση μοντέλων AI.
- **Όφελος:** Επιτρέπει την εξαγωγή στατιστικών μοτίβων υγείας χωρίς να αποκαλύπτεται το ακριβές βιομετρικό αποτύπωμα του συγκεκριμένου χρήστη.

6.4.2 PETs για Συνδεσιμότητα (Linkability) και Ανιχνευσιμότητα (Detectability)

Ψευδωνυμοποίηση - Ephemeral Identifiers & BLE MAC Address Randomization

- **Εφαρμογή:** Εφαρμογή δυναμικής αλλαγής της διεύθυνσης MAC του Bluetooth σε τακτά χρονικά διαστήματα (π.χ., κάθε 15 λεπτά) και χρήση εφήμερων αναγνωριστικών συνεδρίας (session tokens).
- **Όφελος:** Αποτρέπει τρίτους σαρωτές (trackers) σε δημόσιους χώρους από το να συνδέσουν τις μετακινήσεις με τη συγκεκριμένη συσκευή.

Ανωνυμοποίηση - k-Anonymity στην επικοινωνία με το νέφος

- **Εφαρμογή:** Ομαδοποίηση των δεδομένων k χρηστών πριν από την επεξεργασία στο νέφος, ώστε κάθε εγγραφή να μην διακρίνεται από τουλάχιστον $k-1$ άλλες. Αυτό εμποδίζει την εξαγωγή συμπερασμάτων για μεμονωμένους χρήστες από συγκεντρωτικά δεδομένα, ενισχύοντας την προστασία κατά την ανάλυση δεδομένων υγείας.

Ανωνυμοποίηση - Mixnets για Δρομολόγηση Αιτημάτων Συγχρονισμού

- **Εφαρμογή:** Δρομολόγηση των αιτημάτων συγχρονισμού μέσω ενδιάμεσων κόμβων (mix nodes) που αναμειγνύουν τα μηνύματα πολλαπλών χρηστών, αποκρύπτοντας τα μεταδεδομένα επικοινωνίας (διεύθυνση IP, χρόνος, συχνότητα). Αυτό προστατεύει από επιθέσεις ανίχνευσης και συσχέτισης σε επίπεδο δικτύου.

6.4.3 PETs για Έλλειψη Ενημέρωσης (Unawareness) και Μη-Συμμόρφωση (Non-compliance)

User-Centric Privacy Dashboards & Just-in-Time Consent

- **Εφαρμογή:** Δημιουργία διαδραστικού πίνακα ελέγχου στη συνοδευτική εφαρμογή, ο οποίος επιτρέπει στον χρήστη να βλέπει ποια δεδομένα συλλέγονται, να τροποποιεί τις προτιμήσεις του και να ανακαλεί τη συγκατάθεσή του εύκολα. Παράλληλα, εφαρμογή ειδοποιήσεων Just-in-Time που ζητούν ρητή συγκατάθεση τη στιγμή που το δαχτυλίδι πρόκειται να καταγράψει ή να μοιραστεί ευαίσθητα δεδομένα (π.χ., παρακολούθηση εμμηνορροϊκού κύκλου).

Data Minimization Engine (On-Device Processing)

- **Εφαρμογή:** Επεξεργασία των ακατέργαστων δεδομένων (raw PPG waveforms) τοπικά στον επεξεργαστή του δαχτυλιδιού ή του smartphone (Edge Computing).
- **Όφελος:** Στο cloud αποστέλλονται μόνο συγκεντρωτικά/παράγωγα αποτελέσματα (π.χ. «μέσοι παλμοί: 72 bpm») και όχι τα πλήρη ακατέργαστα σήματα.

Decentralized Identifiers (DIDs) & Self-Sovereign Identity (SSI)

- **Εφαρμογή:** Χρήση αποκεντρωμένων ταυτοτήτων αντί για κλασικά email/passwords για τη σύνδεση της συσκευής στο οικοσύστημα, ώστε ο χρήστης να διατηρεί τον πλήρη έλεγχο της ψηφιακής του ταυτότητας.

6.5 Νομική και Κανονιστική Συμμόρφωση των Προτεινόμενων Μέτρων

Ο Πίνακας 4 αντιστοιχίζει τις προτεινόμενες PETs με τα σχετικά άρθρα του GDPR και συνοψίζει τη συμβολή κάθε μίας στη συμμόρφωση.

Πίνακας 4: *Αντιστοίχιση των προτεινόμενων PETs με άρθρα του GDPR*

PET	Άρθρα GDPR	Συμβολή στη συμμόρφωση
Κρυπτογράφηση End-to-End	Άρθρο 32	Εμπιστευτικότητα κατά τη μετάδοση και αποθήκευση, με κλειδιά αποκλειστικά στον χρήστη.
Ομομορφική Κρυπτογράφηση	Άρθρο 32	Ανάλυση στο νέφος χωρίς αποκρυπτογράφηση, μηδενική πρόσβαση του παρόχου στα δεδομένα.
Διαφορική Ιδιωτικότητα	Άρθρο 5 παρ. 1 στοιχ. γ, Άρθρο 25	Προστασία από συναγωγή και επαναναγνώριση, εξαγωγή στατιστικών μοτίβων με ασφάλεια.
Ψευδωνυμοποίηση (Ephemeral IDs, BLE MAC Randomization)	Άρθρο 4 παρ. 5, Άρθρο 5 παρ. 1 στοιχ. γ	Αποτροπή συσχέτισης και ανίχνευσης μέσω Bluetooth.
k-Anonymity	Άρθρο 5 παρ. 1 στοιχ. γ, Άρθρο 25	Ομαδοποίηση k χρηστών, αποτροπή εξαγωγής συμπερασμάτων για μεμονωμένα άτομα.
Mixnets	Άρθρο 32, Άρθρο 25	Απόκρυψη μεταδεδομένων επικοινωνίας (IP, χρόνος, συχνότητα).

PET	Άρθρα GDPR	Συμβολή στη συμμόρφωση
Privacy Dashboards & Just-in-Time Consent	Άρθρο 7, Άρθρα 13–14	Ενημερωμένη, συγκεκριμένη και ανακλητή συγκατάθεση, διαφάνεια.
Data Minimization Engine	Άρθρο 5 παρ. 1 στοιχ. γ	Αποστολή μόνο παράγωγων δεδομένων, ελαχιστοποίηση όγκου.
DIDs & SSI	Άρθρο 5 παρ. 1 στοιχ. γ, Άρθρο 25	Αυτονομία χρήστη, ελαχιστοποίηση δεδομένων κατά την αυθεντικοποίηση.

Τα προτεινόμενα μέτρα καλύπτουν τις επτά θεμελιώδεις αρχές του Άρθρου 5 του GDPR ως εξής:

- **Διαφάνεια:** Τα User-Centric Privacy Dashboards και οι ειδοποιήσεις Just-in-Time εξασφαλίζουν διαφάνεια και ενημερωμένη συγκατάθεση, επιτρέποντας στον χρήστη να γνωρίζει ποια δεδομένα συλλέγονται και να τροποποιεί τις προτιμήσεις του. Τα ZKP θα μπορούσαν να ενισχύσουν περαιτέρω την απόδειξη συμμόρφωσης χωρίς αποκάλυψη δεδομένων.
- **Περιορισμός του Σκοπού:** Η Ψευδωνυμοποίηση και η k-Anonymity περιορίζουν τη χρήση δεδομένων στους δηλωμένους σκοπούς, ενώ τα DIDs/SSI διασφαλίζουν ότι η ταυτότητα χρησιμοποιείται μόνο για την αυθεντικοποίηση και όχι για δευτερογενείς σκοπούς.
- **Ελαχιστοποίηση Δεδομένων:** Το Data Minimization Engine, η k-Anonymity και η επεξεργασία επί της συσκευής (On-Device Processing) μειώνουν δραστικά τον όγκο των δεδομένων που διακινούνται και αποθηκεύονται στο νέφος, συμμορφούμενα με την αρχή της ελαχιστοποίησης.
- **Ακρίβεια:** Η τοπική επεξεργασία και η διαφορική ιδιωτικότητα διατηρούν την ακρίβεια των παραγόμενων αποτελεσμάτων, ενώ παράλληλα προστατεύουν τα ατομικά δεδομένα από μη εξουσιοδοτημένη πρόσβαση.
- **Περιορισμός Αποθήκευσης:** Η αποστολή μόνο παράγωγων δεδομένων στο νέφος, σε συνδυασμό με την k-Anonymity, περιορίζει τον χρόνο και τον όγκο αποθήκευσης ευαίσθητων πληροφοριών.
- **Ακεραιότητα και Εμπιστευτικότητα:** Η κρυπτογράφηση End-to-End, η ομομορφική κρυπτογράφηση και τα Mixnets θωρακίζουν τα δεδομένα σε όλα τα στάδια της επεξεργασίας, από τη συσκευή έως το νέφος.
- **Λογοδοσία:** Η τεκμηρίωση των μέτρων, η διενέργεια PIA (Άρθρο 35) και η τήρηση αρχείων δραστηριοτήτων επεξεργασίας (Άρθρο 30) αποδεικνύουν τη συμμόρφωση του υπευθύνου επεξεργασίας.

Ωστόσο, τα βιομετρικά δεδομένα που συλλέγονται από το έξυπνο δαχτυλίδι (καρδιακός ρυθμός, HRV, SpO_2, θερμοκρασία, δεδομένα κύκλου) συνιστούν ειδικές κατηγορίες δεδομένων κατά την έννοια του Άρθρου 9 του GDPR. Αυτό συνεπάγεται πρόσθετες υποχρεώσεις:

- **Ρητή Συγκατάθεση:** Η επεξεργασία δεδομένων υγείας απαιτεί ρητή συγκατάθεση (explicit consent), η οποία δεν μπορεί να τεκμαίρεται από σιωπή ή αδράνεια. Τα User-Centric Privacy Dashboards και οι ειδοποιήσεις Just-in-Time διασφαλίζουν ότι η συγκατάθεση είναι

ενημερωμένη, συγκεκριμένη και ανακλητή, ενώ τα DIDs/SSI ενισχύουν την αυθεντικοποίηση της ταυτότητας του χρήστη κατά τη διαδικασία συγκατάθεσης.

- **Περιορισμοί στη Διεθνή Μεταφορά:** Η χρήση Mixnets και κρυπτογράφησης End-to-End διευκολύνει τη συμμόρφωση με τα Άρθρα 44–49, καθώς τα δεδομένα παραμένουν κρυπτογραφημένα ακόμη και κατά τη διασυνοριακή μεταφορά. Παρόλα αυτά, απαιτούνται πρόσθετες εγγυήσεις, όπως Πρότυπες Συμβατικές Ρήτρες (SCCs) και αξιολογήσεις επιπτώσεων μεταφοράς (TIAs).
- **Εκτίμηση Αντικτύπου (DPIA):** Βάσει του Άρθρου 35, η επεξεργασία δεδομένων υγείας σε μεγάλη κλίμακα απαιτεί DPIA. Η μεθοδολογία PIA της CNIL μπορεί να εφαρμοστεί για την αξιολόγηση των κινδύνων και την τεκμηρίωση των μέτρων μετριασμού, συμπεριλαμβανομένων των PETs που προτάθηκαν.

Παρά την ισχυρή τεχνική ενίσχυση που παρέχουν οι προτεινόμενες PETs, η πλήρης συμμόρφωση με τον GDPR απαιτεί πρόσθετα οργανωτικά και νομικά μέτρα:

- **Συμφωνίες Επεξεργασίας Δεδομένων (DPAs):** Απαιτούνται με όλους τους τρίτους (παρόχους νέφους, διαφημιστές, ερευνητές) για τη διασφάλιση της συμμόρφωσης. Η ύπαρξη DIDs/SSI διευκολύνει τη διαχείριση των συγκαταθέσεων και την ιχνηλασιμότητα των ροών δεδομένων.
- **Διαχείριση Δικαιωμάτων Υποκειμένων:** Παρόλο που τα dashboards διευκολύνουν την άσκηση των δικαιωμάτων πρόσβασης, διόρθωσης και διαγραφής, η τεχνική υλοποίηση της διαγραφής σε κατανεμημένα συστήματα (π.χ., ομοσπονδιακή μάθηση, Mixnets) παραμένει πρόκληση. Απαιτούνται σαφείς διαδικασίες και μηχανισμοί για την ικανοποίηση των αιτημάτων των χρηστών.
- **Ενημέρωση και Εκπαίδευση:** Οι χρήστες πρέπει να κατανοούν τις ρυθμίσεις ιδιωτικότητας και τις επιπτώσεις των επιλογών τους. Απαιτούνται σαφείς πολιτικές απορρήτου και εκπαιδευτικό υλικό, ενώ τα dashboards πρέπει να είναι σχεδιασμένα με τρόπο που να μην αποπροσανατολίζει τον χρήστη.
- **Συνεχής Παρακολούθηση και Προσαρμογή:** Η συμμόρφωση δεν είναι μια εφάπαξ διαδικασία. Απαιτείται συνεχής παρακολούθηση των εξελισσόμενων απειλών, ενημέρωση των PETs και επαναξιολόγηση των κινδύνων, ιδίως όταν επέρχονται αλλαγές στο ρυθμιστικό πλαίσιο ή στην αρχιτεκτονική του συστήματος.

6.6 Συζήτηση Αποτελεσμάτων

Η ανάλυση με τη μεθοδολογία LINDDUN ανέδειξε απειλές και στις επτά κατηγορίες για το έξυπνο δαχτυλίδι, με κρισιμότερες την Αποκάλυψη Πληροφοριών (Disclosure) και τη Μη-Συμμόρφωση (Non-compliance), ακολουθούμενες από τη Συνδεσιμότητα (Linkability), την Αναγνωρισιμότητα (Identifiability) και την Έλλειψη Ενημέρωσης (Unawareness). Οι απειλές αυτές τεκμηριώνονται από πραγματικά περιστατικά (π.χ. η παραβίαση της Ultrahuman το 2026 και οι ευπάθειες BLE) και

οδήγησαν στην πρόταση ενός πολυεπίπεδου πλαισίου PETs, κατανεμημένων σε επίπεδο συσκευής, εφαρμογής και νέφους.

Τα προτεινόμενα μέτρα αναμένεται να μειώσουν σημαντικά τους κινδύνους ιδιωτικότητας:

- Κρυπτογράφηση End-to-End και Ομομορφική Κρυπτογράφηση θωρακίζουν τα δεδομένα σε κάθε στάδιο, επιτρέποντας παράλληλα την ανάλυση στο νέφος χωρίς αποκάλυψη.
- Διαφορική Ιδιωτικότητα και k-Anonymity προστατεύουν από συναγωγή και επαναναγνώριση, διατηρώντας τη στατιστική χρησιμότητα.
- Ψευδωνυμοποίηση, Ephemeral Identifiers και Mixnets αποτρέπουν τη συσχέτιση και την ανίχνευση σε επίπεδο δικτύου.
- Privacy Dashboards, Just-in-Time Consent και DIDs/SSI ενισχύουν τη διαφάνεια, τον έλεγχο και την αυτονομία του χρήστη.

Ωστόσο, το υπολογιστικό κόστος της ομομορφικής κρυπτογράφησης και των ZKP επιβαρύνει την μπαταρία, η διαφορική ιδιωτικότητα εισάγει θόρυβο που μειώνει την ακρίβεια, ενώ η πολυπλοκότητα υλοποίησης απαιτεί εξειδικευμένες γνώσεις.

Οι περιορισμοί που προκύπτουν από την ανάλυση είναι οι εξής:

- **Ποιοτική φύση της LINDDUN:** Δεν ποσοτικοποιεί τον κίνδυνο, απαιτώντας συμπληρωματικές μεθόδους όπως η PIA.
- **Έλλειψη πραγματικών δεδομένων:** Η ανάλυση βασίζεται σε θεωρητικό μοντέλο και όχι σε δεδομένα από πραγματικές δοκιμές πεδίου.
- **Γενικευσιμότητα:** Τα αποτελέσματα ενδέχεται να μην επεκτείνονται σε όλα τα έξυπνα δαχτυλίδια.
- **Τεχνικοί περιορισμοί:** Οι συσκευές έχουν περιορισμένους πόρους και χωρητικότητα μνήμης, γεγονός που περιορίζει την εφαρμογή ορισμένων PETs.
- **Νομικές προκλήσεις:** Η διασυνοριακή μεταφορά και η τεχνική υλοποίηση της διαγραφής σε κατανεμημένα συστήματα παραμένουν δύσκολες ως προς την συμμόρφωσης με τον GDPR.

7 *Συμπεράσματα και Μελλοντική Έρευνα*

7.1 Σύνοψη της Εργασίας

Η παρούσα διπλωματική εργασία είχε ως αντικείμενο τη συστηματική μελέτη των ζητημάτων ιδιωτικότητας που προκύπτουν στα ενδυτά συστήματα (wearable systems). Μέσα από μια ολιστική προσέγγιση που συνδύασε βιβλιογραφική επισκόπηση, ανάλυση απειλών με τη μεθοδολογία LINDDUN, αξιολόγηση Τεχνολογιών Ενίσχυσης Ιδιωτικότητας (PETs) και εξέταση του νομικού πλαισίου, η εργασία ανέδειξε το πολυδιάστατο τοπίο των κινδύνων που αντιμετωπίζουν οι χρήστες φορητών συσκευών. Τα ευρήματα αυτά επιβεβαιώθηκαν μέσω της μελέτης περίπτωσης των έξυπνων δαχτυλιδιών, στην οποία εφαρμόστηκε το σύνολο του θεωρητικού πλαισίου.

Πιο συγκεκριμένα:

1. Στο Κεφάλαιο 1 παρουσιάστηκε το πλαίσιο της εργασίας, ο σκοπός, το αντικείμενο και η δομή της.
2. Στο Κεφάλαιο 2 αναλύθηκαν τα ενδυτά συστήματα ως τεχνολογική κατηγορία, με έμφαση στους αισθητήρες, τις λειτουργίες, τις εφαρμογές και τις προκλήσεις τους.
3. Στο Κεφάλαιο 3 δόθηκε έμφαση στους κινδύνους και τις απειλές ιδιωτικότητας που σχετίζονται με τα ενδυτά συστήματα, με έμφαση στη συλλογή και υπερσυλλογή δεδομένων, την παρακολούθηση συμπεριφοράς, τις διαρροές, την επαναναγνώριση και την έλλειψη διαφάνειας, τεκμηριωμένες με πραγματικά περιστατικά παραβίασης δεδομένων.
4. Στο Κεφάλαιο 4 παρουσιάστηκαν οι βασικές PETs (ανωνυμοποίηση και ψευδωνυμοποίηση, ομομορφική κρυπτογράφηση, ασφαλής πολυμερής υπολογιστική, διαφορική ιδιωτικότητα, αποδεικτικά μηδενικής γνώσης, ομοσπονδιακή μάθηση και κατανεμημένη αναλυτική), καθώς και οι συνδυαστικές προσεγγίσεις για βέλτιστη προστασία.
5. Στο Κεφάλαιο 5 εξετάστηκε το νομικό και κανονιστικό πλαίσιο, με έμφαση στον GDPR, τις απαιτήσεις συμμόρφωσης.
6. Στο Κεφάλαιο 6 εφαρμόστηκε όλη η θεωρητική γνώση σε μια μελέτη περίπτωσης έξυπνου δαχτυλιδιού, αναδεικνύοντας απειλές, προτείνοντας PETs και αξιολογώντας τη νομική συμμόρφωση.

7.2 Κύρια Ευρήματα

Τα κυριότερα ευρήματα της εργασίας συνοψίζονται ως εξής:

1. **Τα ενδυτά συστήματα αντιμετωπίζουν πολυδιάστατες απειλές ιδιωτικότητας.** Η μαζική και συνεχής συλλογή βιομετρικών δεδομένων, η παρακολούθηση συμπεριφοράς, οι διαρροές, η επαναναγνώριση και η έλλειψη διαφάνειας συνθέτουν ένα σύνθετο τοπίο κινδύνων. Η μεθοδολογία LINDDUN αποδείχθηκε αποτελεσματική για τη συστηματική ανάδειξη αυτών των απειλών, καλύπτοντας επτά διακριτές κατηγορίες.
2. **Οι PETs αποτελούν τα βασικά τεχνικά εργαλεία για την προστασία της ιδιωτικότητας.** Κάθε τεχνολογία προσφέρει συγκεκριμένα πλεονεκτήματα, αλλά καμία δεν επαρκεί από μόνη της. Ο συνδυασμός διαφορετικών PETs, όπως ομοσπονδιακή μάθηση με διαφορική ιδιωτικότητα ή ομομορφική κρυπτογράφηση, παρέχει πολυεπίπεδη προστασία και αντισταθμίζει τους επιμέρους περιορισμούς. Πρόσφατες έρευνες δείχνουν ότι ολοκληρωμένα πλαίσια PETs μπορούν να μειώσουν τους κινδύνους ιδιωτικότητας έως και 70%.
3. **Η συμμόρφωση με τον GDPR είναι υποχρεωτική αλλά απαιτεί ολιστική προσέγγιση.** Τα δεδομένα υγείας που συλλέγονται από ενδυτά συστήματα εμπίπτουν στις ειδικές κατηγορίες του Άρθρου 9, απαιτώντας ρητή συγκατάθεση και αυστηρά μέτρα ασφαλείας. Οι PETs αποτελούν τα τεχνικά μέσα υλοποίησης των νομικών απαιτήσεων, αλλά η πλήρης συμμόρφωση προϋποθέτει επιπλέον οργανωτικά μέτρα, όπως PIA, DPAs και διαχείριση διασυνοριακών ροών.
4. **Τα έξυπνα δαχτυλίδια παρουσιάζουν ιδιαίτερες προκλήσεις.** Η διακριτικότητά τους, η συνεχής λειτουργία τους, οι περιορισμένοι πόροι τους και η έλλειψη οθόνης τα καθιστούν ευάλωτα σε επιθέσεις και δυσχεραίνουν την άσκηση ελέγχου από τον χρήστη. Παράλληλα, η διαχείριση ευαίσθητων δεδομένων απαιτεί αυξημένη προσοχή.
5. **Η ισορροπία μεταξύ προστασίας και λειτουργικότητας είναι κρίσιμη.** Η εφαρμογή προηγμένων PETs συνεπάγεται υπολογιστικό κόστος, απώλεια ακρίβειας και πολυπλοκότητα υλοποίησης. Οι κατασκευαστές καλούνται να βρουν τη βέλτιστη ισορροπία, λαμβάνοντας υπόψη τις ανάγκες των χρηστών, τους διαθέσιμους πόρους και τις ρυθμιστικές απαιτήσεις.

7.3 Συμβολή της Εργασίας

Σε θεωρητικό επίπεδο, η εργασία παρέχει μια ολοκληρωμένη επισκόπηση των απειλών ιδιωτικότητας στα ενδυτά συστήματα, οργανωμένη βάσει του πλαισίου LINDDUN. Επιπλέον, αναλύει τις σύγχρονες PETs και τις συνδυαστικές προσεγγίσεις τους, προσφέροντας ένα ενημερωμένο εργαλείο αναφοράς. Τέλος, συνδέει την τεχνική ανάλυση με το νομικό πλαίσιο του GDPR, αναδεικνύοντας την αλληλεξάρτηση τεχνολογίας και κανονιστικών απαιτήσεων.

Σε πρακτικό επίπεδο, η εργασία: (α) προσφέρει ένα μεθοδολογικό πρότυπο για την ανάλυση απειλών ιδιωτικότητας σε ενδυτά συστήματα, το οποίο μπορεί να εφαρμοστεί σε διαφορετικά σενάρια· (β) προτείνει συγκεκριμένα μέτρα μετριασμού για τα έξυπνα δαχτυλίδια, αξιοποιήσιμα από κατασκευαστές και σχεδιαστές· και (γ) αναδεικνύει τις προκλήσεις συμμόρφωσης, καθώς και πρακτικές λύσεις για την αντιμετώπισή τους.

7.4 Περιορισμοί και Μελλοντική Έρευνα

Η εργασία υπόκειται σε ορισμένους περιορισμούς: η μελέτη περίπτωσης βασίστηκε σε θεωρητικό μοντέλο και σε δημοσίως διαθέσιμες πληροφορίες και όχι σε δεδομένα πεδίου, ενώ η αξιολόγηση κινδύνου είχε ποιοτικό χαρακτήρα. Καθώς η τεχνολογία των ενδυτών συσκευών συνεχίζει να εξελίσσεται, η ισορροπία μεταξύ καινοτομίας και ιδιωτικότητας θα παραμείνει κεντρικό ζήτημα. Με την ολοκλήρωση της εργασίας τίθενται οι ακόλουθες κατευθύνσεις για μελλοντική έρευνα:

1. Ανάπτυξη ελαφρύτερων κρυπτογραφικών μεθόδων για συσκευές με περιορισμένους πόρους, όπως τα έξυπνα δαχτυλίδια.
2. Εξέταση της επίδρασης των αναδυόμενων τεχνολογιών (π.χ., 6G, edge computing, AI) στην ιδιωτικότητα των ενδυτών συστημάτων.
3. Πειραματική αξιολόγηση των προτεινόμενων PETs σε πραγματικές συσκευές, με μέτρηση της κατανάλωσης ενέργειας, της καθυστέρησης και της απώλειας ακρίβειας.
4. Ποσοτική αξιολόγηση κινδύνου με συνδυασμό της LINDDUN και της DPIA σε δεδομένα πεδίου από πραγματικούς χρήστες.

7.5 Επίλογος

Συμπερασματικά, η προστασία της ιδιωτικότητας στα ενδυτά συστήματα δεν αποτελεί απλώς μια τεχνική πρόκληση, αλλά ένα πολυδιάστατο ζήτημα που απαιτεί τη συνέργεια τεχνολογίας, νομικού πλαισίου και οργανωτικών πρακτικών. Τα έξυπνα δαχτυλίδια, ως αντιπροσωπευτικό παράδειγμα, αναδεικνύουν τόσο τις δυνατότητες όσο και τις ευπάθειες των φορητών συσκευών. Η υιοθέτηση των PETs από τον σχεδιασμό, σύμφωνα με την αρχή του Privacy by Design, αποτελεί τη μόνη βιώσιμη στρατηγική για την οικοδόμηση εμπιστοσύνης και τη διασφάλιση της βιωσιμότητας των εφαρμογών σε ένα αυστηρό ρυθμιστικό περιβάλλον.

Βιβλιογραφία

Article 29 Data Protection Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. *WP 248 rev.01*. Διαθέσιμο: https://ec.europa.eu/newsroom/article29/items/611236/en

Cavoukian, A. (2012), Privacy by Design. *IEEE Technology and Society Magazine*. Διαθέσιμο: https://presentations.boussiasevents.gr/files/_boussias_conferences_content/presentations/data_privacy/2022/Cavoukian_Data_Privacy_22.pdf

CNIL (2018a), *Privacy Impact Assessment (PIA) – Methodology*. Commission Nationale de l'Informatique et des Libertés. Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

CNIL (2018b), *Privacy Impact Assessment (PIA) – Knowledge Bases*. Commission Nationale de l'Informatique et des Libertés. Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

ENISA (2022), *Data Protection Engineering – From Theory to Practice*. European Union Agency for Cybersecurity, January 2022. Διαθέσιμο: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Data%20Protection%20Engineering.pdf

GDPR Local (2026), GDPR for Wearable Technology. Διαθέσιμο: https://gdprlocal.com/gdpr-for-wearable-technology/

Hong, J. I., Ng, J. D., Lederer, S., and Landay, J. A. (2004), Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In: *Proceedings of the 5th Conference on Designing Interactive Systems (DIS '04)*, ACM, New York, USA. Διαθέσιμο: https://dl.acm.org/doi/10.1145/1013115.1013125

Li, Y., et al. (2020), Wearable technology: Fundamentals, advancements and prospects. *IEEE Access 8, 110296–110317.* https://doi.org/10.1109/ACCESS.2020.2998393

Limniotis, K. (2022), Data Sharing – Use cases in the Health Care Sector. Personal Data Sharing – Emerging Technologies, ENISA Workshop. Brussels. Διαθέσιμο : https://www.enisa.europa.eu/sites/default/files/all_files/Kostas_Limniotis_ENISA%20Workshop%202022-10-07.pdf#1%231

LINDDUN (2026), *Privacy threat types*. KU Leuven. Διαθέσιμο: https://linddun.org

Mahyoub, M. (2024), Privacy Engineering in Smart Home (SH) Systems: A Comprehensive Privacy Threat Analysis and Risk Management Approach. Διαθέσιμο: https://www.academia.edu/145822661/Privacy_Engineering_in_Smart_Home_Sh_Systems_A_Comprehensive_Privacy_Threat_Analysis_and_Risk_Management_Approach

Shang, X. (2024), The Current Status and Future Trends of Wearable Devices. In: Proceedings of the 5th International Conference on Signal Processing and Machine Learning. Διαθέσιμο: https://www.researchgate.net/publication/387447374_The_Current_Status_and_Future_Trends_of_Wearable_Devices

Shirvani, G., Ghasemshirazi, S., and Beigzadeh, B. (2024), Federated Learning: Attacks, Defenses, Opportunities, and Challenges. *arXiv preprint* arXiv:2403.06067. Διαθέσιμο: https://arxiv.org/abs/2403.06067

Doherty C., Baldwin M., Lambe R., Altini M. (2025), Privacy in consumer wearable technologies: a living systematic analysis of data policies across leading manufacturers. Npj, digitalmedicine Διαθέσιμο: https://www.researchgate.net/publication/392696072_Privacy_in_consumer_wearable_technologies_a_living_systematic_analysis_of_data_policies_across_leading_manufacturers

Kurz M., Gstoettner R., Sonnleitner E. (2021), Smart Rings vs. Smartwatches: Utilizing Motion Sensors for Gesture Recognition . *Applied Sciences*, 11(5), 2015. Διαθέσιμο: https://www.mdpi.com/2076-3417/11/5/2015

Fiore M., Bianconi A., Sicari G., Conni A., Lenzi J., Tomaiuolo G., Zito F., Golinelli D., Sanmarchi F. (2024), The Use of Smart Rings in Health Monitoring—A Meta-Analysis. *Applied Sciences*, 14(23), 10778. Διαθέσιμο: https://www.mdpi.com/2076-3417/14/23/10778

Diamantopoulou V., Argyropoulos N., Kalloniatis C., Gritzalis S. (2017), Supporting the design of privacy-aware business processes via privacy process patterns. *IEEE Xplore*. Διαθέσιμο: https://ieeexplore.ieee.org/document/7956536

Ludwig J., Moonsamy V., Groβe-Kampann M. (2024), The Rings of Tracking: Evaluating Security and Privacy in the Smart Ring Ecosystem. *IEEE Xplore*. Διαθέσιμο: https://ieeexplore.ieee.org/document/10917364

Rai A. (2024), Smart Rings, Smarter Threats: The BLE Security Perspective [dataset]. Carnegie Mellon University, KiltHub. Διαθέσιμο: https://kilthub.cmu.edu/articles/dataset/Smart_Rings_Smarter_Threats_The_BLE_Security_Perspective/28098791

Saha T., Ding S., Qin S., Fishman H., Pham R. Gu T., Lin M., Xian Y., Sabbagh B., Abdal A., Ji G., Sakdaphetsiri K., Fung Y., Lam W., Khan M., Luan H., Wang Z., Tang S., Djassemi O., Sandhu S., Xu S., Wang J. (2026), A fully integrated smart ring for daily biochemical monitoring. *Nature Communications*. Διαθέσιμο: https://www.nature.com/articles/s41467-026-75980-z

Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο (2016), Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικός Κανονισμός για την Προστασία Δεδομένων). *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*, L 119, 4.5.2016. Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679